

# The Best Cyber Insights of 2023

Click each image to see each report in full. All were published in July 2023

## Average Ransom Payments

Amount of each known payment -20% from Q4/22

Average known  
Payout =



**USD \$327,883**



Published July 2023

## Cyber & Digital Identity

Framework to secure the use of DI

Published July '23



Published Jul '23

## Cyber Security Manual

Guide for Firms Against Threats



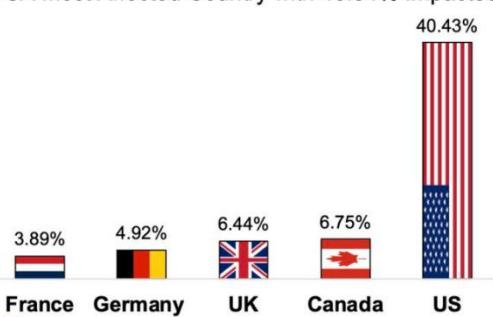
Published July 2023

## Exploring AI Risk

Open-Source Security Guide

## Ransom Victims By Country

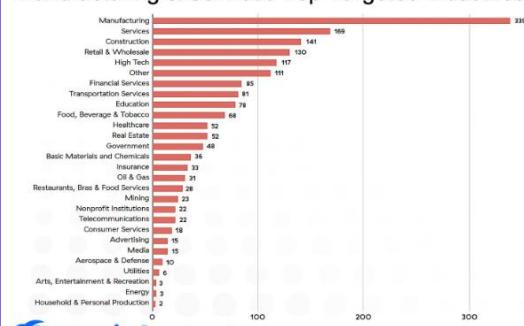
USA Most Affected Country with 40.34% Impacted



Published July 2023

## Ransom Attacks By Industry

Manufacturing & Services Top Targeted Industries



Published July 2023

## Top 5 Ransomware Families

based on the # of victims listed on their leak sites

#1 = LockBit

#2 = BlackCat/ALPHV

#3 = Clop

#4 = BlackBasta

#5 = Karakurt



Published July 2023

## Most Active Ransom Groups

49% of Ransomware Attacks are by LockBit

LockBit 49%

Clop 19%

BlackCat/ALPHV 13%

Royal 12%

Play 7%

Acronis

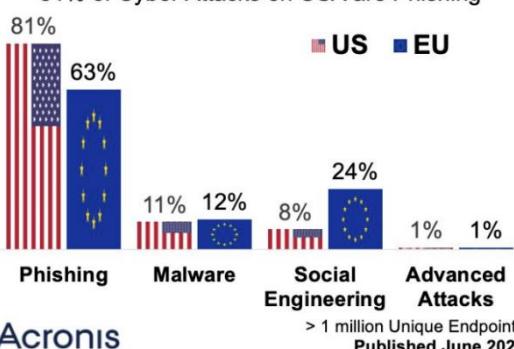
> 1 million Unique Endpoints  
Published June 2023

# The Best Cyber Insights of 2023

Click each image to see each report in full. All were published in July 2023

## US vs EU Cyber Attacks

81% of Cyber Attacks on USA are Phishing

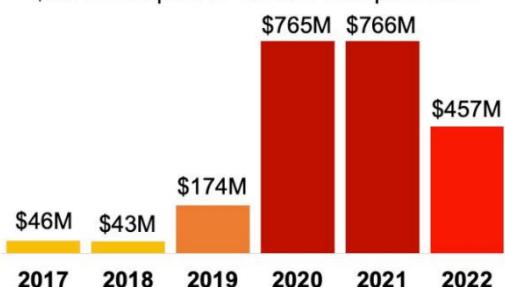


Acronis

> 1 million Unique Endpoints  
Published June 2023

## Payments to Ransom Groups

\$457M was paid to Ransom Groups in 2022

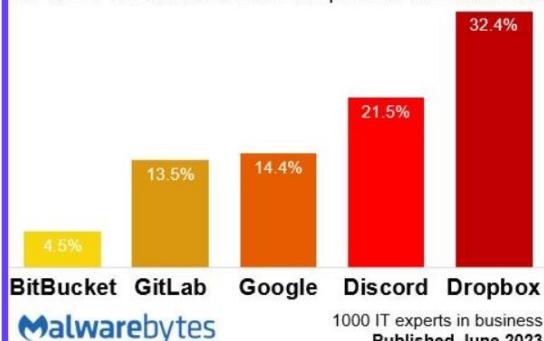


Acronis

> 1 million Unique Endpoints  
Published June 2023

## Malware Host Platforms

32.4% of Threat actors use Dropbox to host malware



Malwarebytes

1000 IT experts in business  
Published June 2023

## Malware ads Keywords

Rufus is the most common search word at 18.3%

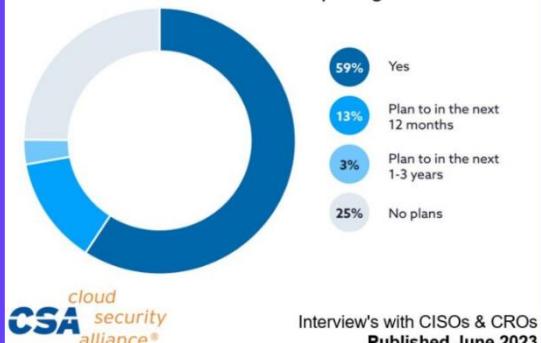


Malwarebytes

1000 IT experts in business  
Published June 2023

## Cloud Service Process

59% of Banks use cloud computing for their Data

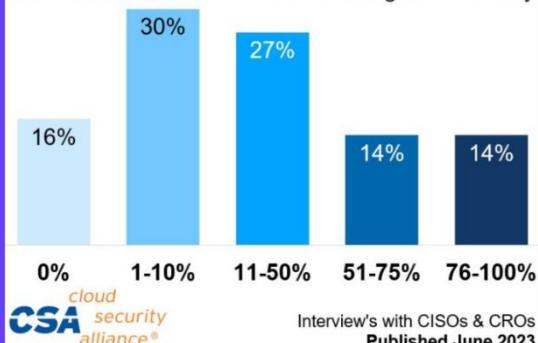


cloud security alliance®

Interview's with CISOs & CROs  
Published June 2023

## Public Cloud in Finance Orgs

28% use Public Cloud for >50% of regulated activity

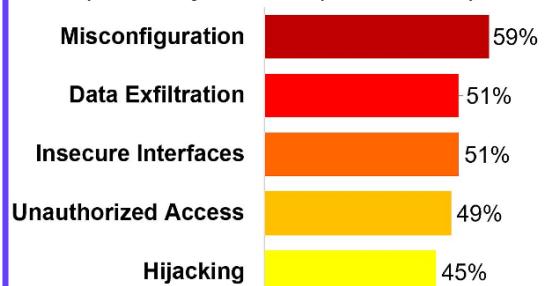


cloud security alliance®

Interview's with CISOs & CROs  
Published June 2023

## Top Cloud Security Threats

59% say Misconfiguration is top cloud security threat



CHECK POINT

Survey of 1,052 Cybersecurity Professionals  
Published June 2023

## Most Secure Insurance Firms

MetLife "most Cyber Secure Insurance firm in USA"

#1 = MetLife

#2 = MGIC

#3 = The Hartford

#4 = Guardian Life

#5 = Aegis

Security Scorecard Forbes

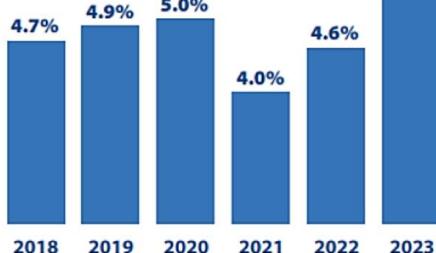
Forbes & Security Scorecard  
Published June 2023

# Cyber Insights: Cyber Budgets & Salaries

Click each image to see each report in full. All were published in June 2023

## Budget Increase < Inflation

Cybersecurity budget increase are at a six year high



Survey of 1,200 Security Pros  
Source: 2023 Cyberthreat Defense Report, CyberEdge Group, LLC

## Cybersecurity Budgets

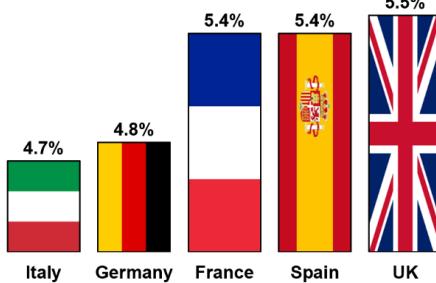
55% of cyber budgets increase by 5% to 9% in '23



Survey of 1,200 Security Pros  
Source: 2023 Cyberthreat Defense Report, CyberEdge Group, LLC

## European Cyber Budgets

5.5% increase in average cyber budget for UK firms



Survey of 1,200 Security Pros  
Source: 2023 Cyberthreat Defense Report, CyberEdge Group, LLC

## Cyber Investment Priorities

Top investment of Sec Leaders = Security Operations

- #1 = Security Operations with SIEM
- #2 = Vulnerability Management
- #3 = Identity & Access Management
- #4 = Endpoint Management & Protection
- #5 = Application & Product Security



Survey of 800 Cyber Security Leaders  
Published June 2023

## Growth in Spend on Cyber

23% annual revenue growth at Palo Alto Networks

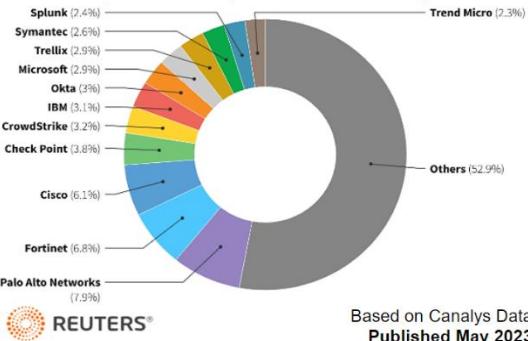
Palo Alto Networks • CrowdStrike Holdings • Zscaler



Refinitiv Analysts' Estimates for 2023  
Published May 2023

## Cyber Security Market

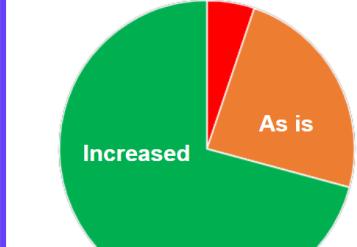
7.9% of Cyber Security Market share is by Palo Alto



Based on Canalys Data  
Published May 2023

## SaaS Resource Investment

Firms increase investment in SaaS Security Tools

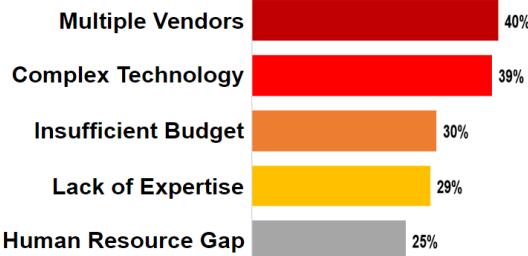


CSA cloud security alliance™

1,130 IT & Security Pros  
Published Jun 2023

## Barriers to Secure Identities

30% of firms cite Budget Limitations as a key barrier



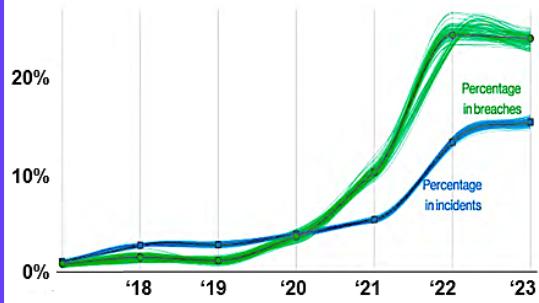
Survey of 529 Security Professionals  
Published June 2023

# Cyber Insights: Ransomware Numbers

Click each image to see each report in full. All were published in June 2023

## Ransoms in Cyber Attacks

Ransomware = 24% of Breaches & 16% of Incidents



**verizon** ✓

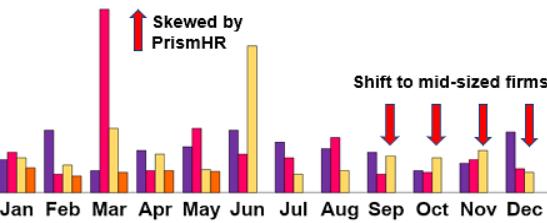
953,894 incidents, 254,968 breaches

Published June 2023

## Size of Ransom Victims

Ransom Gangs prefer targeting smaller sized firms

■ 2020 ■ 2021 ■ 2022 ■ 2023

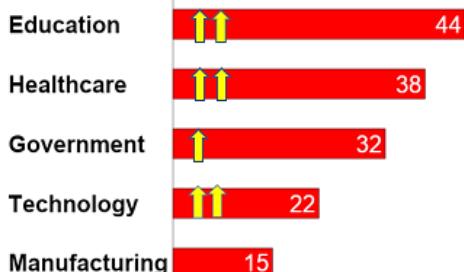


**BLACKFOG**  
Privacy. Security. Prevention.

Published June 2023

## Ransom Victims by Sector

Education experienced the most incidents this year

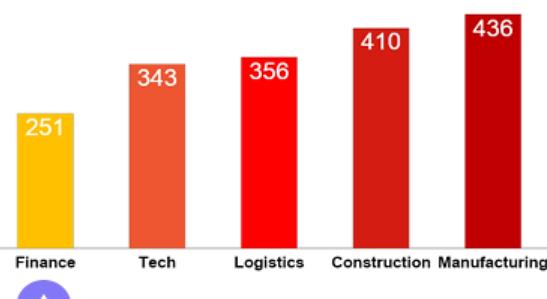


**BLACKFOG**  
Privacy. Security. Prevention.

Published June 2023

## Ransomware In Sectors

Manufacturing most targeted sector with 436 cases

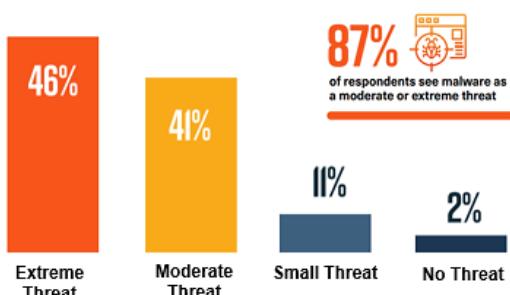


**NordLocker**

Analysis of 1 year of ransomware  
Published June 2023

## Ransomware Threat

87% says Malware is a moderate to extreme Threat

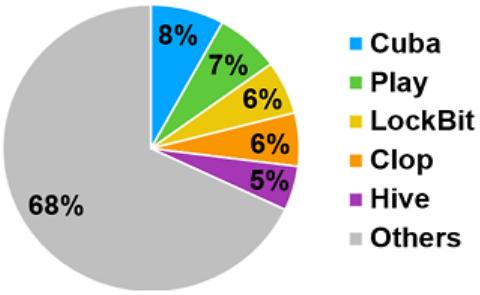


**BULLWALL**

Survey of 453 Cyber Pros  
Published May 2023

## Ransomware used in Q1 '23

Cuba was most active, followed by Play & LockBit



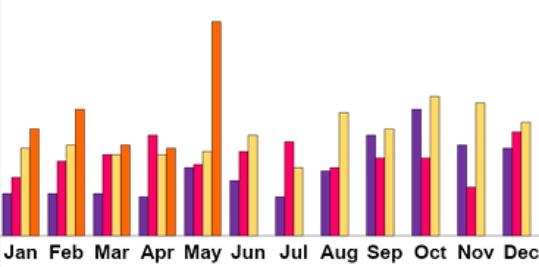
**Trellix**

Published June 2023

## # of “Successful” Ransoms

May had a massive 66 publicly disclosed attacks

■ 2020 ■ 2021 ■ 2022 ■ 2023



**BLACKFOG**  
Privacy. Security. Prevention.

Published June 2023

## # of Victims by Cyber Gang

Alphv number of victims increased 76% last month

Blackbasta ■ March ■ April

Royal ■ 16%

Bianlian ■ 67%

Alphv ■ 76%

Lockbit ■ 13%

**GUIDEPOINT SECURITY**

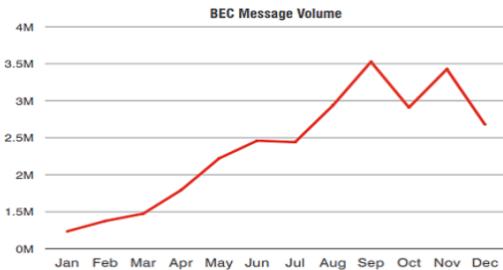
24 Ransom Leak Sites  
Published May 2023

# Cyber Insights: Threat Landscape

Click each image to see each report in full. All were published in June 2023

## Cyber Threat Landscape

3.5M of Business Email Compromised in September

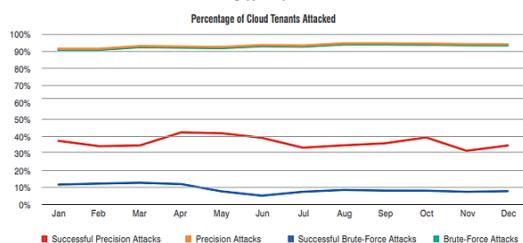


proofpoint.

Data from Proofpoint deployments  
Published June 2023

## Cyber Threat Landscape

98% of Cloud Tenants targeted by Precision

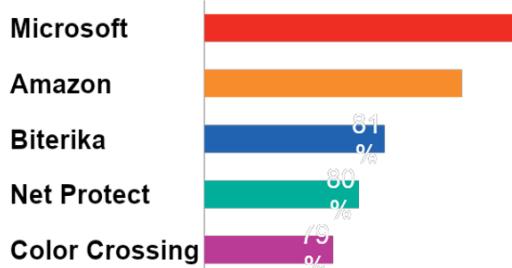


proofpoint.

Data from Proofpoint deployments  
Published June 2023

## Cyber Threat Landscape

86% brute-force attacks victims use Microsoft

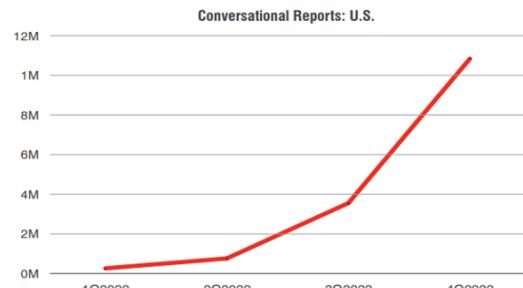


proofpoint.

Data from Proofpoint deployments  
Published June 2023

## Cyber Threat Landscape

Increasing trend in number of Conversational Attacks

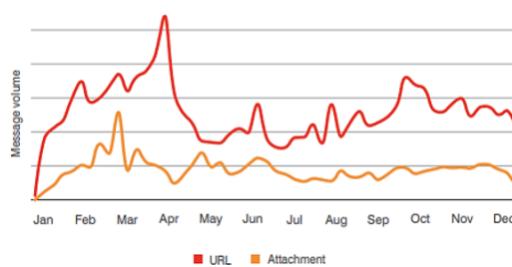


proofpoint.

Data from Proofpoint deployments  
Published June 2023

## Cyber Threat Landscape

URLs accounted three quarters of all threats overall

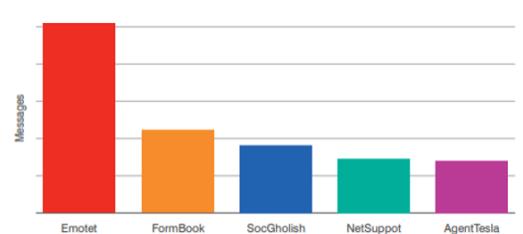


proofpoint.

Data from Proofpoint deployments  
Published June 2023

## Cyber Threat Landscape

Emotet is the leading choice of Malware

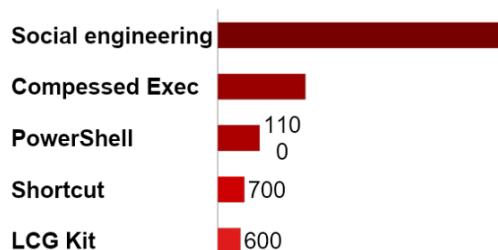


proofpoint.

Data from Proofpoint deployments  
Published June 2023

## Cyber Threat Landscape

Social Engineering is the most used technique

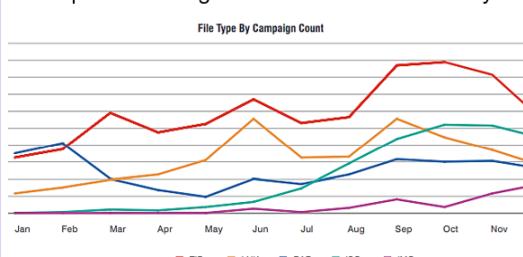


proofpoint.

Data from Proofpoint deployments  
Published June 2023

## Cyber Threat Landscape

Zip files leading choice for Malware delivery

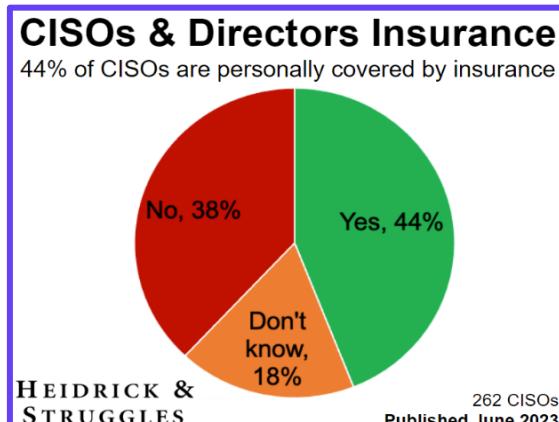
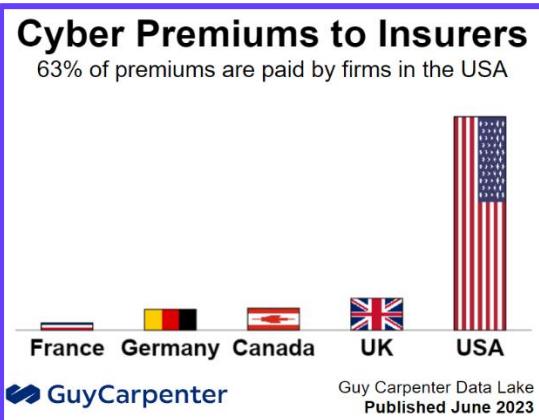
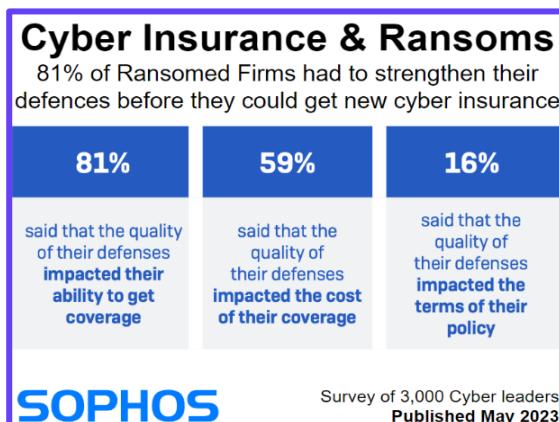
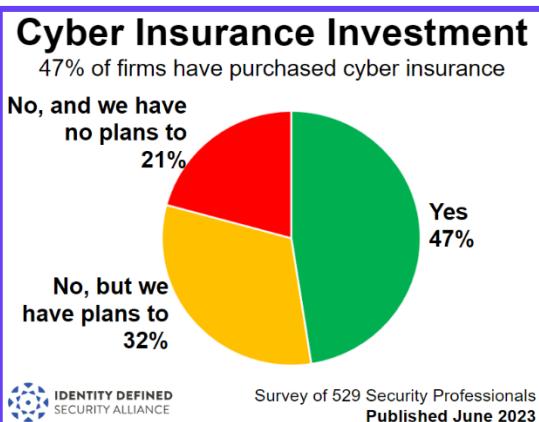
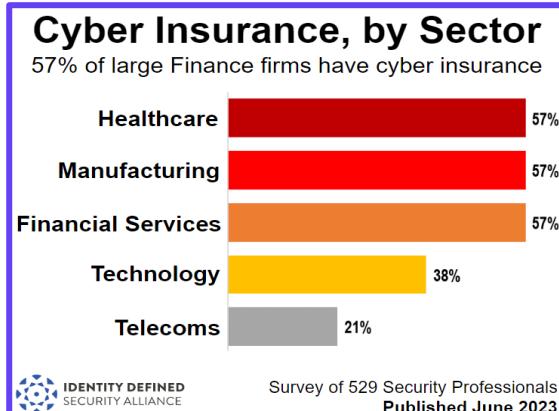
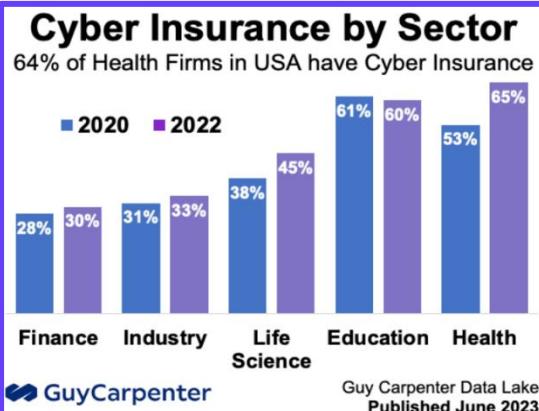


proofpoint.

Data from Proofpoint deployments  
Published June 2023

# Cyber Insights: Insurance

Click each image to see each report in full. All were published in June 2023



# Cyber Insights: CISOs & Execs

Click each image to see each report in full. All were published in June 2023

## Top Board CISO Traits

Infosec tenure ranked at top trait for Board CISOs

#1 = Tenure

#2 = Experience

#3 = Scalability

#4 = Education

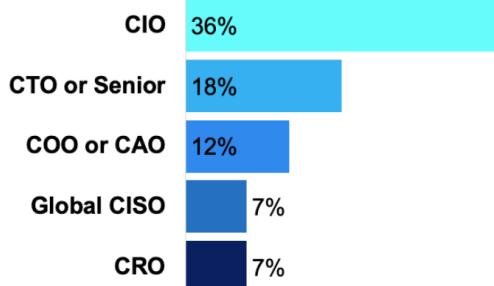
#5 = Diversity



More than 330 CISOs  
Published June 2023

## CISOs Reporting Line

36% of CISOs report to the Chief Information Officer

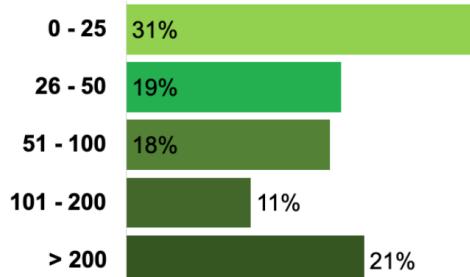


HEIDRICK &  
STRUGGLES

262 senior CISOs interviewed by H&S  
Published June 2023

## CISO Department Size

31% of CISOs have < 26 Staff in their Department

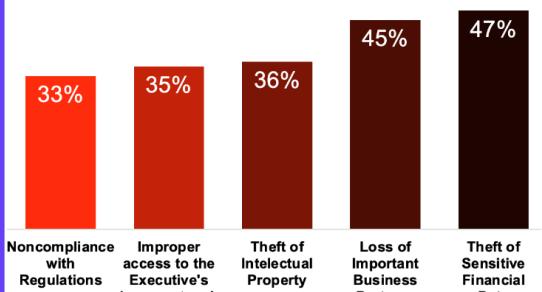


HEIDRICK &  
STRUGGLES

262 senior CISOs interviewed by H&S  
Published June 2023

## Cyber Attacks on Executives

47% involve theft of sensitive financial data

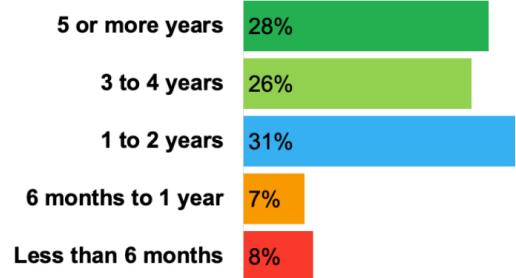


BLACK CLOAK

16,400 IT Security Pro's  
Published May 2023

## CISOs Tenure in Current Job

8% of CISOs have been in role less than 6 months



HEIDRICK &  
STRUGGLES

262 senior CISOs interviewed by H&S  
Published June 2023

## Functions owned by CISOs

90% of CISOs own the Security Operations function

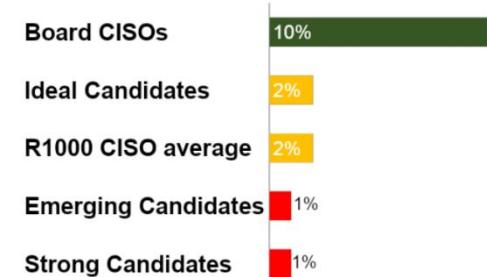


HEIDRICK &  
STRUGGLES

262 senior CISOs interviewed by H&S  
Published June 2023

## CISOs Ready for the Board?

10% of CISOs at biggest firms are board certified

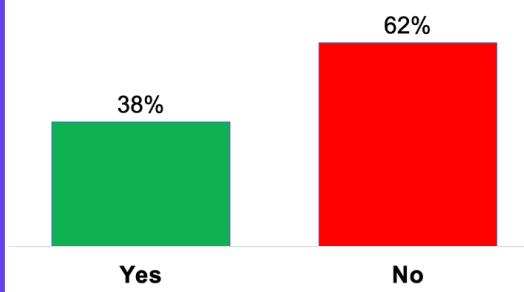


IANS + ARTICO + CAP

More than 330 CISOs  
Published June 2023

## Cyber Attacks on Executives

62% of Companies don't have a dedicated team



BLACK CLOAK

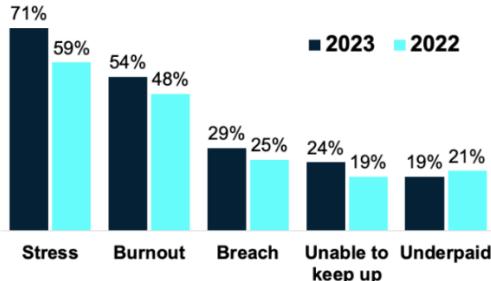
16,400 IT Security Pro's  
Published May 2023

# Cyber Insights: CISOs Challenges

Click each image to see each report in full. All were published in June 2023

## Why CISOs Quit their Job

71% of CISOs say **Stress** might make them resign



HEIDRICK & STRUGGLES

262 CISOs  
Published June 2023

## Top Concerns of Cyber Pros

Insufficient Staff is most often mentioned by CISOs

- #1 = Insufficient Staff
- #2 = Culture of Organisation
- #3 = Speed of Business Change
- #4 = Budget
- #5 = **Shadow IT**

CLUBCISO  
Powered by Telstra Purple

Survey of 800 Cyber Security Leaders  
Published June 2023

## Digitization CISO Challenges

48% say Personal Litigation is CISO's top challenge

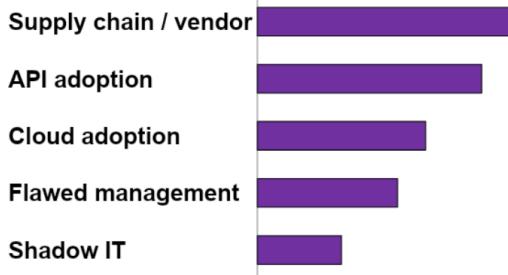


SALT

Survey of 300 CISOs & CSOs  
Published June 2023

## Digitization CISO Challenges

38% say Supply chains are the biggest security gap

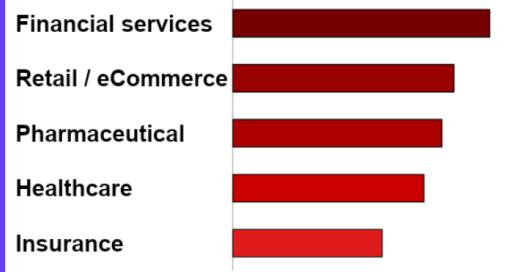


SALT

Survey of 300 CISOs & CSOs  
Published June 2023

## Digitization CISO Challenges

43% say Finance API security a top priority

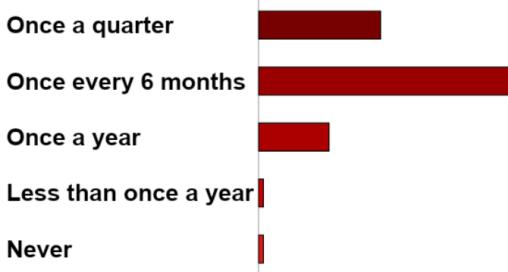


SALT

Survey of 300 CISOs & CSOs  
Published June 2023

## Digitization CISO Challenges

57% give a cyber presentation every 6 months

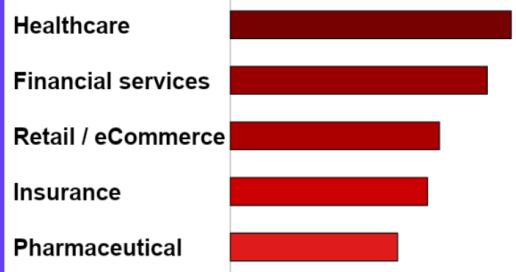


SALT

Survey of 300 CISOs & CSOs  
Published June 2023

## Digitization CISO Challenges

Healthcare gives cyber presentation every 3 months

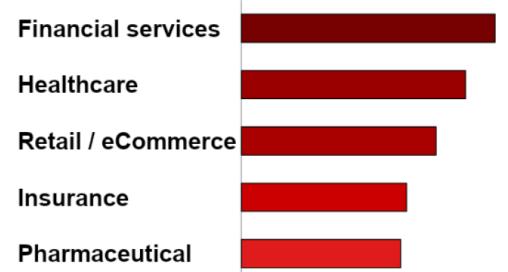


SALT

Survey of 300 CISOs & CSOs  
Published June 2023

## Digitization CISO Challenges

43% say finance has difficulty justifying security cost



SALT

Survey of 300 CISOs & CSOs  
Published June 2023

# Cyber Insights: Ransomware Insights

Click each image to see each report in full. All were published in June 2023

### Ransomware Gangs

LockBit3 increased its victim count with 385

LockBit3	385
BlackCat	190
Black Basta	169
ViceSociety	87
Royal	51

**Orange Cyberdefense**

> 6,500 Extorted Firms  
Published June 2023

### Ransom Victims per Gang

30% of all publicised victims listed by LockBit 3.0

LockBit	30%
Hive	22%
Clop	12%
Royal	7%
ALPHV	5%

**Trellix**

Published June 2023

### Ransomware Groups

855 of reported Ransomware cases are by LockBit

Lockbit	855
Conti	796
Pysa	311
Revil	284
Maze	264

**NordLocker**

Analysis of 1 year of ransomware  
Published June 2023

### Ransomware Victims

48% of publicised Ransom Victims now in the USA

India	4%
Canada	4%
Germany	4%
UK	8%
USA	48%

**Trellix**

Published June 2023

### Sectors Affected by Ransom

25% of Attacked firms are in Industrial Sectors

Industrial Goods	25%
Retail	14%
Technology	11%
Health	8%
Financial Services	6%

**Trellix**

Published June 2023

### Ransomware Threat Level

32% believe that they are Very Likely to be a target

Not at all	4%
Extremely Likely	16%
Slightly Likely	17%
Moderately Likely	31%
Very Likely	32%

**BULLWALL**

Survey of 453 Cyber Pros  
Published May 2023

### Ransomware Risk Index

Firms in USA are targeted much more than in India

India	0.3
Brazil	0.6
France	0.9
UK	0.9
USA	1

**NordLocker**

Analysis of 1 year of ransomware  
Published June 2023

### Ransom Payments Decrease

Size of each known payment -20% from Q4/22

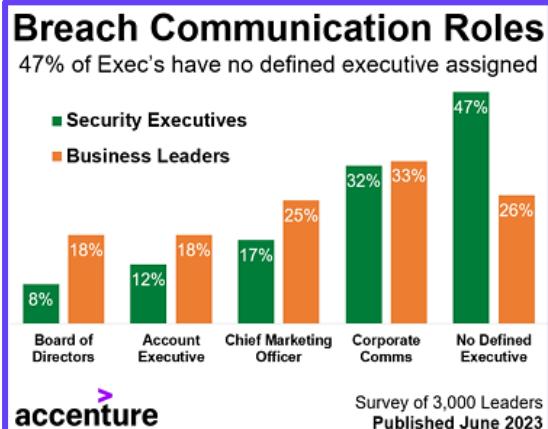
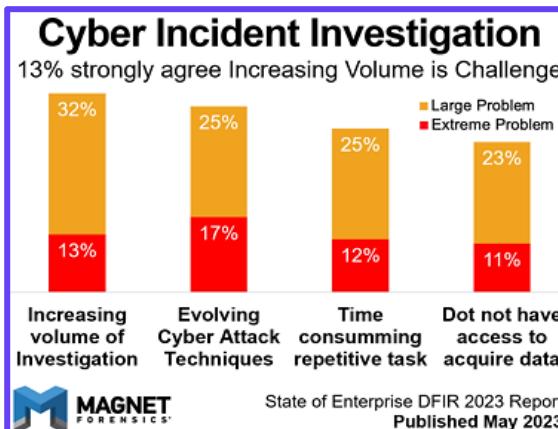
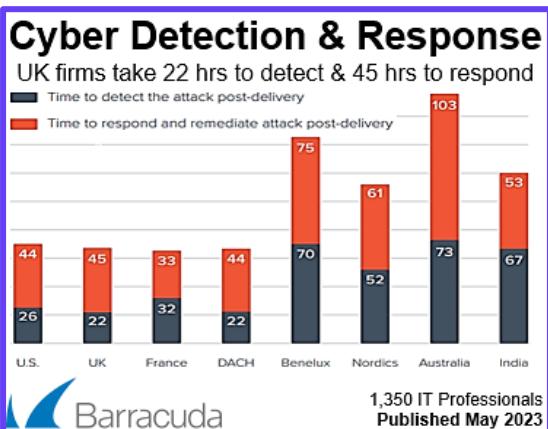
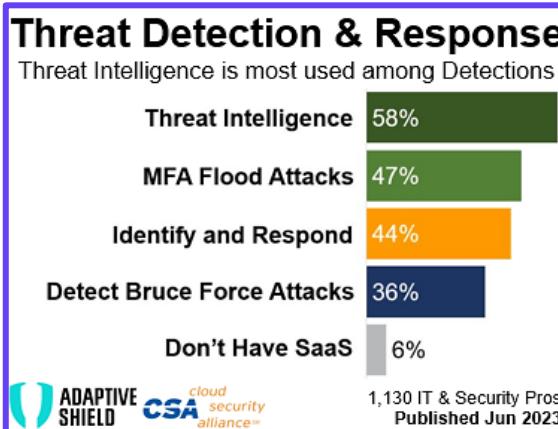
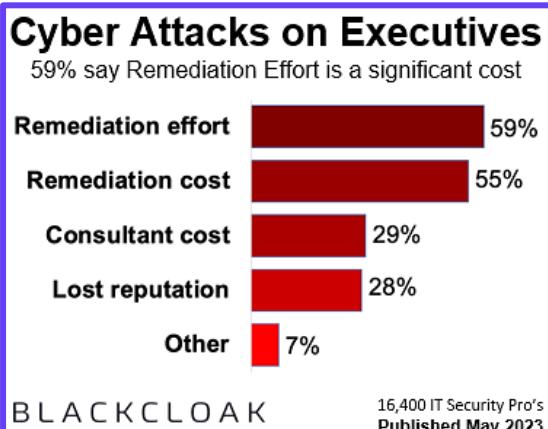
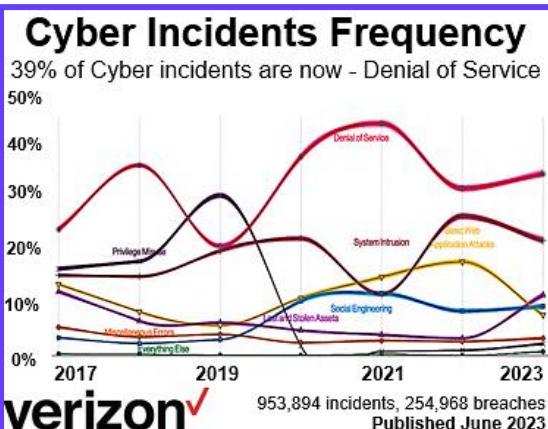
Average known Payout = **USD \$327,883**

**BLACKFOG**  
Privacy. Security. Prevention.

Published June 2023

# Cyber Insights: *Incident Management*

Click each image to see each report in full. All were published in June 2023



# Cyber Insights: Cyber Risk Management

Click each image to see each report in full. All were published in June 2023

## Emerging Risks for Firms

Cloud Concentration & 3<sup>rd</sup> Party Viability at Top

**Attention from Firms**

**Level of Risk**

**Gartner** 321 Risk Mngrs. Published May 2023

## Risk Management Cycle

4 stages: Risk, Relationship, Vulnerabilities, Quality

**enisa** Survey of over 1,081 Organisations Published June 2023

## Cyber Risk Management

48% only implement controls for critical functions

- Deploy security after transformation is initialized if vulnerabilities are detected
- Implement security controls, balancing speed and risk management
- Embed security controls in all transformation Initiatives from the beginning.

**accenture** Survey of 3,000 Leaders Published June 2023

## Vulnerability Management

22% of firms implement vulnerability management

- Yes, but only for internet-facing assets
- Yes, but only for critical IT-assets
- Partially, but we plan to cover all internal and external assets
- No, but we plan to implement a vulnerability management process

**enisa** Survey of over 1,081 Organisations Published June 2023

## Mitigating Cyber Threats

42% say MFA is the most important technology

Technology	Percentage
Multi-factor Authentication	42.3%
Endpoint Detection & Response	41.8%
Email Encryption	36.2%
Risked-based Authentication	32.5%
Network Segmentation	28.7%

**CYBEREDGE GROUP** Survey of 1,200 Security Pros Source: 2023 Cyberthreat Defense Report, CyberEdge Group, LLC

## Cyber Change Makers

Top operational practices for strong cybersecurity

- #1 = **Excel** at integrating cybersecurity
- #2 = **Leverage** cybersecurity as-a-service
- #3 = **More Commitment** to protect
- #4 = **Rely** more on automation

**accenture** Survey of 3,000 Leaders Published June 2023

## Achieving Cyber Resilience

33% of firms have confidence in their capability

Aspect	Percentage
importance of knowing workforce can recover from incident	69%
effectiveness at knowing	58%
confidence in capability to recover incident	33%

**OSTERMAN RESEARCH** **IMMERSIVE LABS** 570 Senior Security Pro's Published June 2023

## Cyber & Firm Resilience

How Cyber Drives Resilience

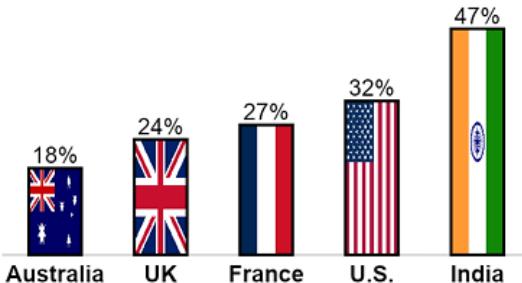
**accenture** Published June 2023

# Cyber Insights: AI Cyber Security

Click each image to see each report in full. All were published in June 2023

## Cyber & AI Voice Scams

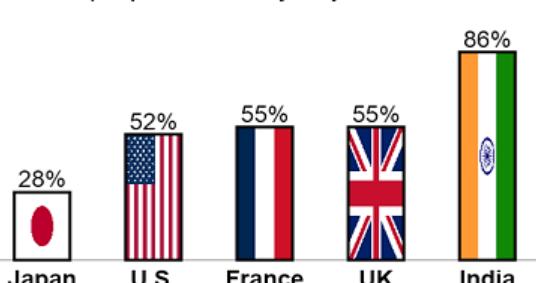
47% of respondents in India experienced AI scams



Survey of 7,000 adults  
Published May 2023

## Cyber & AI Voice Scams

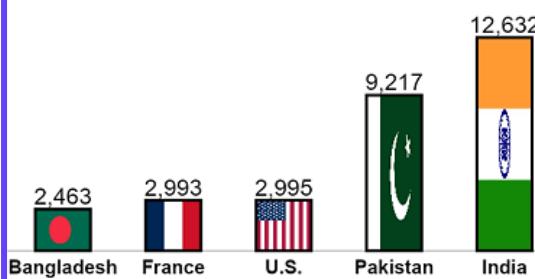
86% of people in India say they share their voice



Survey of 7,000 adults  
Published May 2023

## Cyber Security & ChatGPT

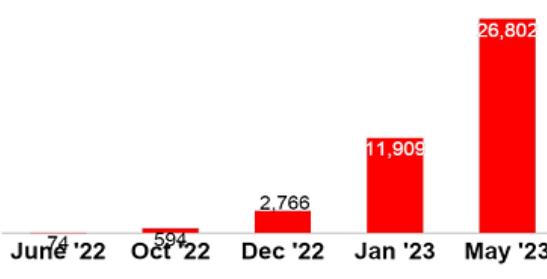
12,632 compromised ChatGPT accounts in India



Published June 2023

## Cyber Security & ChatGPT

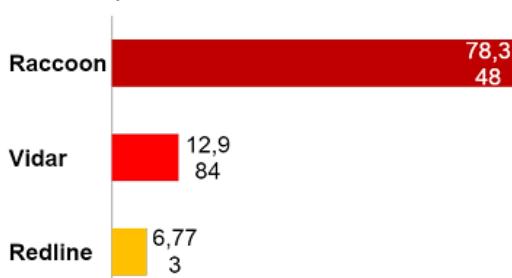
26,802 compromised ChatGPT accounts last month



Includes ChatGPT v1, v2, v3 & v4  
Published June 2023

## Cyber Security & ChatGPT

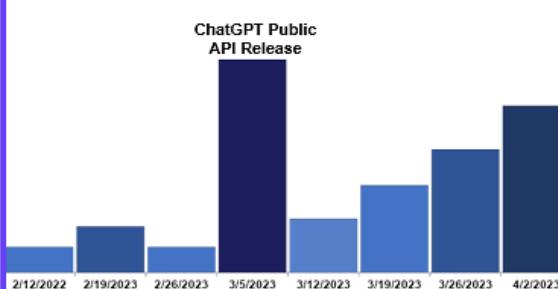
78K compromised ChatGPT hosts on Raccoon



Published June 2023

## Cyber Threats from AI

New “Grayware” accelerated when GPT published



paloalto NETWORKS  
Analysis of 40 data types from different regions  
Published June 2023

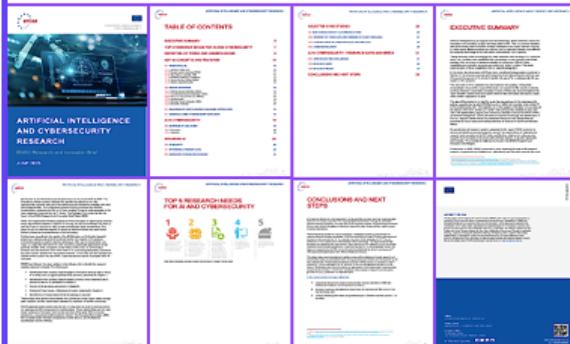
## Cybersecurity for AI ENISA framework

Published Jun '23



## AI & Cybersecurity ENISA Research & Innovation Brief

Published Jun '23

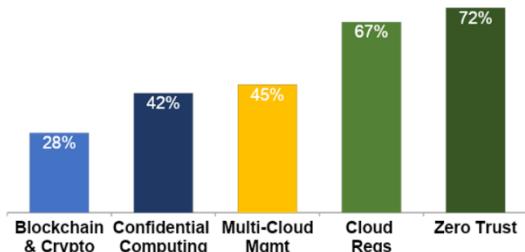


# Cyber Insights: Cloud Security

Click each image to see each report in full. All were published in June 2023

## Cloud Security Priorities

72% of CISOs focus on Zero Trust for Cloud Security



Interviews with CISOs & CROs  
Published June 2023

## Cloud Security Practices

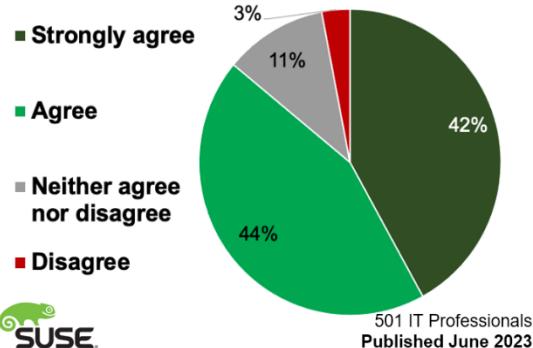
38% use Security Automation as a Security Practice



501 IT Professionals  
Published June 2023

## Cloud Security Skills

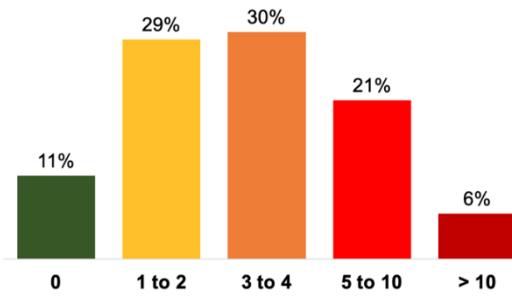
86% say their team can detect & fix gaps in Cloud



501 IT Professionals  
Published June 2023

## Cloud Security Incidents

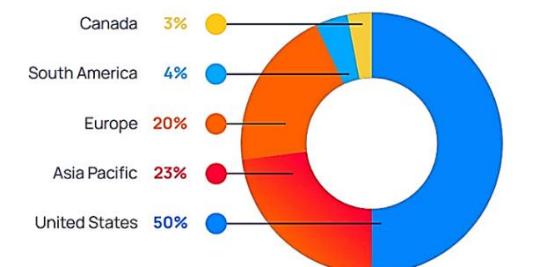
30% of Firms had 3 to 4 Cloud Incidents in past year



501 IT Professionals  
Published June 2023

## Attacks using AWS Keys

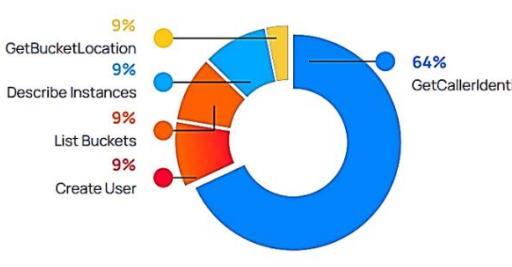
50% of AWS Key Exploitation is observed from USA



Data from Honeypot set up by Orca  
Published June 2023

## Attacks using AWS Keys

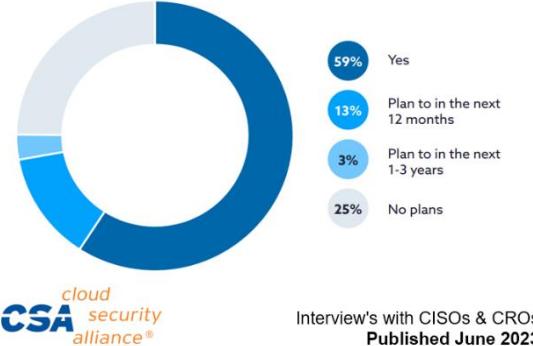
64% of observed attacks used "GetCallerIdentity"



Data from Honeypot set up by Orca  
Published June 2023

## Cloud Service Process

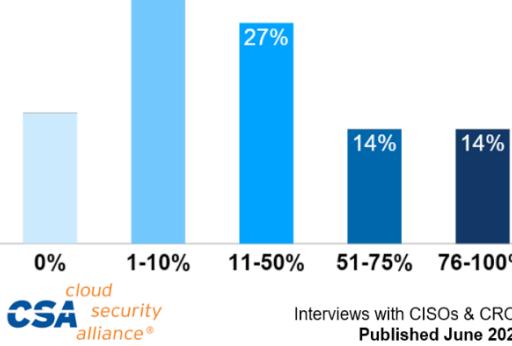
59% of Banks use cloud computing for their Data



Interview's with CISOs & CROs  
Published June 2023

## Public Cloud in Finance Orgs

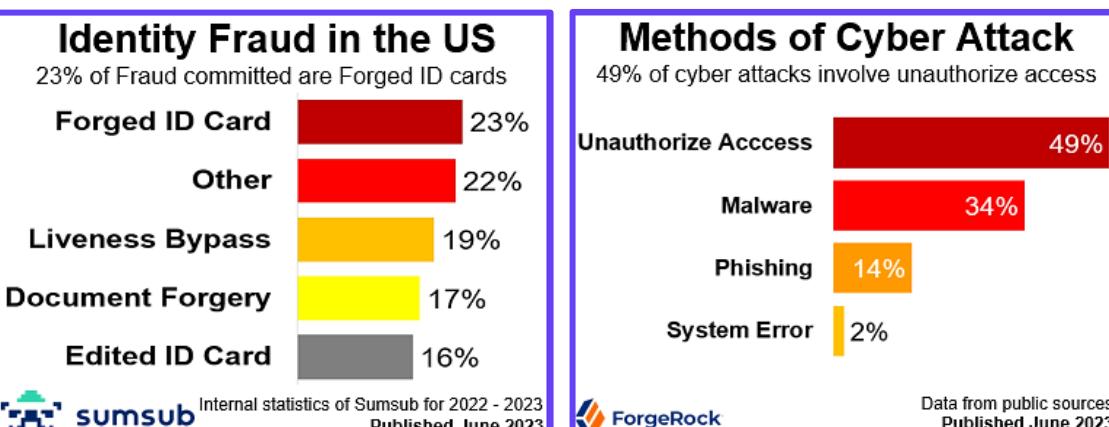
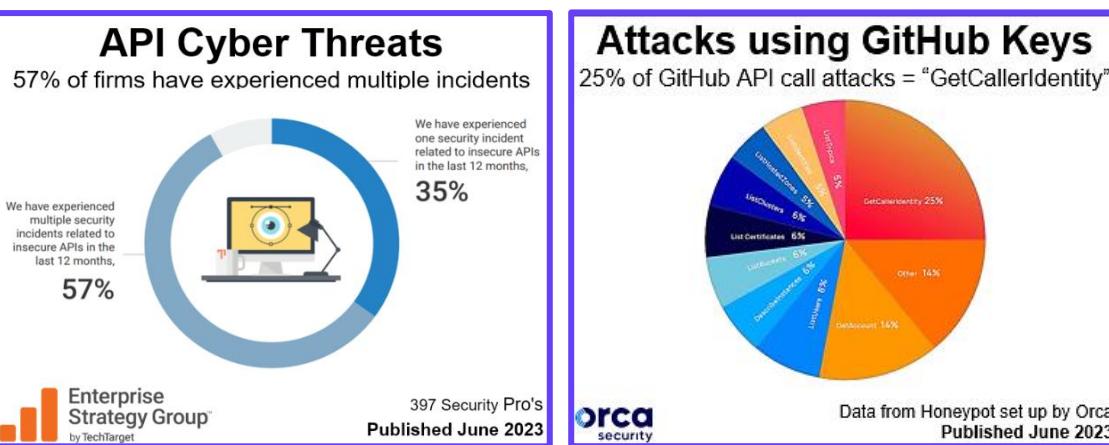
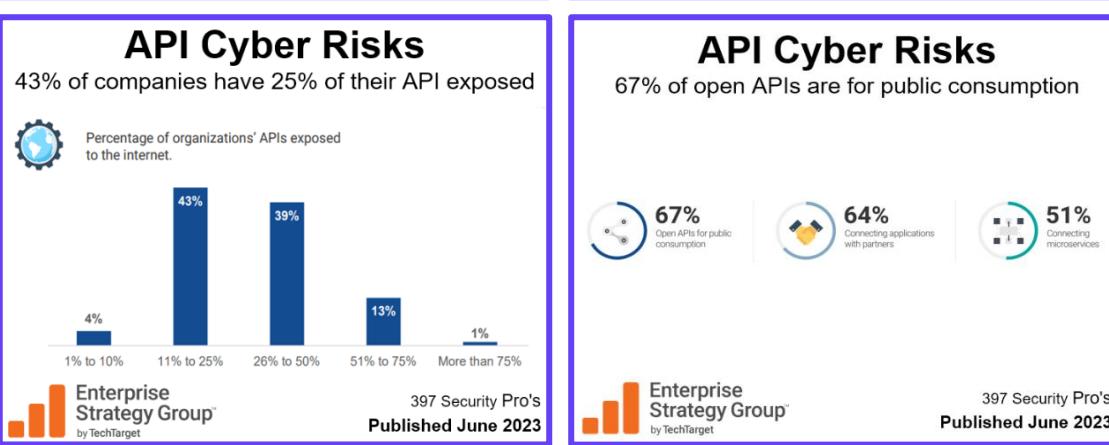
28% use Public Cloud for >50% of regulated work



Interviews with CISOs & CROs  
Published June 2023

# Cyber Insights: Software & API Security

Click each image to see each report in full. All were published in June 2023



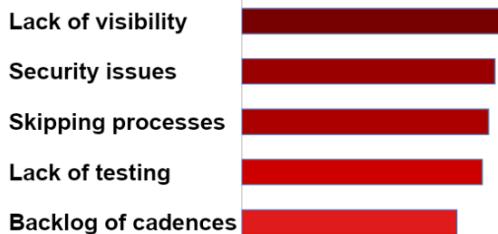


# Cyber Insights: Cyber Security Flaws

Click each image to see each report in full. All were published in June 2023

## Fast Development Risks

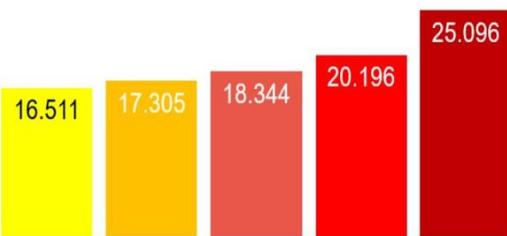
Lack of visibility is the biggest challenge at 41%



397 Security Pro's  
Published June 2023

## New Cyber vulnerabilities

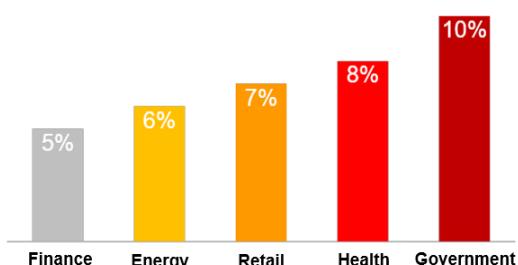
25,096 new vulnerabilities published in 2022



> 150,000 vulnerabilities & > 15,000 products  
Published June 2023

## Cyber Vulnerabilities

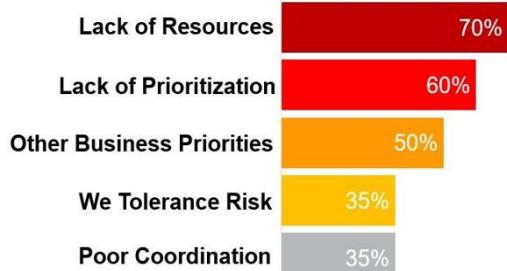
10% of unpatched issues in Gov are High or Critical



Published May 2023

## Cyber Vulnerabilities

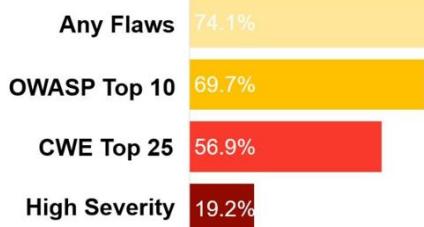
70% of firms say "Lack of Staff" slows remediation



Published May 2023

## Cybersecurity Flaws

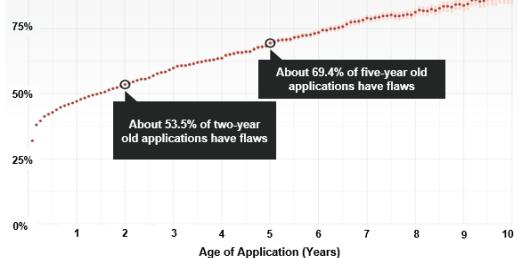
74% of Apps have a security Flaws



> 28,000,000 Scans  
Published Jun 2023

## Software and its Flaws

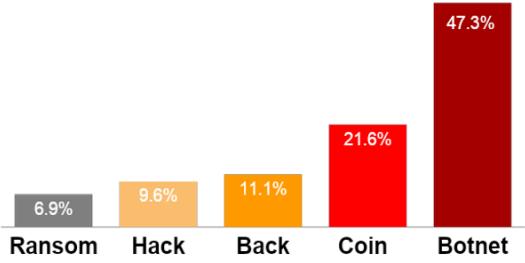
69.4% of 5-year old Apps have 1 and more Flaws



> 28,000,000 Scans  
Published Jun 2023

## Cyber Risk in Linux Systems

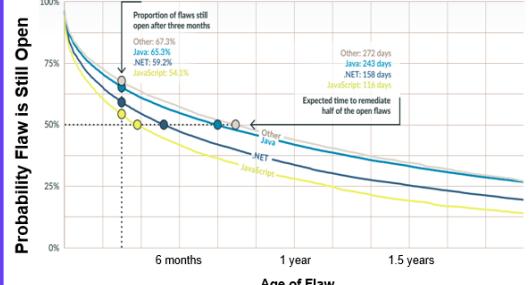
47.3% of threat against Linux systems is Botnets



Analysis of 40 data types from different regions  
Published June 2023

## Remediation Timeline

A Flaw is Open after 3 months with Java at 65.3%



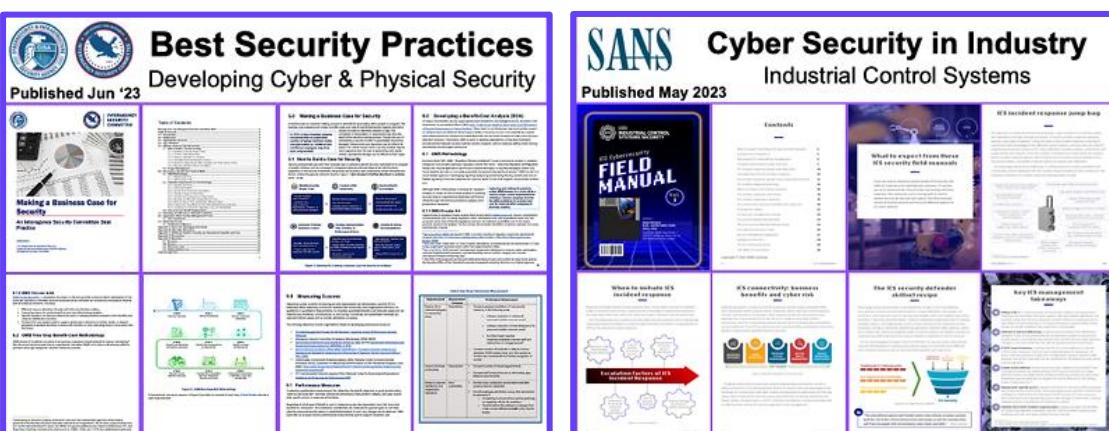
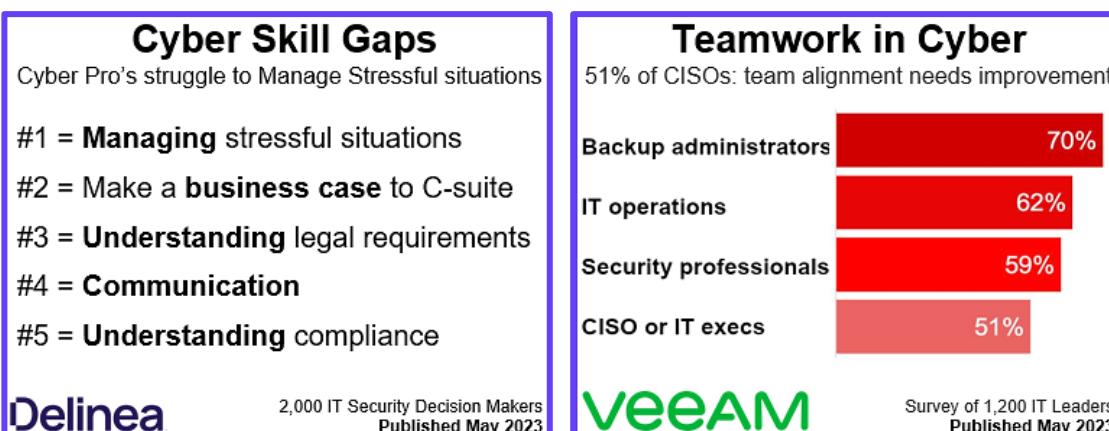
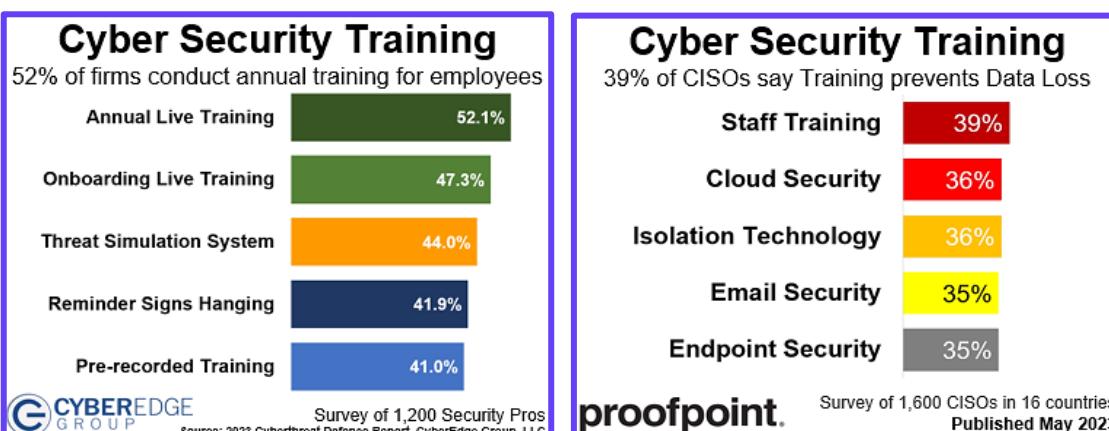
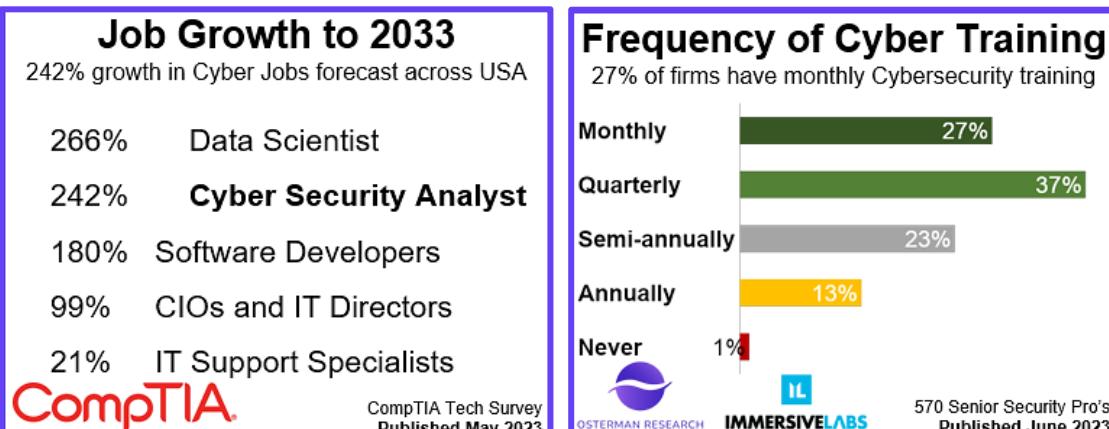
> 28,000,000 Scans  
Published Jun 2023





# Cyber Insights: Cyber Skills

Click each image to see each report in full. All were published in month to June 2023



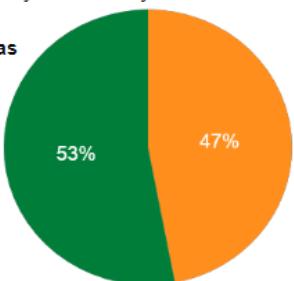
# Cyber Insights: Best Practices

Click each image to see each report in full. All were published in month to June 2023

## Cybersecurity Planning

53% of the firms include cybersecurity from the start

- Include cybersecurity as part of the core transformation team
- Use cybersecurity halfway through the project



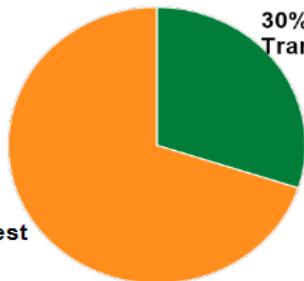
> accenture

Survey of 3,000 Leaders  
Published June 2023

## Cyber Digital Transformation

30% of Firms are Accelerating Cybersecurity Efforts

30% Cyber Transformers



> accenture

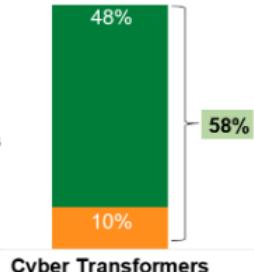
Survey of 3,000 Leaders  
Published June 2023

## Cybersecurity Foundation

58% more likely to have an effective transformation

- Apply strong cybersecurity operational practices
- Embedded cybersecurity into transformation efforts

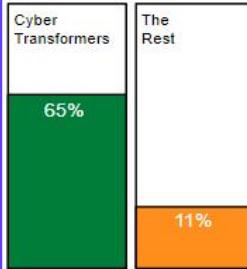
10%  
The rest



Survey of 3,000 Leaders  
Published June 2023

## Leading Cyber Practices

65% of cyber experts use these 3 practices to excel



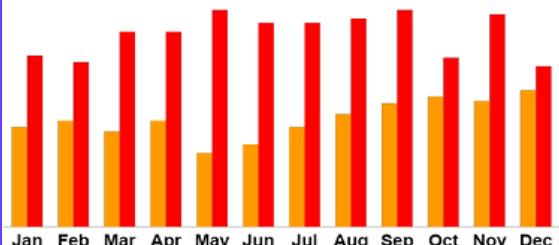
- ① **Integrate cyber risk:** A cyber risk-based framework is completely integrated into their enterprise risk management program.
- ② **Agree on priorities:** Their cybersecurity operations and executive leadership consistently agree on the priority of assets and operations to protect.
- ③ **Look at risk holistically:** They consider cybersecurity risk to a great extent when evaluating overall enterprise risk.

Survey of 3,000 Leaders  
Published June 2023

## Cyber Attacks on Industry

238% increase in attacks compared to previous year

■ 2021 ■ 2022



paloalto

Analysis of 40 data types from different regions  
Published June 2023

## Most Secure Finance Firms

Western Alliance "most Cyber Secure Finance firm USA"

- #1 = Western Alliance Bank
- #2 = Pacific Western Bank
- #3 = Houlihan Lokey
- #4 = New American Funding
- #5 = Fidelity Investments

Security Scorecard

Forbes

Forbes & Security Scorecard  
Published June 2023

## Most Secure Tech Firms

Intel rated "most Cyber Secure Tech firm in USA"

- #1 = Intel
- #2 = Lam Research
- #3 = Micron
- #4 = Broadcom
- #5 = Aretec

Security Scorecard

Forbes

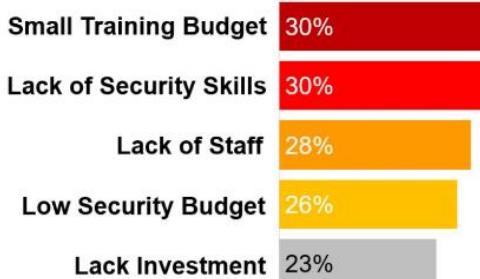
Forbes & Security Scorecard  
Published June 2023

# Cyber Insights: Cyber Challenges

Click each image to see each report in full. All were published in month to June 2023

## Cyber Security Challenges

30% say Inadequate Training Budget is a Challenge



402 cybersecurity decision makers  
Published June 2023

## Cyber Security Priorities

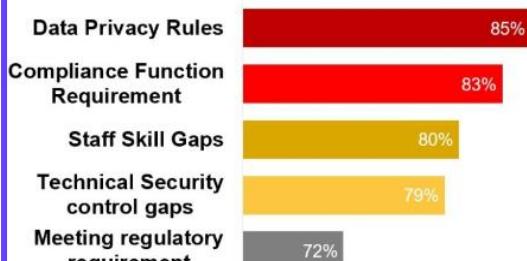
52% say Additional Staff is a top priority in Budget



402 cybersecurity decision makers  
Published June 2023

## Cyber Security Blockers

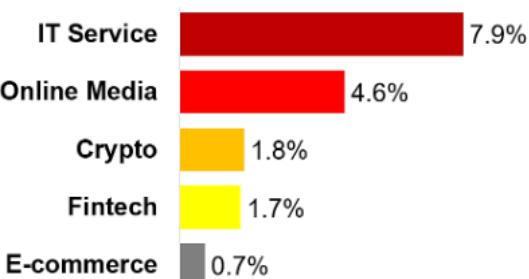
Data Privacy is among the most challenging



Interview's with CISOs & CROs  
Published June 2023

## Fraud-affected Businesses

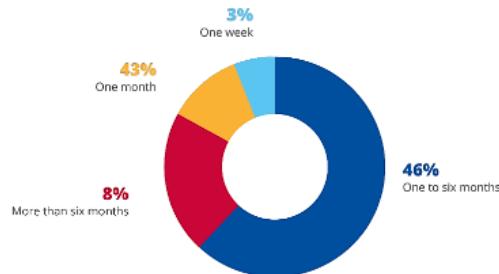
7.9% of Fraud-affected Businesses are IT Services



Internal statistics of Sumsup for 2022 - 2023  
Published June 2023

## Vulnerability Patching

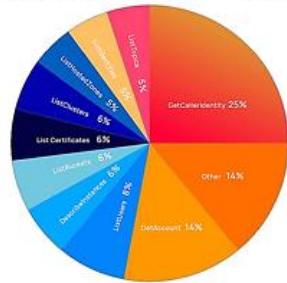
46% of the firms take 1 to 6 months to patch



Survey of over 1,081 Organisations  
Published June 2023

## Attacks using GitHub Keys

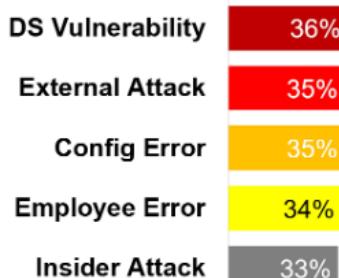
25% of GitHub API call attacks = "GetCallerIdentity"



Data from Honeypot set up by Orca  
Published June 2023

## Cause of Data Loss

36% of CISOs say that DS Vulnerability caused loss



Survey of 1,600 CISOs in 16 countries  
Published May 2023

## Personal Info in Breaches

Name is most common info found in breach records

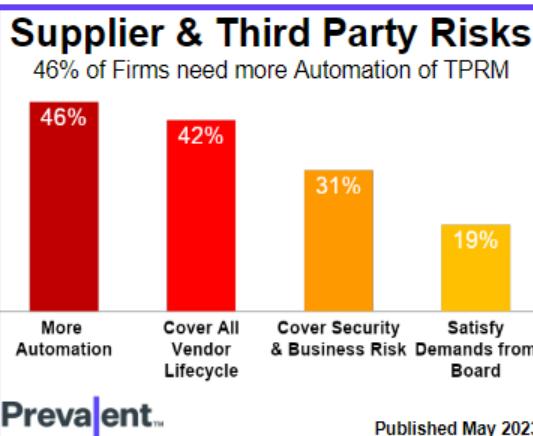
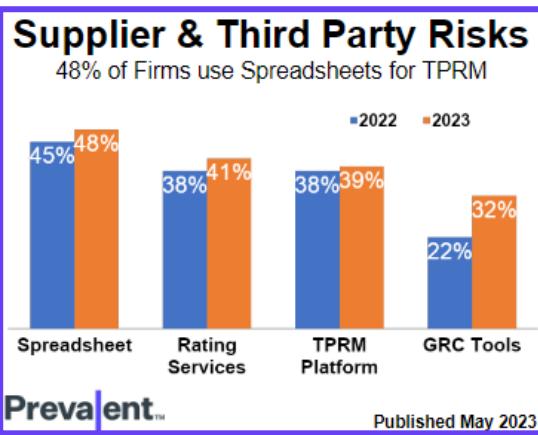
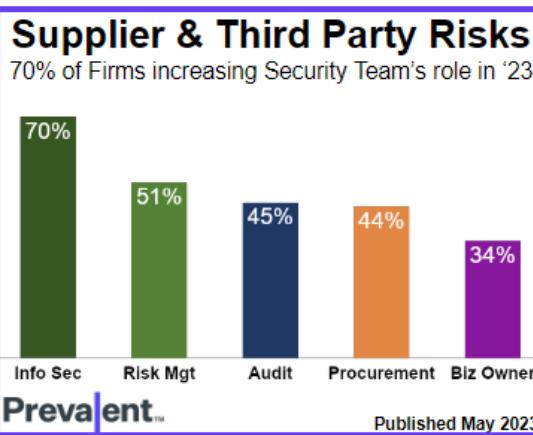
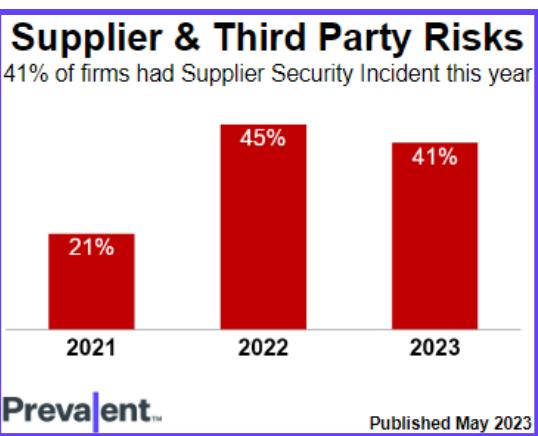
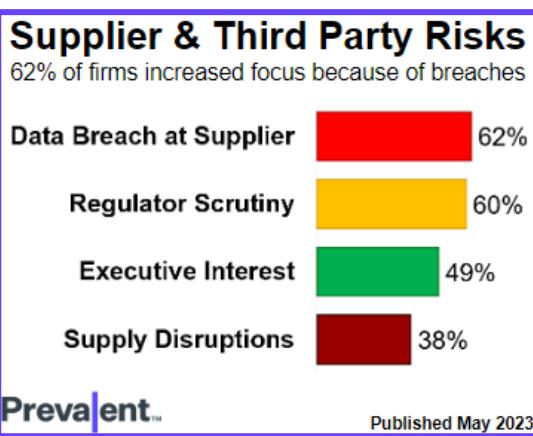
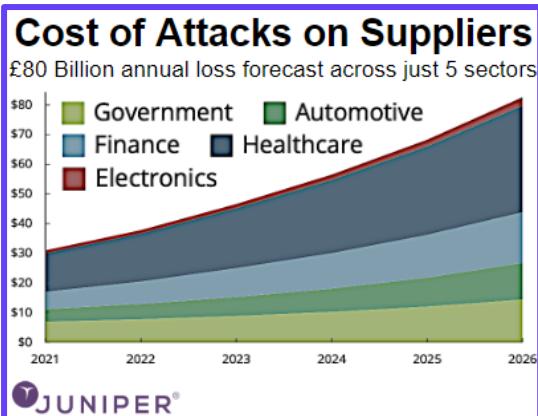
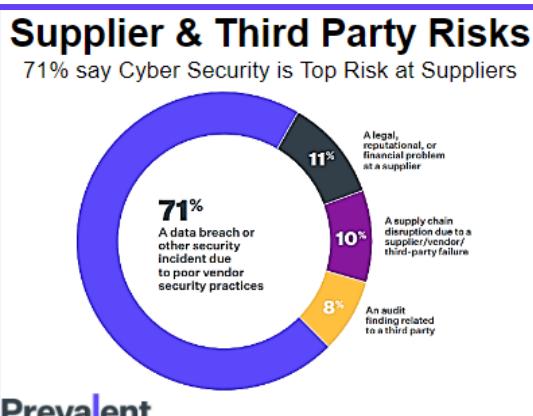
- #1 = Name & Address
- #2 = Social Security Number
- #3 = Protected Health Information
- #4 = Log-in Credentials
- #5 = Credit Card Information



Data from public sources  
Published June 2023

# Cyber Insights: Supplier & 3rd Party Risk

Click each image to see each report in full. All were published in month to March 2023



# Cyber Insights: Cyber Insurance

Click each image to see each report in full. All were published in month to March 2023

### Cyber Insurance Adoption

96% of Higher Education industry have insurance

Higher Education	96%
Financial Industry	95%
Oil & Gas	95%
Media & Leisure	90%
IT Industry	82%

**SOPHOS**

Survey of 3,000 Cyber leaders  
Published May 2023

### Cyber Insurance & Ransoms

81% of Ransomed Firms had to strengthen their defences before they could get new cyber insurance

81%
59%
16%

said that the quality of their defenses impacted their ability to get coverage

said that the quality of their defenses impacted the cost of their coverage

said that the quality of their defenses impacted the terms of their policy

**SOPHOS**

Survey of 3,000 Cyber leaders  
Published May 2023

### Cyber Insurance Adoption

98% of firms in South Africa say they are insured

UK	84%
Brazil	86%
Italy	87%
U.S.	95%
South Africa	98%

**SOPHOS**

Survey of 3,000 Cyber leaders  
Published May 2023

### Cyber Insurance Adoption

96% of largest firms say they're insured for cyber

\$5 billion plus	96%
\$1 billion - \$5 billion	93%
\$250 - \$500 million	92%
\$50 - \$250 million	91%
\$10 - \$50 million	79%

**SOPHOS**

Survey of 3,000 Cyber leaders  
Published May 2023

### Cyber Insurance Adoption

62% of well-defended firms: Insurance is Cheaper

Cheaper to buy	62%
Easier to buy	60%
Sold with better terms	28%

**SOPHOS**

Survey of 3,000 Cyber leaders  
Published May 2023

### Cyber Insurance Prices

10% price rise in UK in Q1, down from 34% in Q4

Region	Q4 (%)	Q1 (%)
ASIA	22%	8%
EU	13%	5%
LATAM	33%	15%
UK	34%	10%
USA	28%	11%

**Marsh**

Global Insurance Market Index  
Published April 2023

### Cyber Insurance Demand

\$33.3 Billion forecast for 2027, (up 179% in 5 years)

Year	USD*
2019	5.8 bn USD*
2022	11.9 bn USD*
2025	22.5 bn USD*
2027	33.3 bn USD*

Munich RE

Cyber Insurance Risk Trends Report  
Published 26<sup>th</sup> April 2023

### Cyber Insurance & Ransoms

58% of firms with Standalone Insurance paid ransom

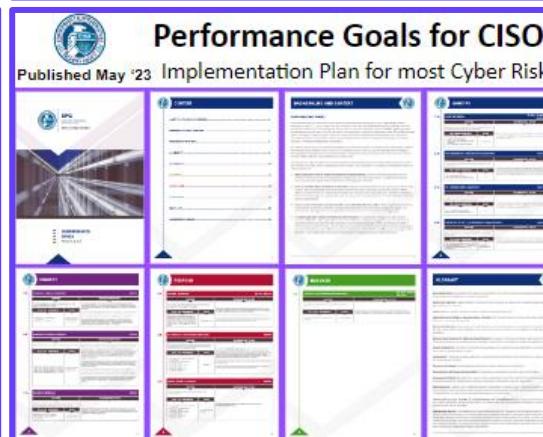
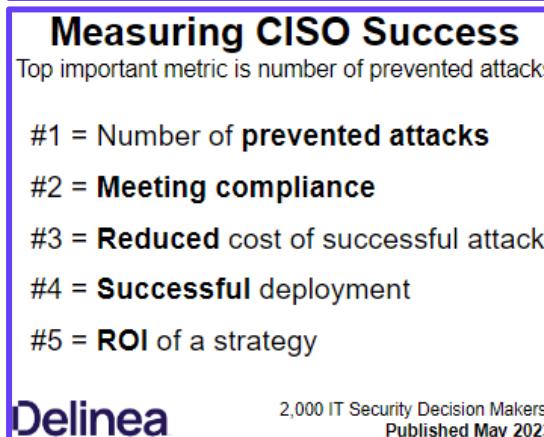
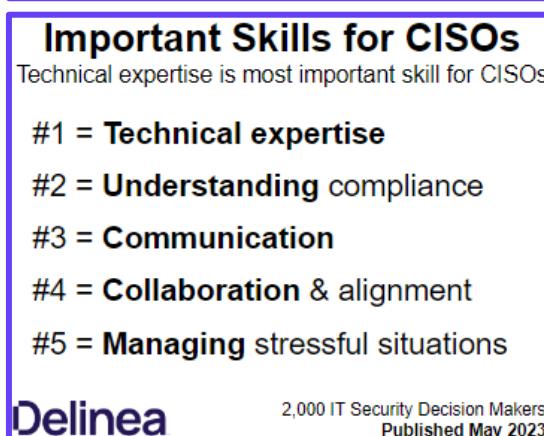
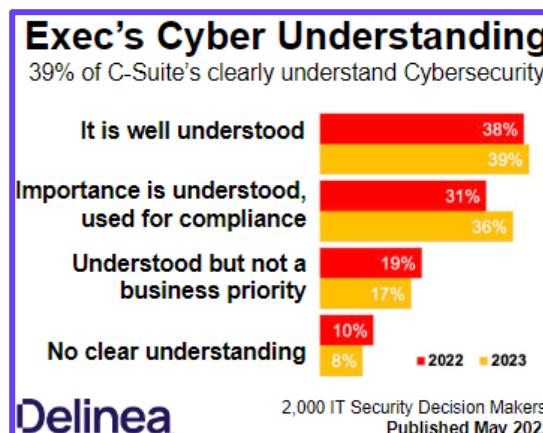
Standalone cyber insurance	58%
Wider insurance	36%
No cyber insurance	15%

**SOPHOS**

Survey of 3,000 Cyber leaders  
Published May 2023

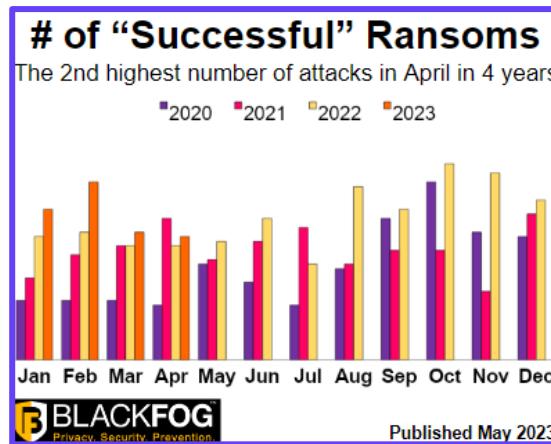
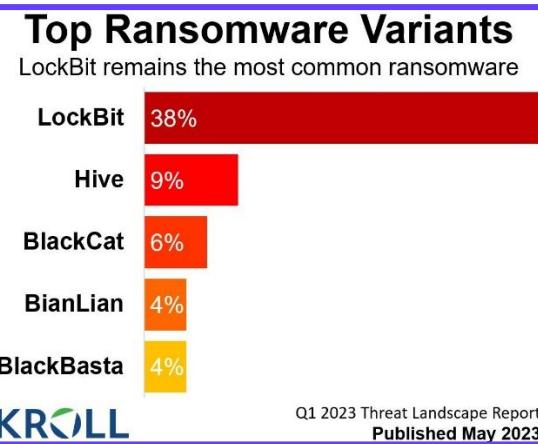
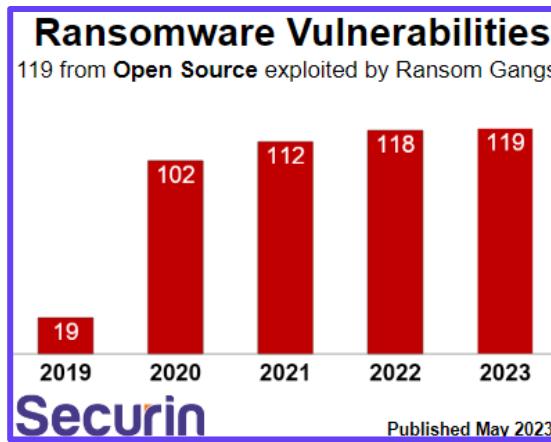
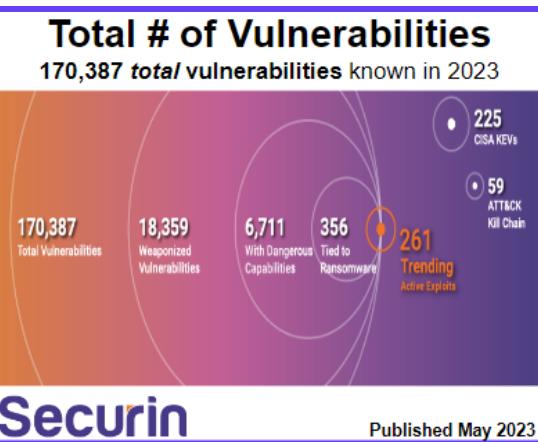
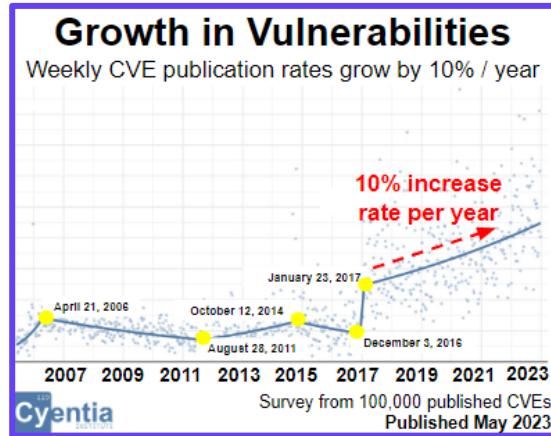
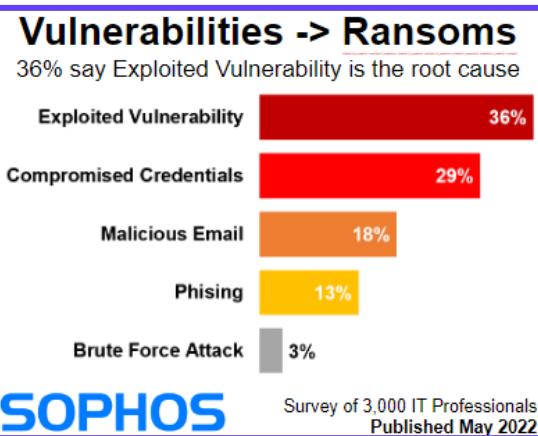
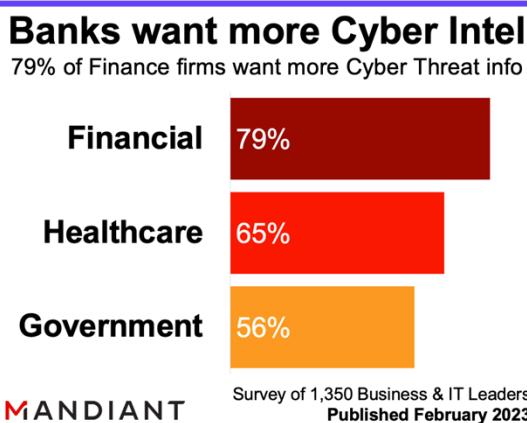
# Cyber Insights: Success for CISOs

Click each image to see each report in full. All were published in month to March 2023



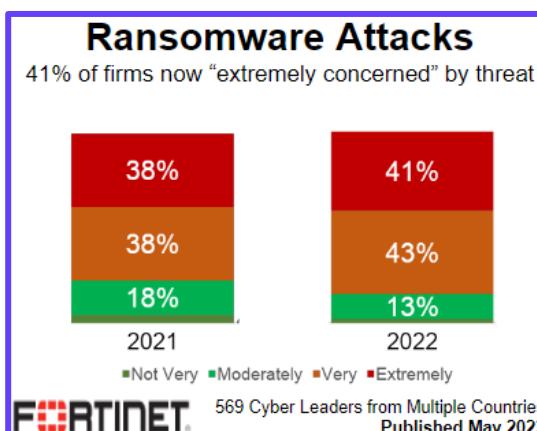
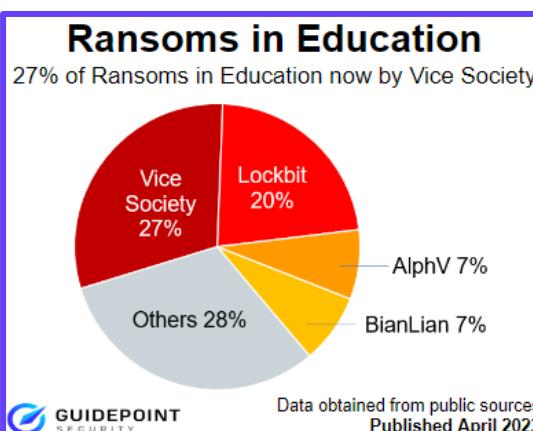
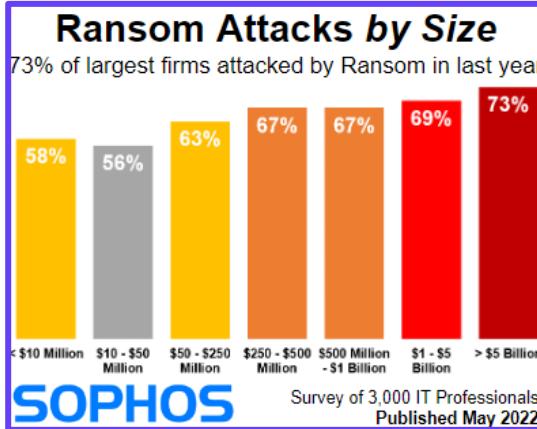
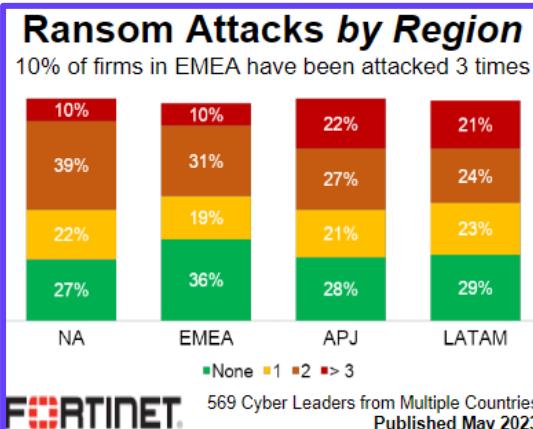
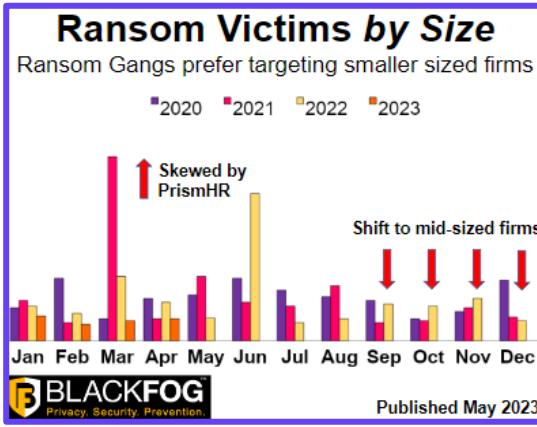
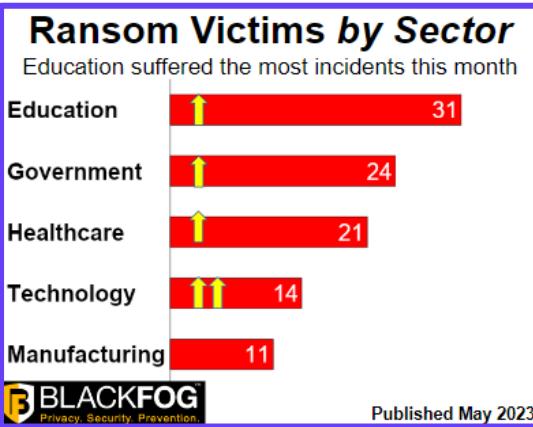
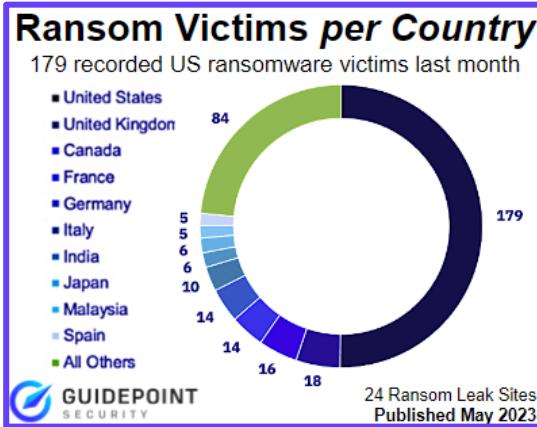
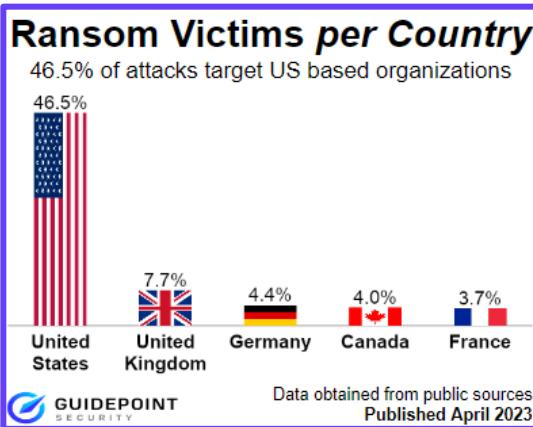
# Cyber Insights: Ransomware Vulnerabilities

Click each image to see each report in full. All were published in month to March 2023



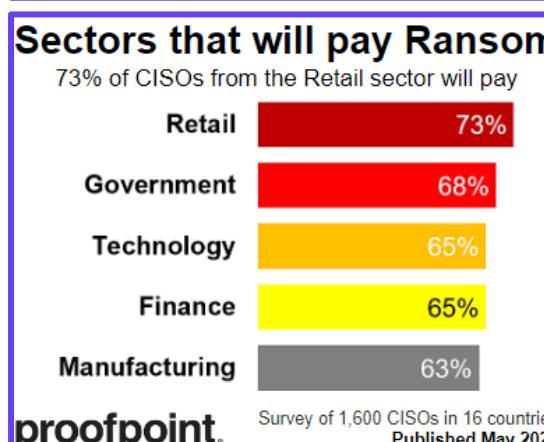
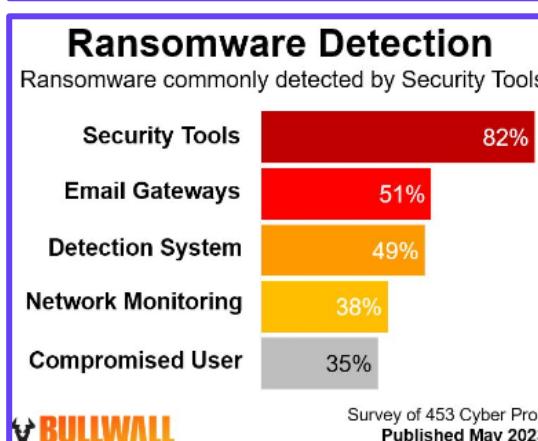
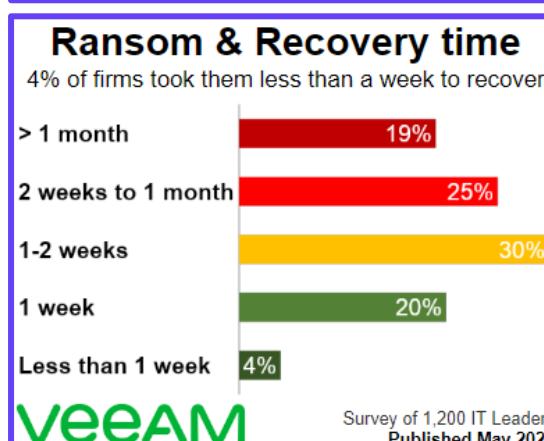
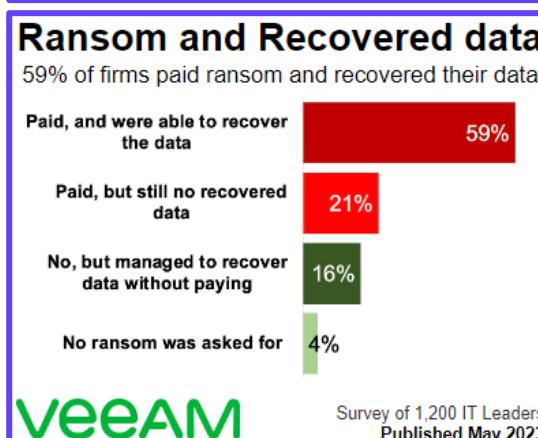
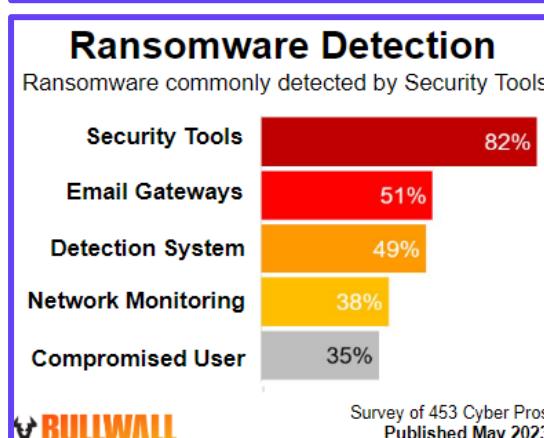
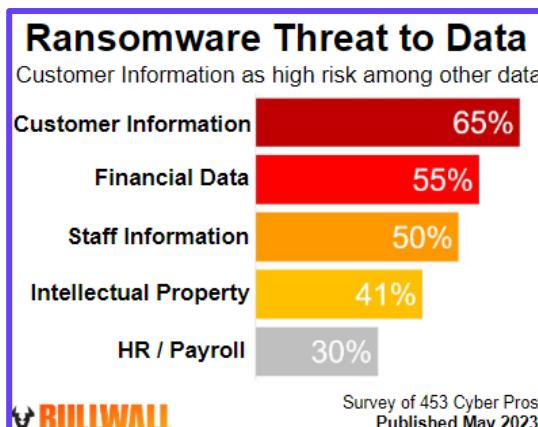
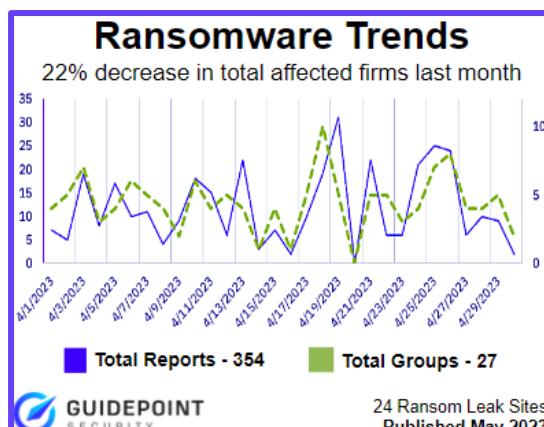
# Cyber Insights: Ransomware Victims

Click each image to see each report in full. All were published in month to March 2023



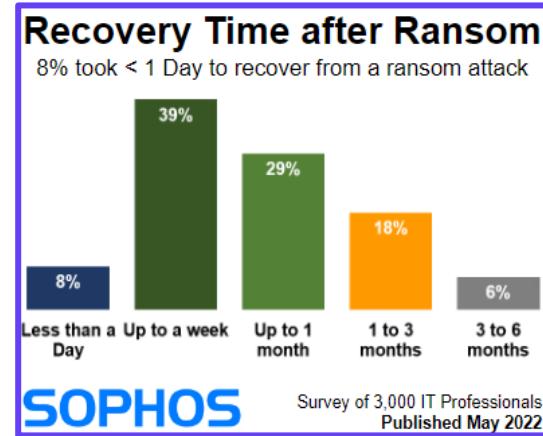
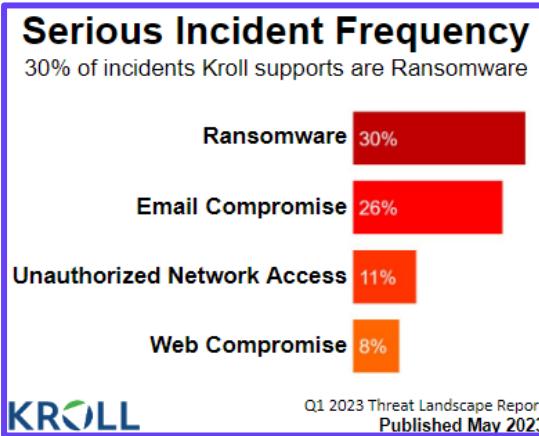
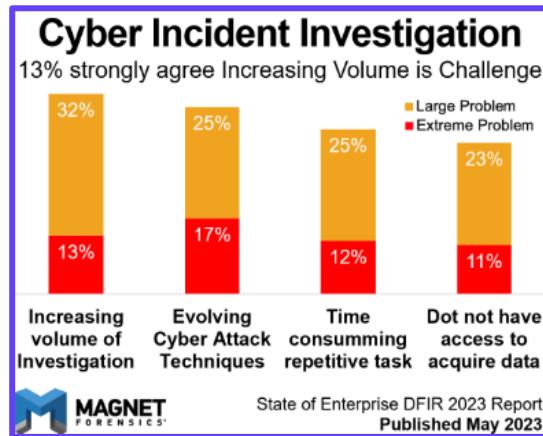
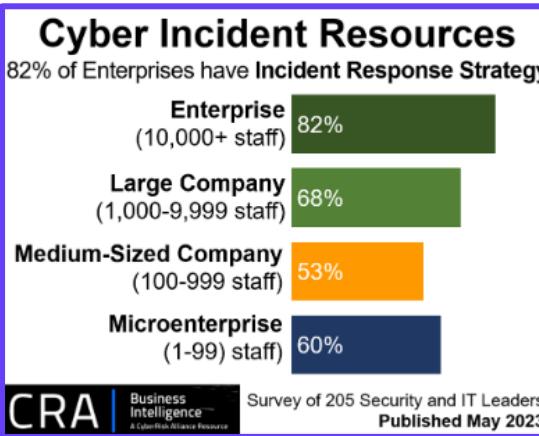
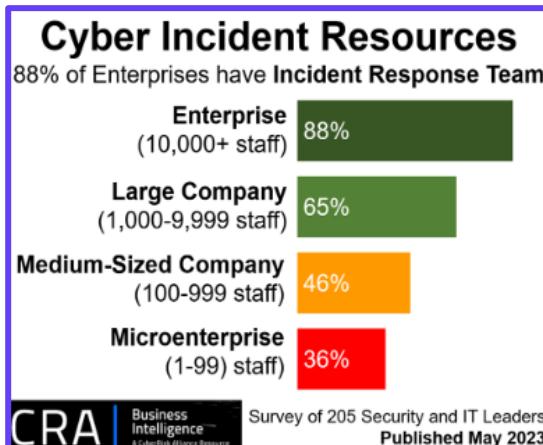
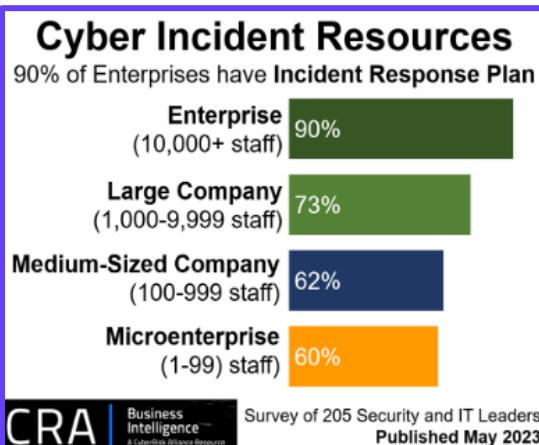
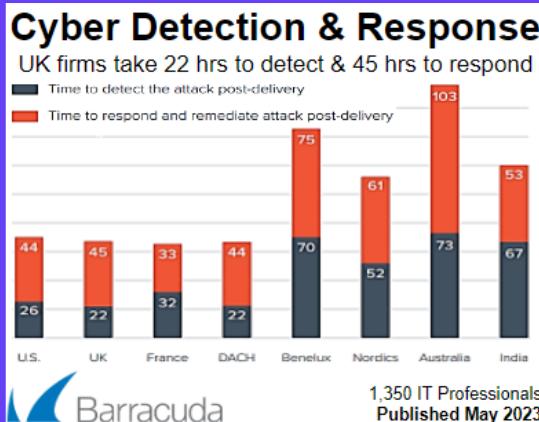
# Cyber Insights: Ransomware Insights

Click each image to see each report in full. All were published in month to March 2023



# Cyber Insights: *Incident Response*

Click each image to see each report in full. All were published in month to March 2023



# Cyber Insights: Email Threats

Click each image to see each report in full. All were published in month to March 2023

### Email attacks by Country

15 suspicious emails reported daily to IT in India

Country	Attacks
India	15
France	11
UK	11
U.S.	9
Australia	7

1,350 IT Professionals  
Published May 2023

Barracuda

### Email Attacks by Firm Size

5 social engineering attacks / mailbox in big firms

Firm Size	Attacks
0 - 100	17
100 - 500	13
500 - 2,000	11
> 2,000	5

1,350 IT Professionals  
Published May 2023

Barracuda

### Spear Phishing Emails

75% of Firms have been hit by Spear Phishing

Response	Percentage
No	25%
Yes	75%

1,350 IT Professionals  
Published May 2023

Barracuda

### Spear Phishing Emails

Spear phishing often leads to infected machines

- #1 = Machines Infected with viruses
- #2 = Sensitive Data Stolen
- #3 = Stolen log-in credentials
- #4 = Direct Monetary Loss
- #5 = Reputation Damage

1,350 IT Professionals  
Published May 2023

Barracuda

### Credential Phishing Emails

1.5% rise in Credential Phishing email attack volume

Year	Known credential phishing links	Unknown credential phishing links
2021	2,279,840	3,942,466
2022	2,328,400	3,965,601

Known credential phishing links  
Unknown credential phishing links

TREND MICRO™  
Scan of > 79 Billion emails  
Published May 2023

### Business Email Compromise

Lures (eg, 'update to Teams service') dominate BEC

Type	Percentage
Lure	62.35%
Business Information	4%
Gift Card	4.87%
Invoice	8.29%
Payroll	14.87%

BEC Attacks on Microsoft Users  
Published May 2023

Microsoft

### Malware attached to Emails

46% rise in unknown (new) malware is a challenge

Year	Known Malware	Unknown Malware
2021	747,866	2,567,642
2022	505,838	3,757,812

Known Malware  
Unknown Malware

TREND MICRO™  
Scan of > 79 Billion emails  
Published May 2023

### Cyber Threat Access Method

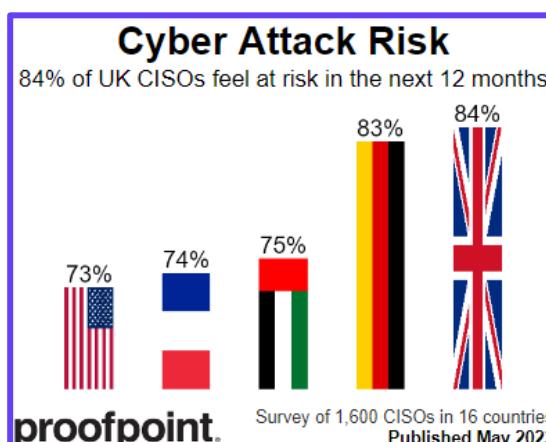
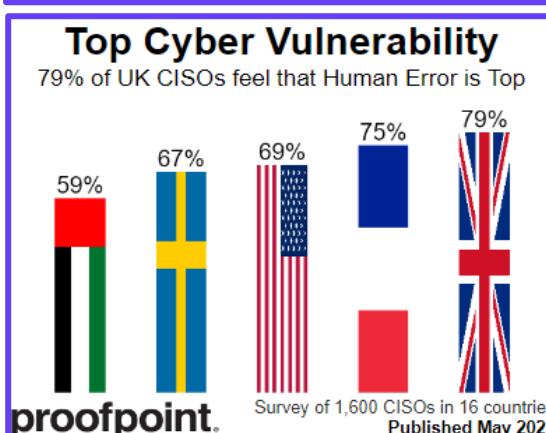
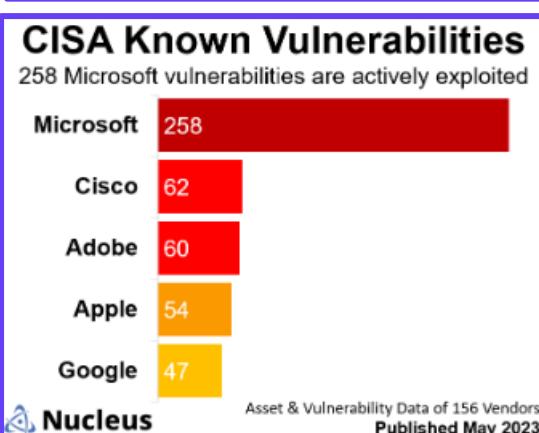
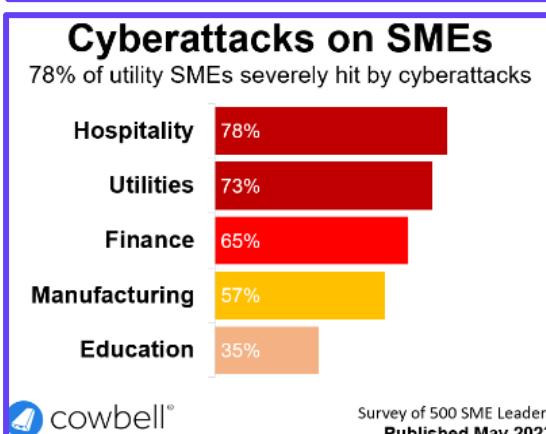
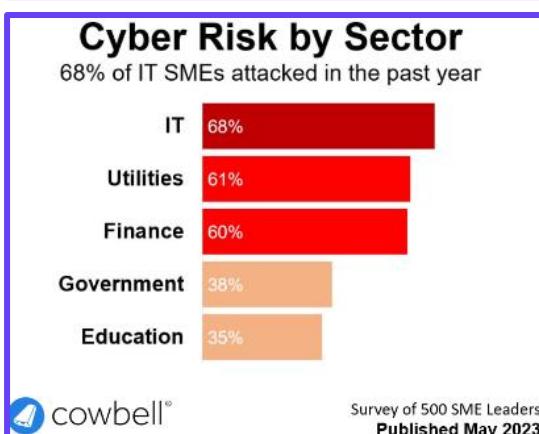
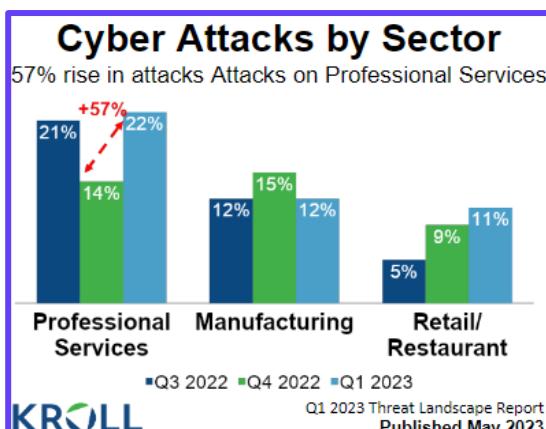
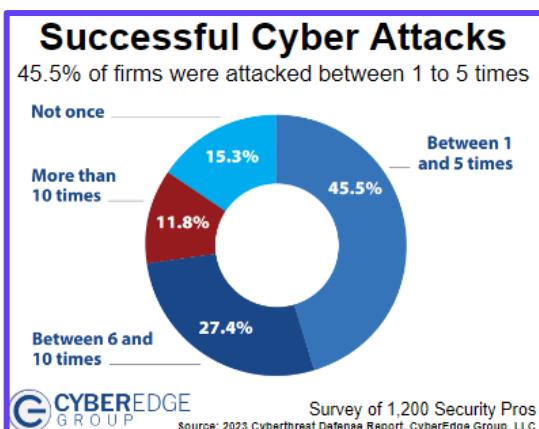
32% of Cybercrime uses Phishing for initial access

Method	Percentage
Phishing	32%
Valid (stolen) Account	18%
External Remote Services	17%
CVE or Zero-Day Exploit	13%

KROLL  
Q1 2023 Threat Landscape Report  
Published May 2023

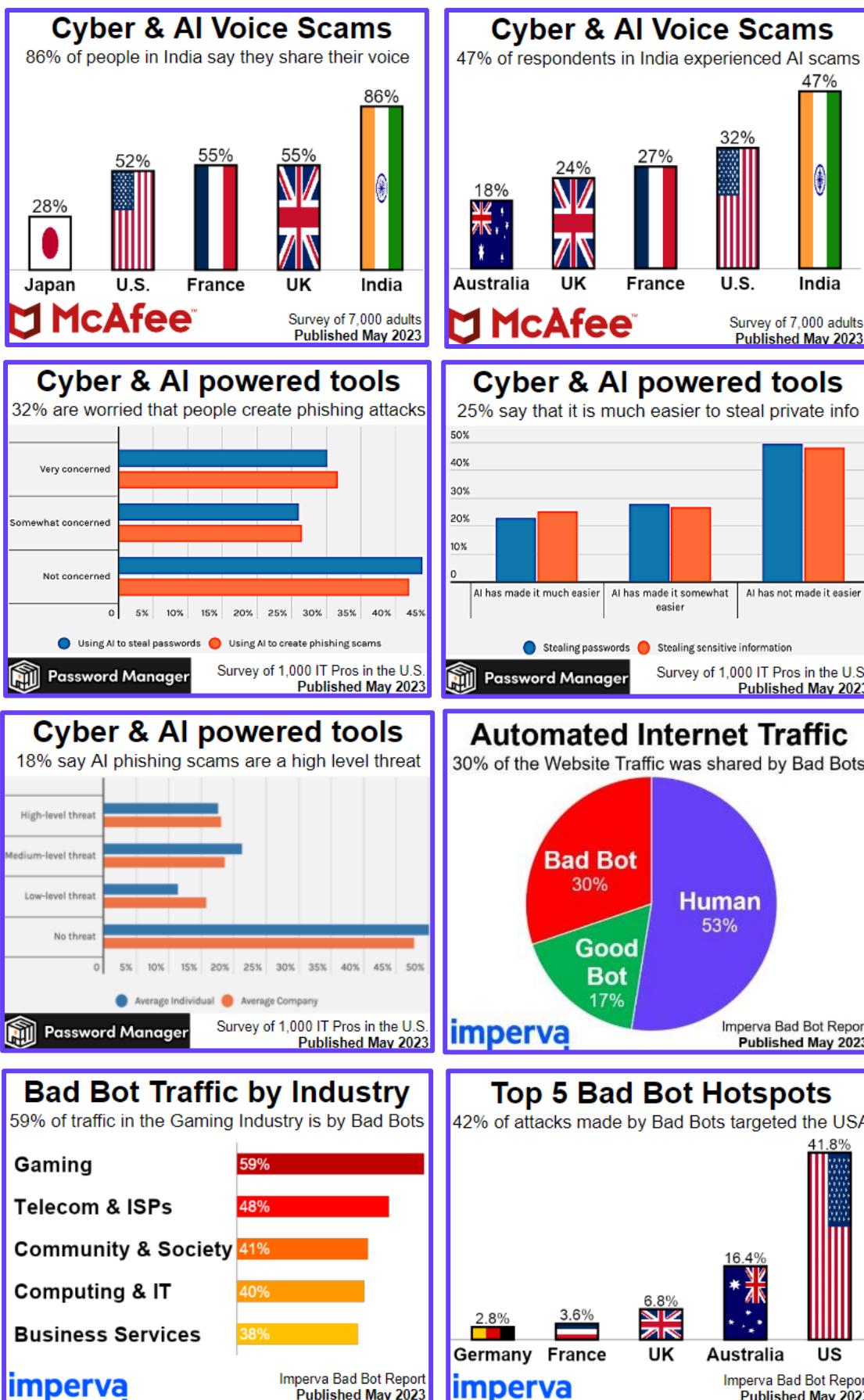
# Cyber Insights: Cyber Attacks

Click each image to see each report in full. All were published in month to March 2023



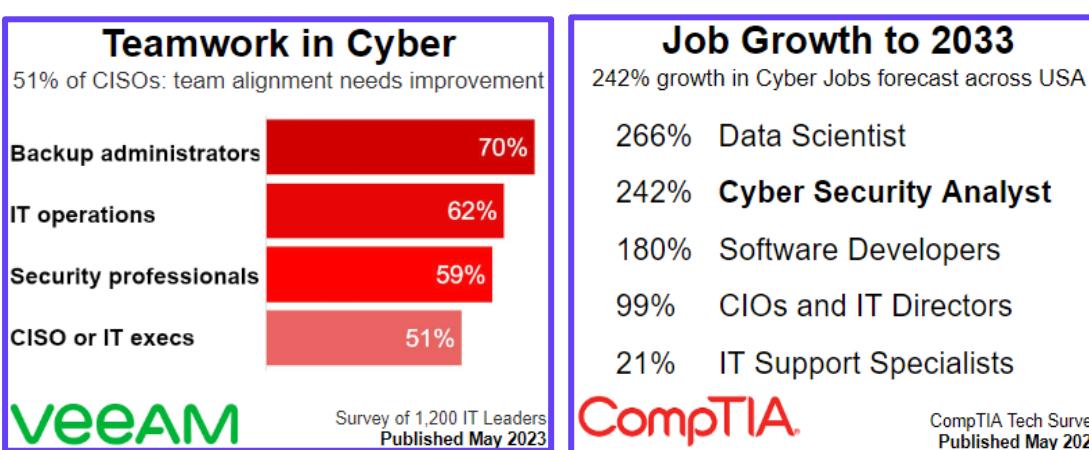
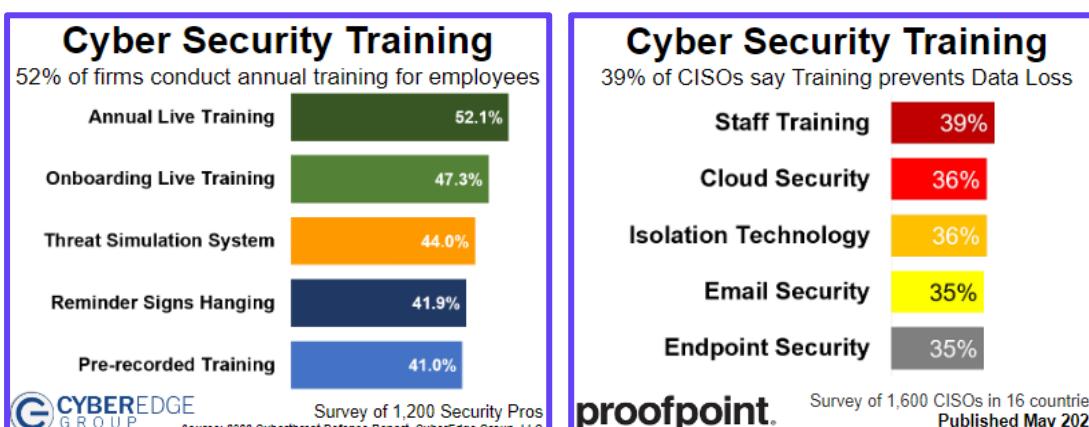
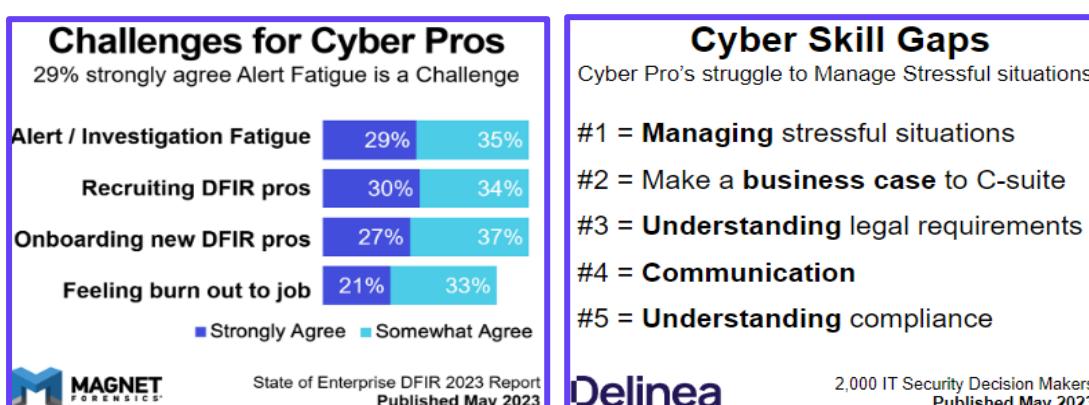
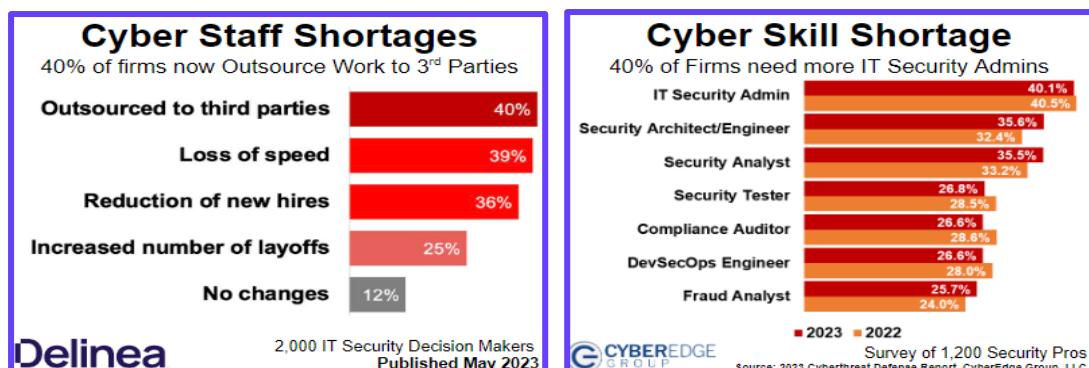
# Cyber Insights: AI and Bots

Click each image to see each report in full. All were published in month to March 2023



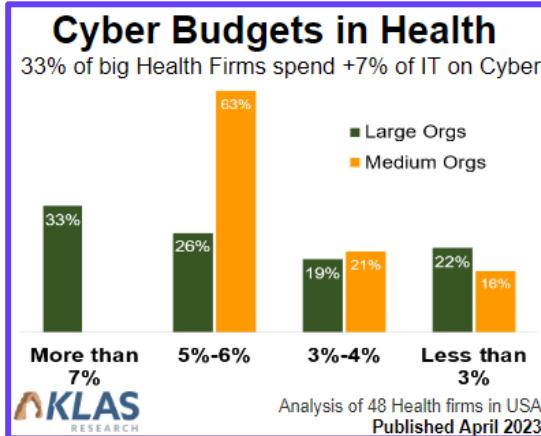
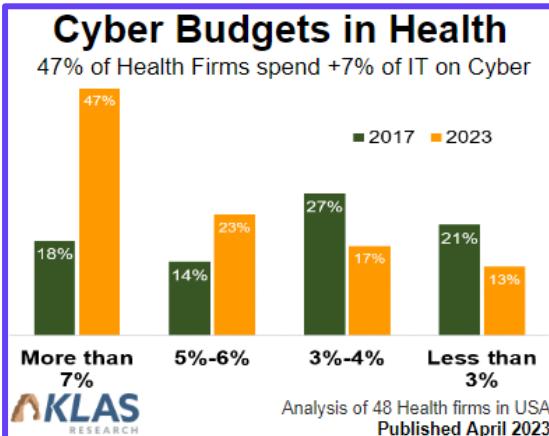
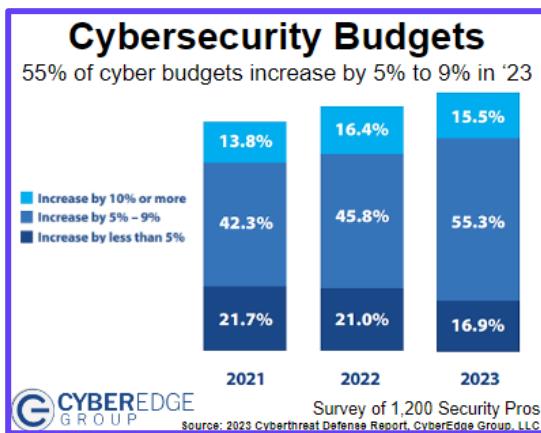
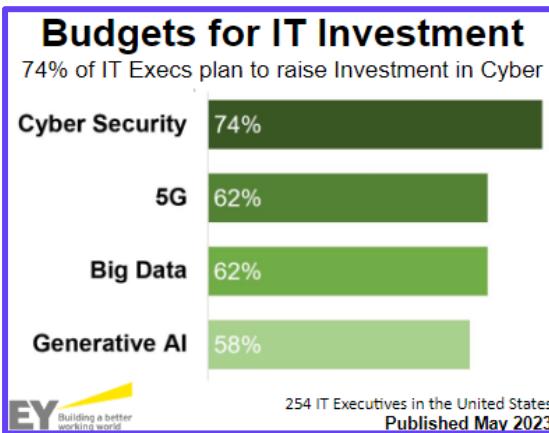
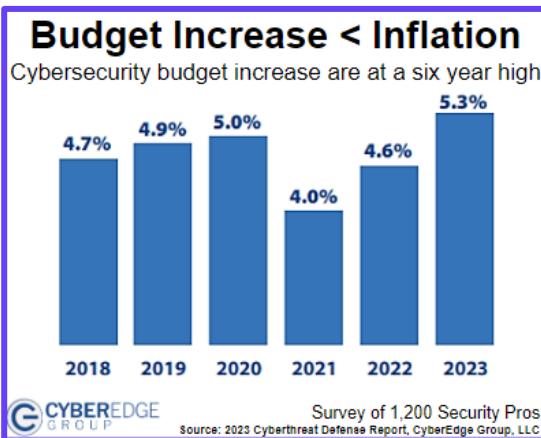
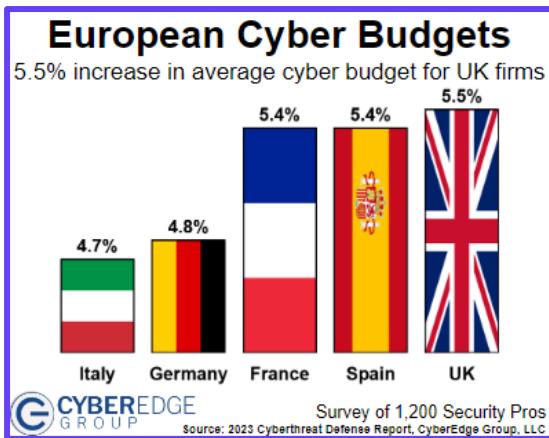
# Cyber Insights: Cyber Talent & Staff

Click each image to see each report in full. All were published in month to March 2023



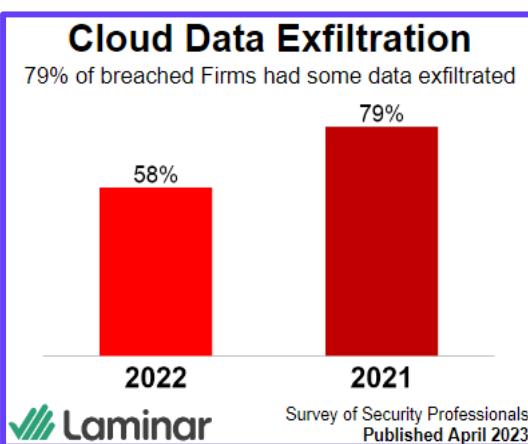
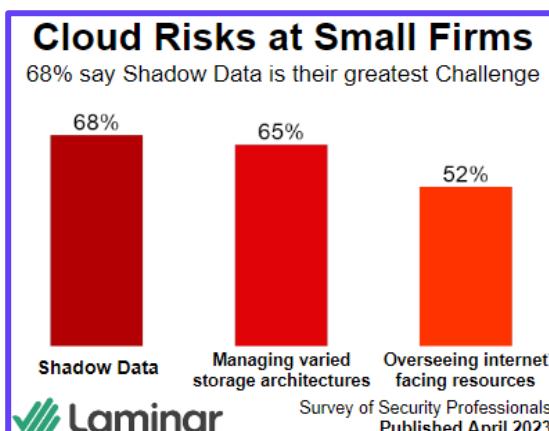
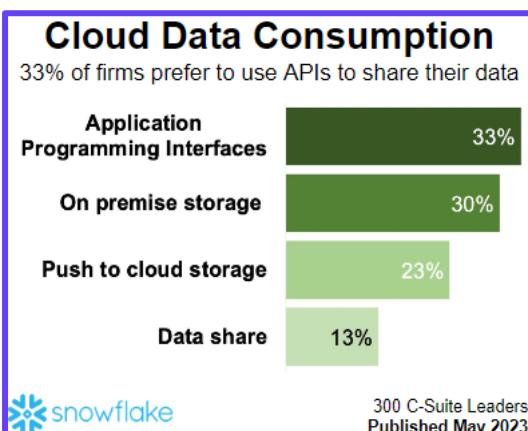
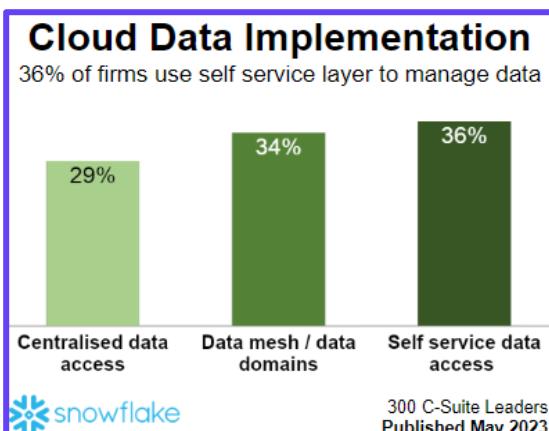
# Cyber Insights: Budget & Salaries

Click each image to see each report in full. All were published in month to March 2023



# Cyber Insights: Cloud Risks

Click each image to see each report in full. All were published in month to March 2023



# Cyber Insights: Cyber Resilience

Click each image to see each report in full. All were published in month to March 2023

## Operational Resilience

Top Priority = Identify Important Business Services

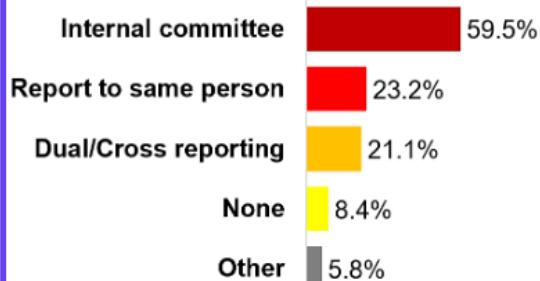
- #1 = Identify Important Bus Services
- #2 = Establish Impact Tolerances
- #3 = Prioritise Vulnerabilities
- #4 = Rehearse Plausible Scenarios
- #5 = Perform IBS Self Assessment



Survey of 334 Op Res leaders in 62 countries  
Published May 2023

## Operational Resilience

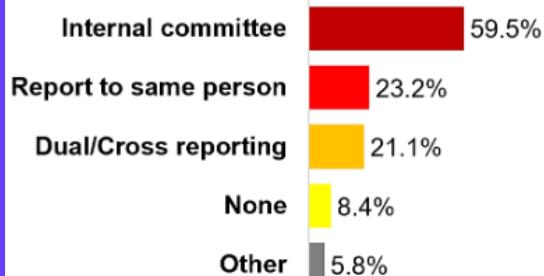
60% of Firms coordinate Resilience & Cyber Risk



Survey of 334 Op Res leaders in 62 countries  
Published May 2023

## Operational Resilience

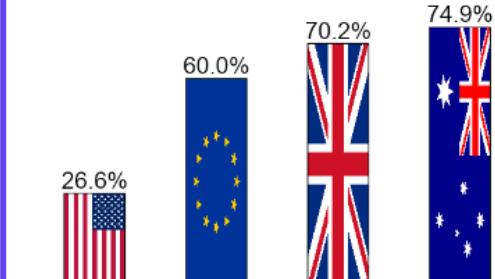
60% of Firms coordinate Resilience & Cyber Risk



Survey of 334 Op Res leaders in 62 countries  
Published May 2023

## Operational Resilience

75% of Australian firms say “regulator does enough”



Survey of 334 Op Res leaders in 62 countries  
Published May 2023

## Operational Resilience

32% of Op Res staff adhere to UK's FCA Approach

- #1 = UK's **FCA** Approach (32%)
- #2 = EU's **DORA** Act (22%)
- #3 = UK's **PRA** Approach (22%)
- #4 = Basel Committee **BCBS** (22%)
- #5 = USA **OCC** Sound Practices (14%)



334 Op Res leaders in 62 countries  
Published May 2023

## Operational Resilience

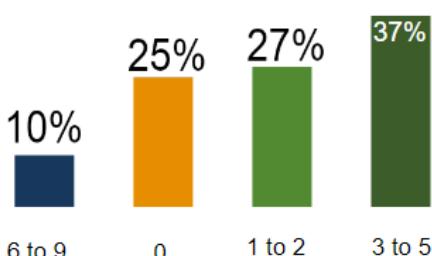
23% of Firms: Head of Resilience owns day-to-day



334 Op Res leaders in 62 countries  
Published May 2023

## Cyber Security Maturity

Intrusion-free firms had 25% boost in cyber maturity



Survey of 570 OT Professionals  
Published May 2023

## Operational Resilience

Top Challenge now is “Embedding OR in our firm”

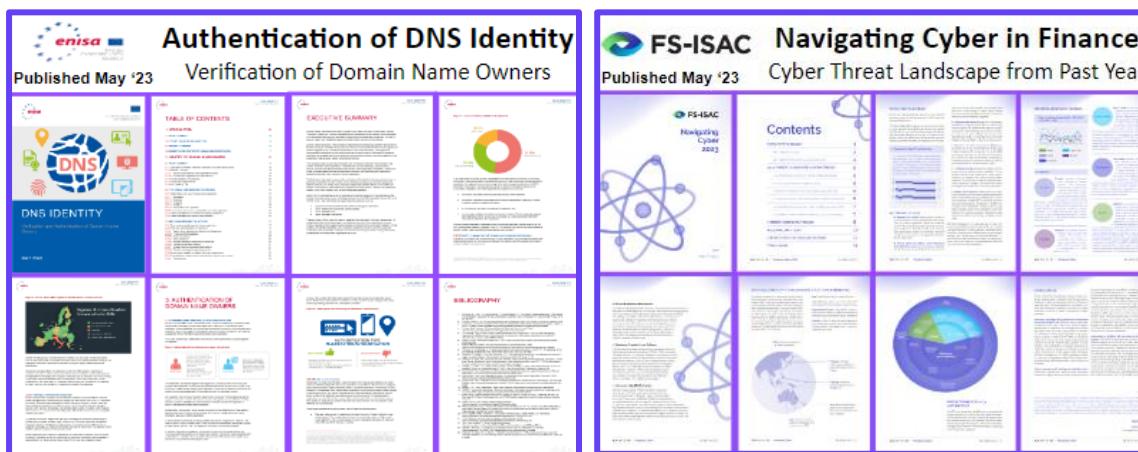
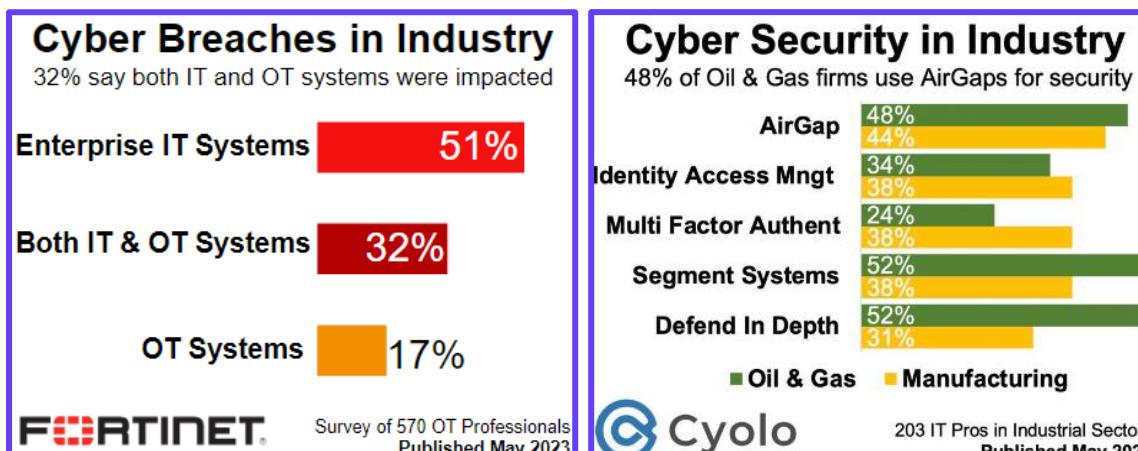
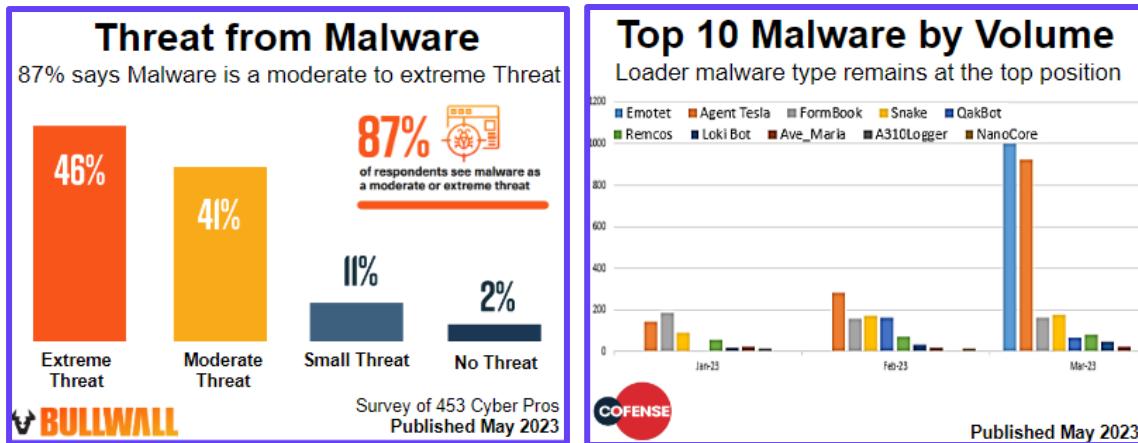
- #1 = To **Embed** Operational Resilience
- #2 = Not enough **Staff** to Implement
- #3 = Monitor **Supply Chain** Risks
- #4 = Address **Legacy** Infrastructure
- #5 = **Governance** of Resilience



334 Op Res leaders in 62 countries  
Published May 2023

# Cyber Insights: Malware & other Threats

Click each image to see each report in full. All were published in month to March 2023

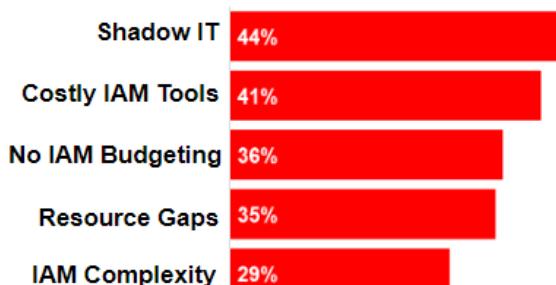


# Cyber Insights: Access Management

Click each image to see each report in full. All were published in month to March 2023

## Identity Access Management

Top 5 Perceived Challenges at firms planning IAM

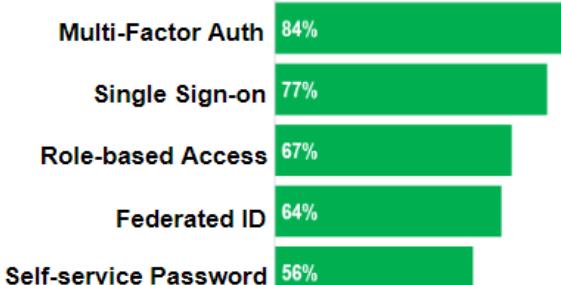


CyberRisk ALLIANCE

Survey of >200 Security Executives  
Published April 2023

## Identity Access Management

Top 5 Controls at firms that (plan to) use IAM

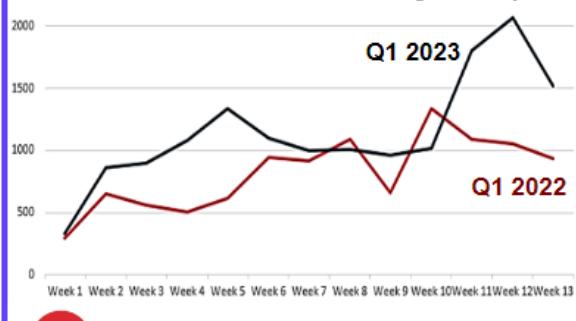


CyberRisk ALLIANCE

Survey of >200 Security Executives  
Published April 2023

## Credential Phishing Activity

40% increase in Credential Phishing vs last year

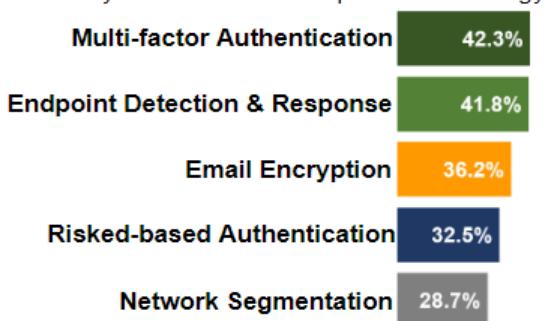


COFENSE

Published May 2023

## Mitigating Cyber Threats

42% say MFA is the most important technology

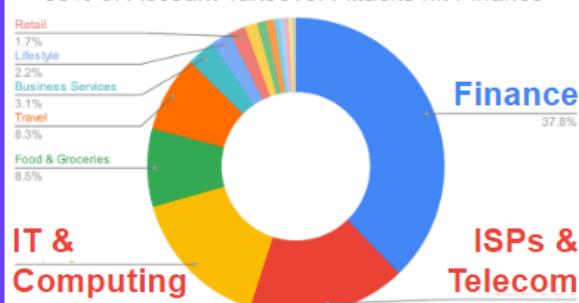


CYBEREDGE GROUP

Survey of 1,200 Security Pros  
Source: 2023 Cyberthreat Defense Report, CyberEdge Group, LLC

## Account Takeover Attacks

38% of Account Takeover Attacks hit Finance

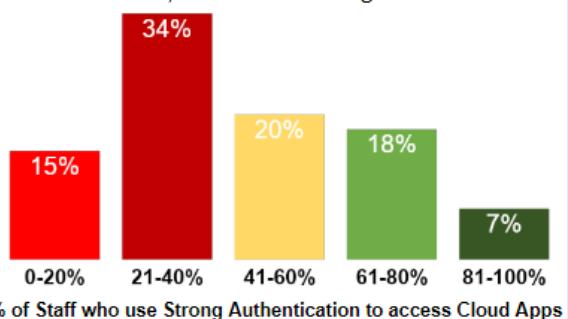


imperva

Imperva Bad Bot Report  
Published May 2023

## Cloud Access Authentication

At 7% of firms, >80% use Strong Authentication



THALES

2,889 IT Managers & Professionals  
Published April 2023

## Cyber Security in Industry

Visibility is Top Priority for Securing Remote Access

#1 = Visibility

#2 = User Education

#3 = Access Control

#4 = End of Life OS

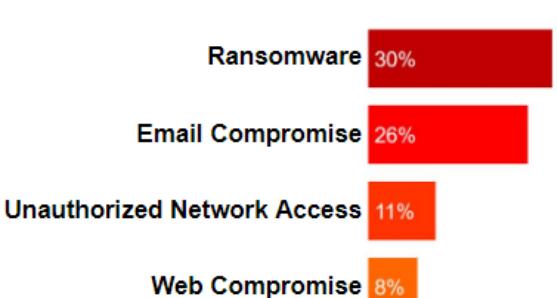
#5 = Policy & Enforcement

Cyolo

203 IT Pros in Industrial Sectors  
Published May 2023

## Serious Incident Frequency

11% of Kroll's incident work= Unauthorised Access



KROLL

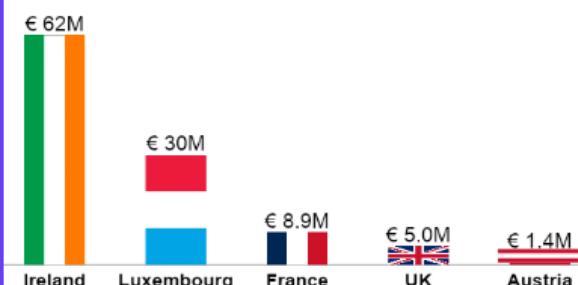
Q1 2023 Threat Landscape Report  
Published May 2023

# Cyber Insights: Cyber Fines & Costs

Click each image to see each report in full. All were published in month to March 2023

## GDPR Fines over last 5 Years

Average fine for GDPR-violations in Ireland is €62M

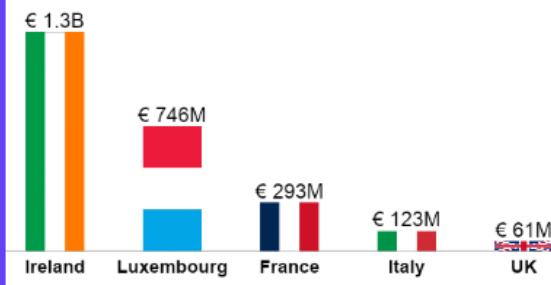


**CMS**

Data from GDPR Enforcement Tracker  
Published May 2023

## GDPR Fines over last 5 Years

1.3B Euros total of GDPR fines issued in Ireland

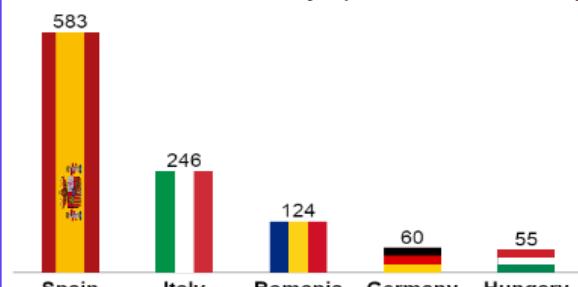


**CMS**

Data from GDPR Enforcement Tracker  
Published May 2023

## GDPR Fines over last 5 Years

583 GDPR fines issued by Spanish Data Authority

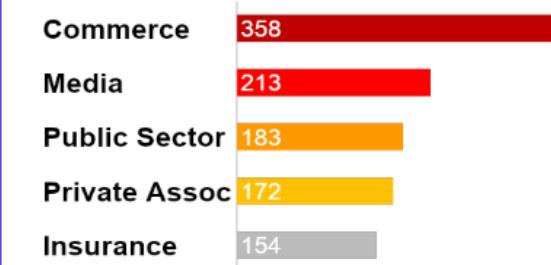


**CMS**

Data from GDPR Enforcement Tracker  
Published May 2023

## GDPR Fines over last 5 Years

358 GDPR fines to date issued to Commerce Sector



**CMS**

Data from GDPR Enforcement Tracker  
Published May 2023

## GDPR Fines by Violations

Insufficient Legal Basis is the Leading Reason

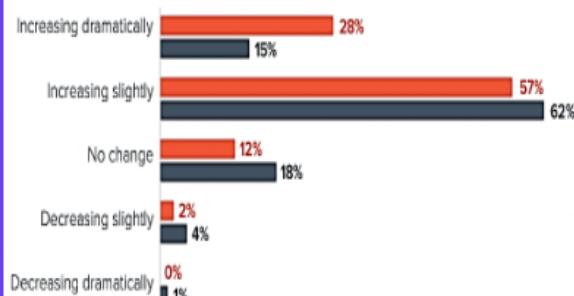
- #1 = Insufficient Legal Basis
- #2 = Insufficient Cyber Security
- #3 = Non-compliance With GDPR
- #4 = Data Subject Rights Not Fulfilled
- #5 = Info Obligations Not Fulfilled

**CMS**

Data from GDPR Enforcement Tracker  
Published May 2023

## Cyber Attack Cost

28% of Firms say the cost of attacks have increased

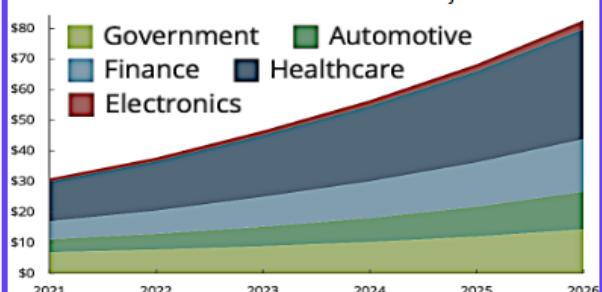


**Barracuda**

1,350 IT Professionals  
Published May 2023

## Cost of Attacks on Suppliers

£80 Billion annual loss forecast across just 5 sectors



**JUNIPER**  
RESEARCH

Published May 2023

## Ransom Payments Decrease

Size of each known payment -20% from Q4/22

Average known  
Payout =



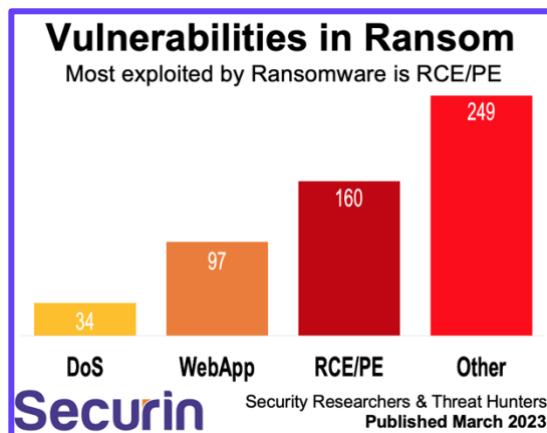
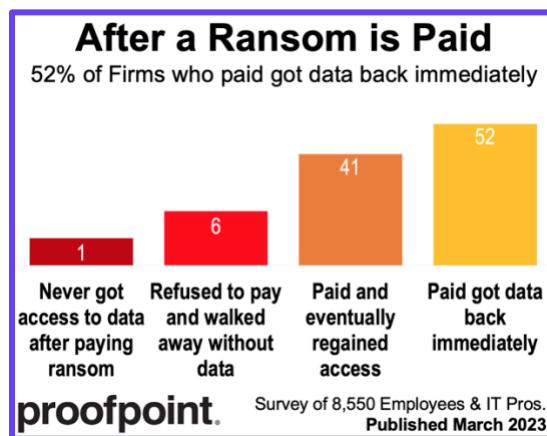
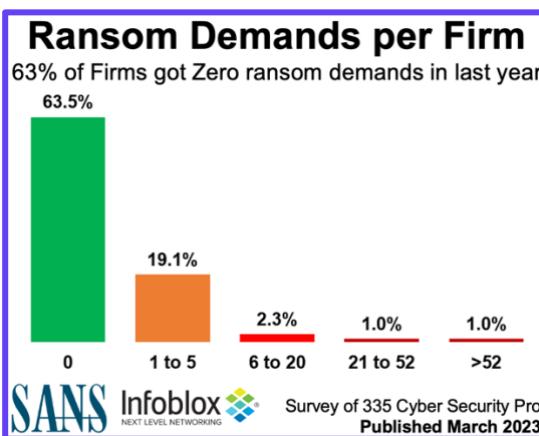
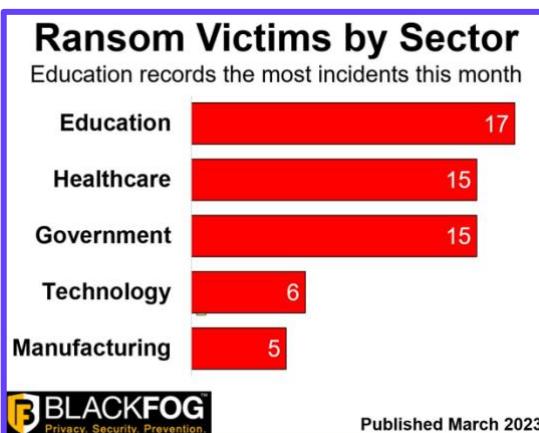
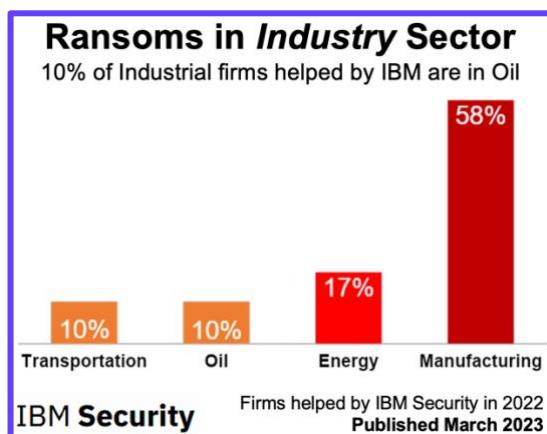
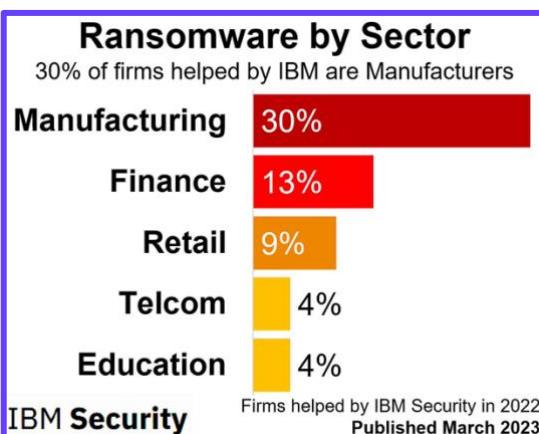
**USD \$327,883**

**BLACKFOG**  
Privacy. Security. Prevention.

Published May 2023

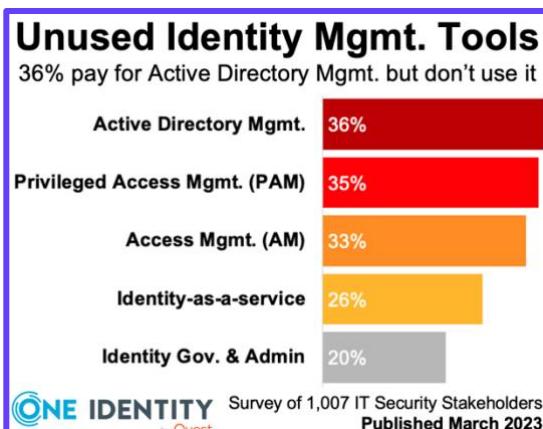
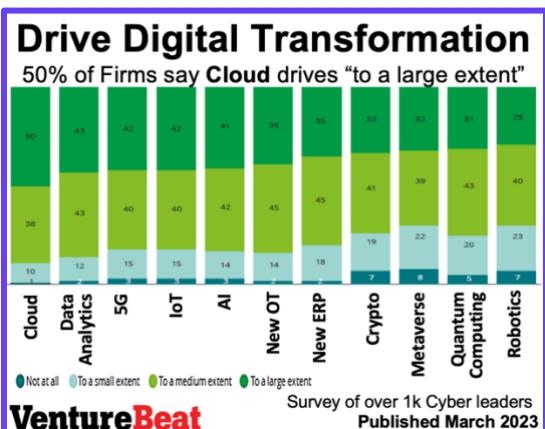
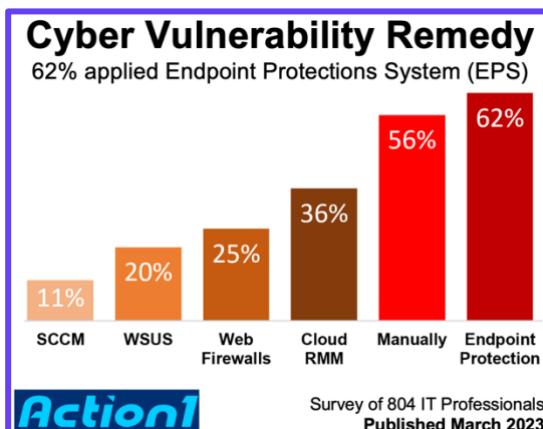
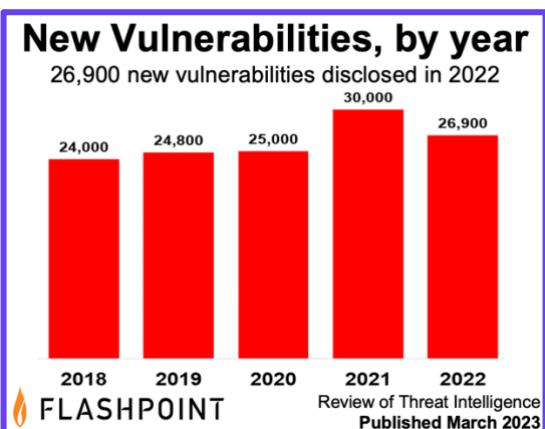
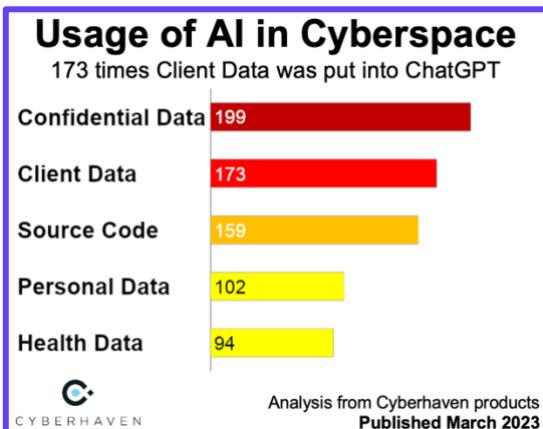
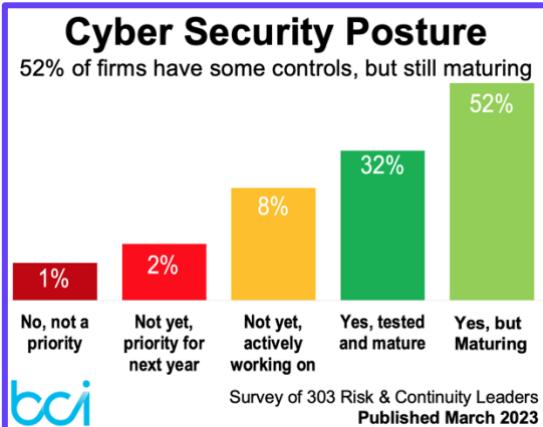
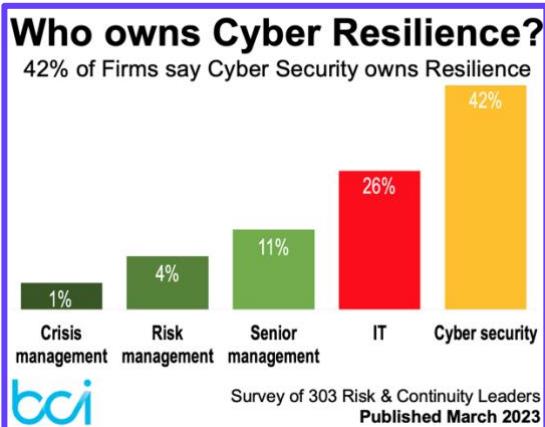
# Cyber Insights: Ransom & Sectors

Click each image to see each report in full. All were published in month to April 2023



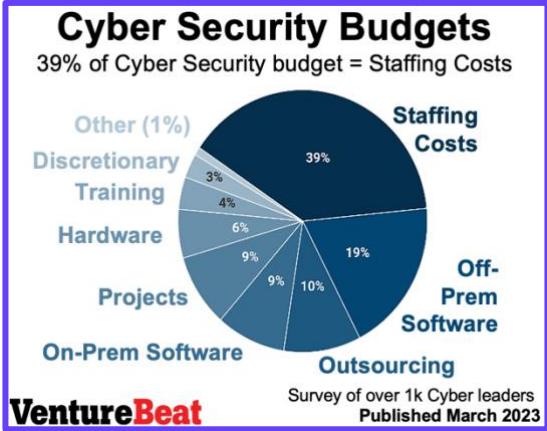
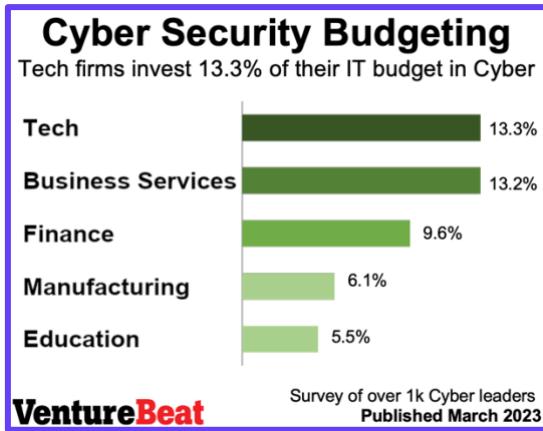
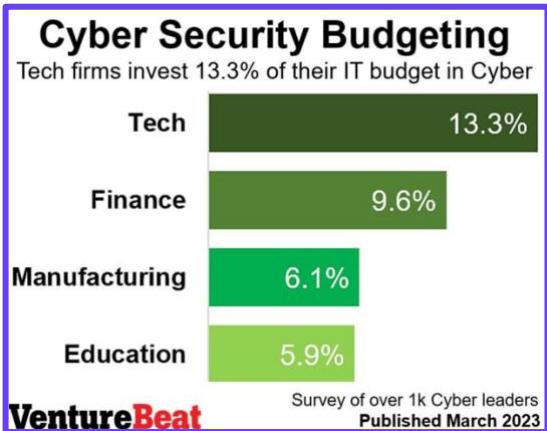
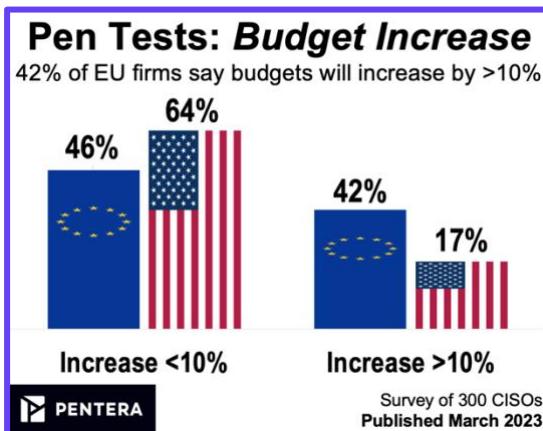
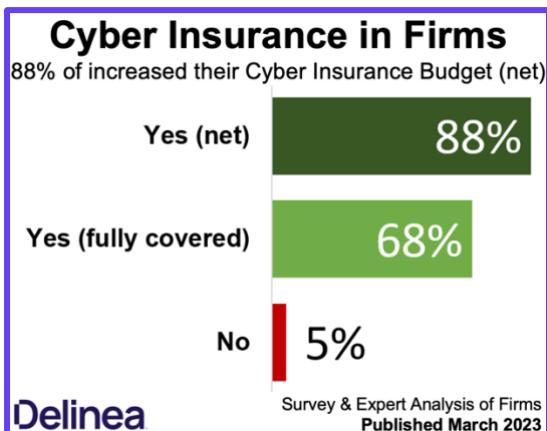
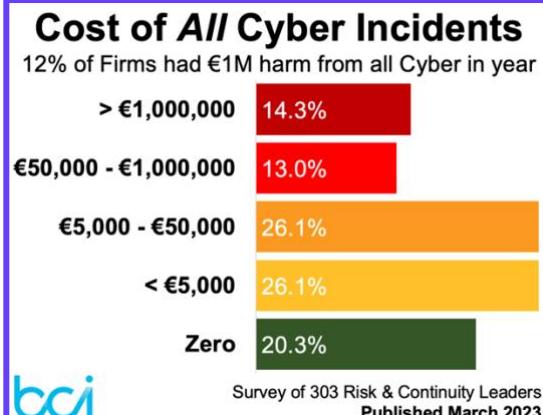
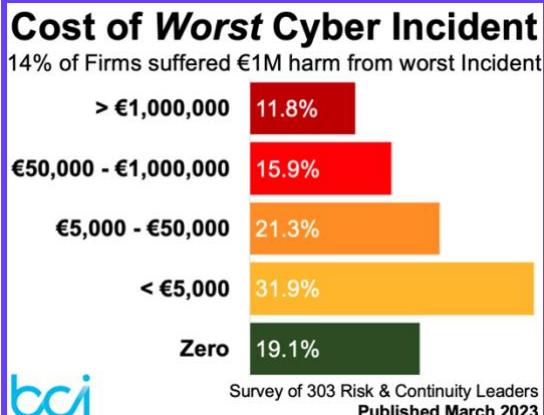
# Cyber Insights: Cyber Risks & Vectors

Click each image to see each report in full. All were published in month to April 2023



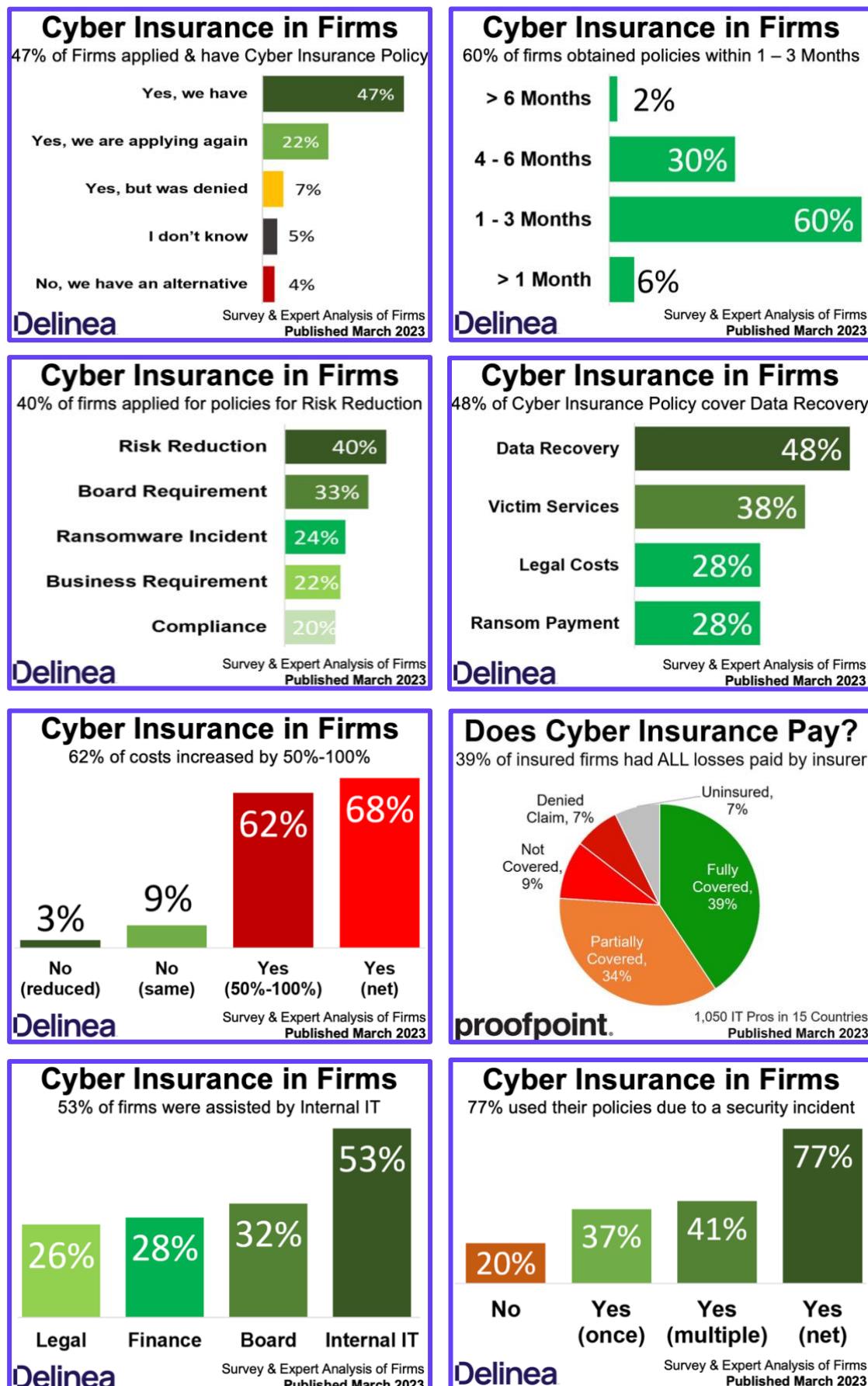
# Cyber Insights: Cyber Finances

Click each image to see each report in full. All were published in month to April 2023



# Cyber Insights: Cyber Insurance

Click each image to see each report in full. All were published in month to April 2023



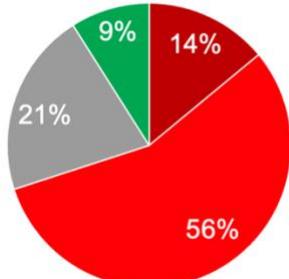
# Cyber Insights: CISOs in Cyber

Click each image to see each report in full. All were published in month to April 2023

## Most Stressful Role = CISO ?

Only 9% of CISOs think other roles are more stressful

- Considerably more stressed
- Somewhat more stressed
- Same level of stress
- Lower level of stress

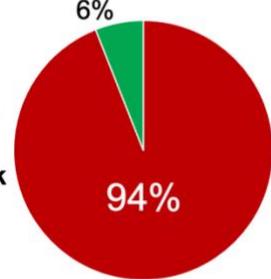


Survey of 200 CISOs  
Published March 2023

## CISO Stress at Work

94% of CISOs say they are Stressed at Work

- Stressed at work
- No stress at work

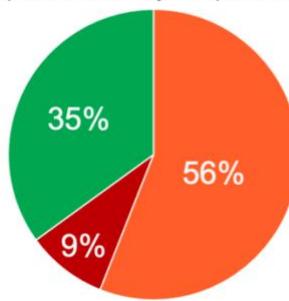


Survey of 200 CISOs  
Published March 2023

## CISOs who are Overloaded

9% of CISOs: ability to protect definitely compromised

- Somewhat
- Definitely
- Not at all

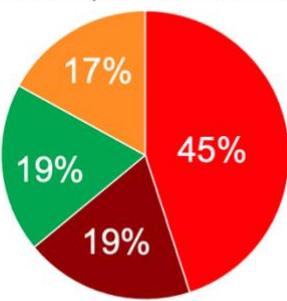


Survey of 200 CISOs  
Published March 2023

## Talent Shortages in Cyber

Only 17% of CISOs never compromise when hiring

- Sometimes
- Frequently
- Once
- Never

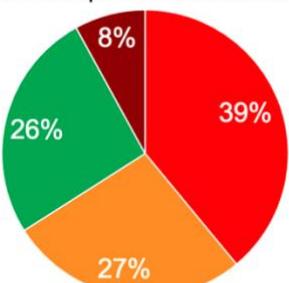


Survey of 200 CISOs  
Published March 2023

## Cyber Security Staff Stress

26% of CISOs say zero Staff quit for Stress in 2022

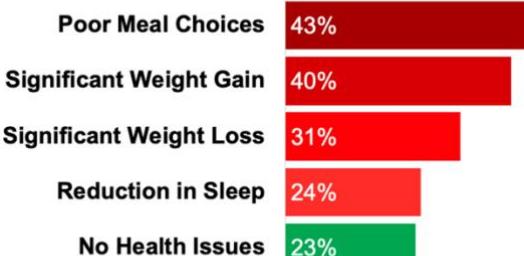
- A few
- Once
- Zero
- Several



Survey of 200 CISOs  
Published March 2023

## Health Impacts on CISOs

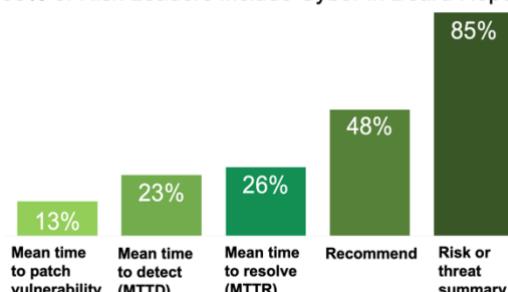
43% of CISOs Eat Poorly due to Lack of Time



Survey of 200 CISOs  
Published March 2023

## Reporting Cyber Resilience

85% of Risk Leaders include Cyber in Board Report

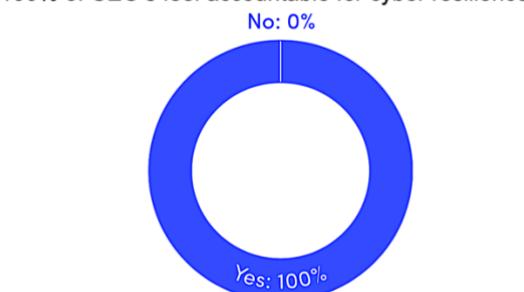


Survey of 303 Risk & Continuity Leaders  
Published March 2023



## CEO's Cyber Accountability

100% of CEO's feel accountable for cyber resilience



Survey of 37 CEO's  
Published March 2023

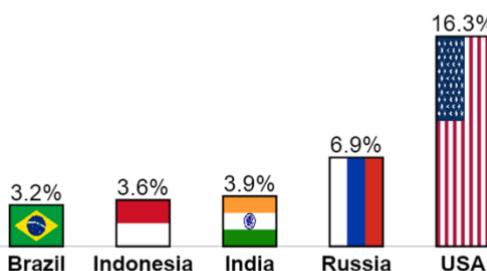


# Cyber Insights: By Country & By Sector

Click each image to see each report in full. All were published in month to April 2023

## Cyber Attacks on Countries

16.3% of attacks target organisations in the USA

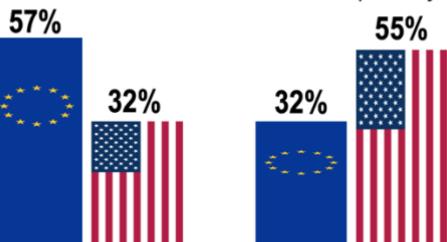


**SOCRadar**  
Your Eyes Beyond

SOCRadar analysis of attacks  
Published March 2023

## Cyber Attack Compromise

55% of USA firms suffered a breach in past 2 years



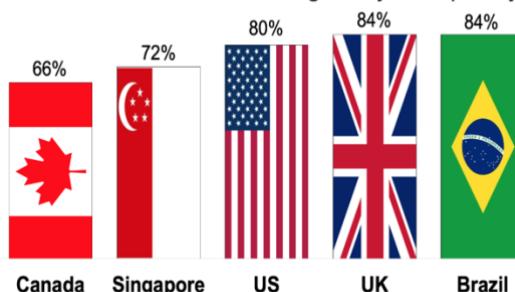
In the past 12 months In the past 24 months

**PENTERA**

Survey of 300 CISOs  
Published March 2023

## Prioritizing Cyber Security

84% of Brazil & UK Boards agree Cyber is priority

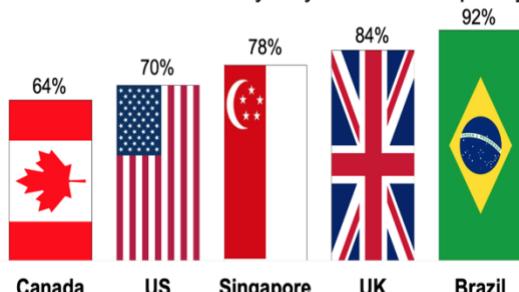


**proofpoint.**

Survey of 600 board directors  
Published March 2023

## Investing in Cyber Security

92% of Brazil Board's say they invested adequately

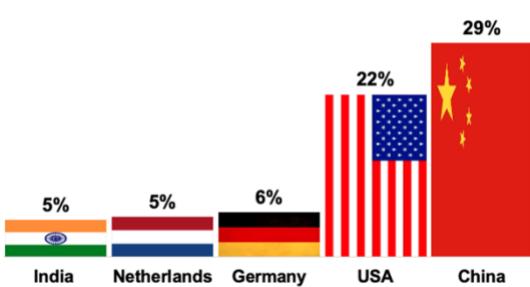


**proofpoint.**

Survey of 600 board directors  
Published March 2023

## Cyber Command & Control

29% of hackers' C&C servers are hosted in China

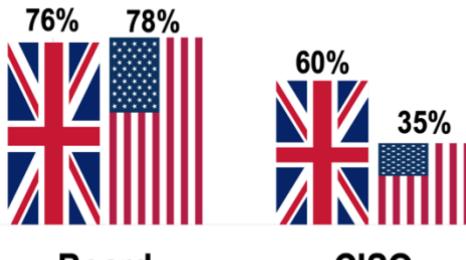


**IronNet**

Analysis from IronNet ecosystem  
Published March 2023

## Cyber Attack: Board vs CISO

35% of CISOs in the USA say their Firm is at Risk



**Board**

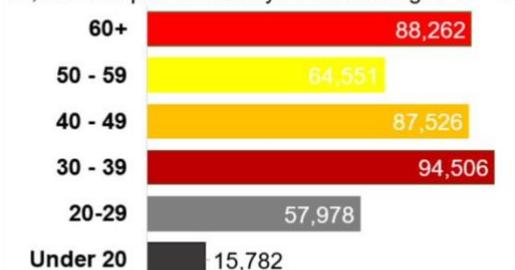
**CISO**

**proofpoint.**

Survey of 600 board directors  
Published March 2023

## Cyber Victims by Age in USA

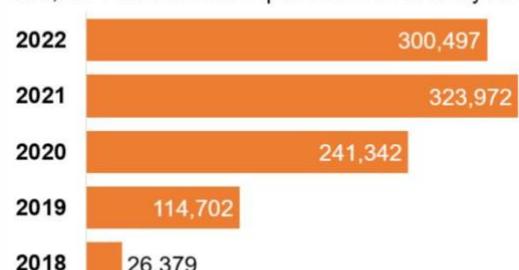
94,506 Complaints filed by Americans aged 30 - 39



Crimes reported to FBI's ICCC unit  
Published March 2023

## Phish Crime Reported in US

300,497 Phish Crimes reported to FBI in last year



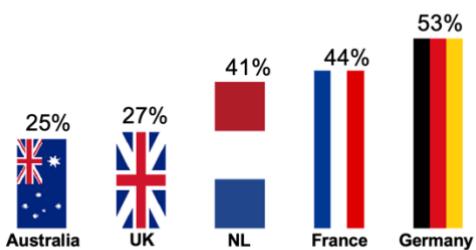
Crimes reported to FBI's ICCC unit  
Published March 2023

# Cyber Insights: Government

Click each image to see each report in full. All were published in month to April 2023

## Cyber for Government Staff

27% in UK say their actions don't impact security

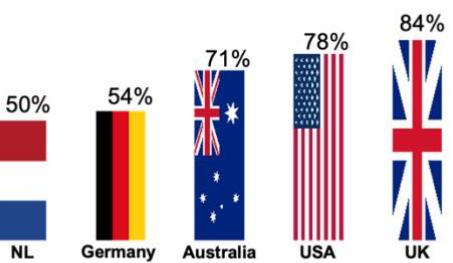


**ivanti**

Survey of 803 Government Staff  
Published March 2023

## Cyber in Governments

84% of UK government staff receive cyber training

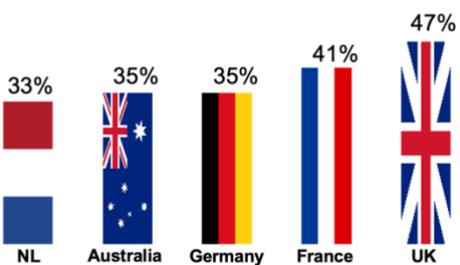


**ivanti**

Survey of 803 Government Staff  
Published March 2023

## Cyber in Governments

47% use their work passwords for over a year

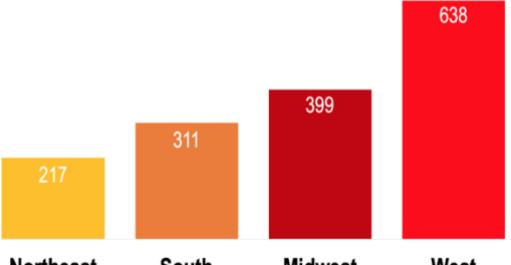


**ivanti**

Survey of 803 Government Staff  
Published March 2023

## Email breaches by Region

West tops the most number of breaches with 638

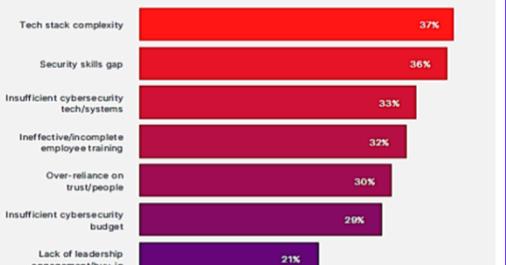


**Securin**

Security Researchers & Threat Hunters  
Published March 2023

## Cyber in Governments

37% say complex tech stack is a significant barrier



**ivanti**

Survey of 803 Government Staff  
Published March 2023

## Cyber in Governments

21% of government staff don't care

17% don't feel safe reporting a security mistake they've made at work to the cybersecurity team.

36% did not report a phishing email they received at work.

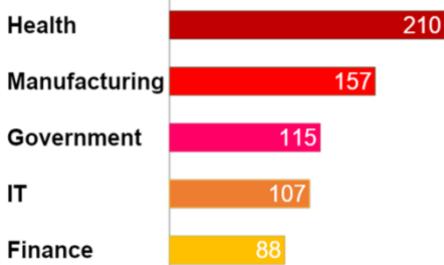
21% say they don't care if their organization gets hacked.

**ivanti**

Survey of 803 Government Staff  
Published March 2023

## Ransomware Victims in USA

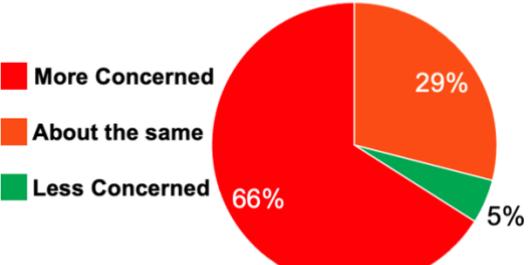
210 Health firms in USA reported Ransom in 2022



Crimes reported to FBI's ICCC unit  
Published March 2023

## Cyber Concern is Growing

66% are more concerned about Attacks than before



**SONICWALL**

Data from SonicWall Survey  
Published March 2023

# Cyber Insights: Consolidation & Mitigation

Click each image to see each report in full. All were published in month to April 2023



# Cyber Insights: Cyber Risk in Sectors

Click each image to see each report in full. All were published in month to April 2023

**Cyber Exposure by Sector**

9% chance of \$40M incident at typical Health Firm

Sector	Average Loss (\$M)	Average Probability (%)
Healthcare	~\$40M	~0.09
Educational Services	~\$30M	~0.06
Finance and Insurance	~\$45M	~0.05
Accommodation and Food Services	~\$30M	~0.04
Professional Services	~\$30M	~0.03
Information	~\$40M	~0.02
Manufacturing	~\$50M	~0.01
Retail	~\$50M	~0.01

**Cyber Risk for Manufactures**

3.4% chance of Insider Misuse causing \$90M Loss

Risk Type	Average Loss (\$M)	Average Probability (%)
Insider Misuse	~\$90M	~0.034
Basic Web Application Attacks	~\$50M	~0.022
Ransomware	~\$25M	~0.018
Social Intrusion	~\$50M	~0.015
Denial of Service	~\$25M	~0.008
Insider Error	~\$75M	~0.008
Social Engineering	~\$75M	~0.008
Social Engineering	~\$75M	~0.008

**Cyber Risk for Finance Firms**

10.4% chance of Insider Error causing a \$38M Loss

Risk Type	Average Loss (\$M)	Average Probability (%)
Insider Error	~\$38M	~0.104
Insider Misuse	~\$40M	~0.08
Basic Web Application Attacks	~\$40M	~0.04
System Intrusion	~\$60M	~0.03
Denial of Service	~\$20M	~0.02
Ransomware	~\$20M	~0.015
Social Engineering	~\$60M	~0.01

**Cyber Risk for Prof. Firms**

3.4% chance of WebApp Attack causing \$34M Loss

Risk Type	Average Loss (\$M)	Average Probability (%)
Insider Error	~\$34M	~0.034
Insider Misuse	~\$60M	~0.03
Basic Web Application Attacks	~\$40M	~0.025
Ransomware	~\$20M	~0.015
Denial of Service	~\$20M	~0.012
Social Engineering	~\$60M	~0.01
Insider Intrusion	~\$60M	~0.01

**Sectors Most Often Targeted**

21.6% of intrusion activity targets Tech sector

Sector	Percentage
Technology	21.6%
Finance	8.4%
Healthcare	8.3%
Telco	7.5%
Retail	6.0%

**Sectors Advertised for Attack**

Education most often advertised by Access Brokers

Sector	Percentage
Education	~15%
Technology	~12%
Industrial	~10%
Manufacturing	~8%
Services	~6%

**Phishing of Industry Brands**

7% of Finance Firms experienced Phishing

Brand Type	Percentage
Finance	7%
Cloud	4%
Telco	3%
Social Media	3%
Ecommerce	3%

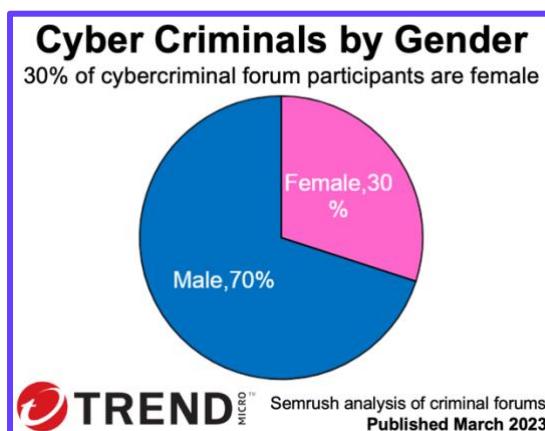
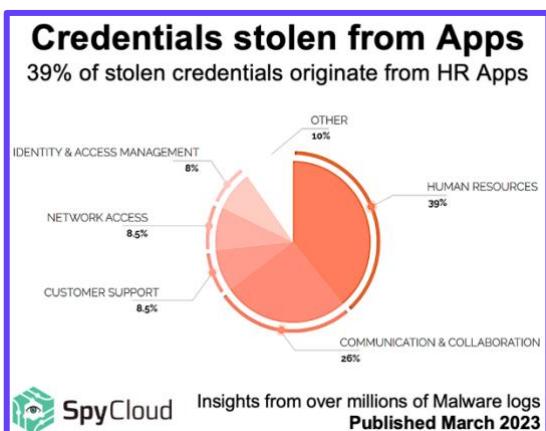
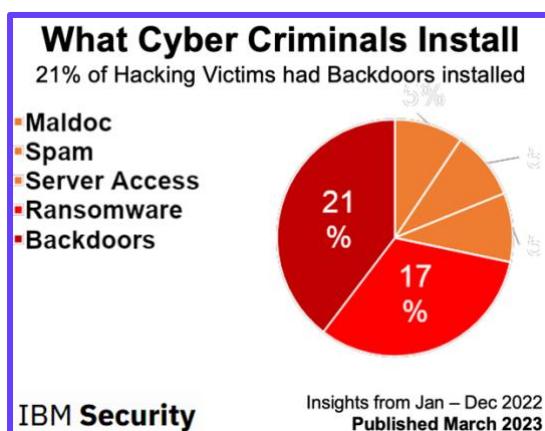
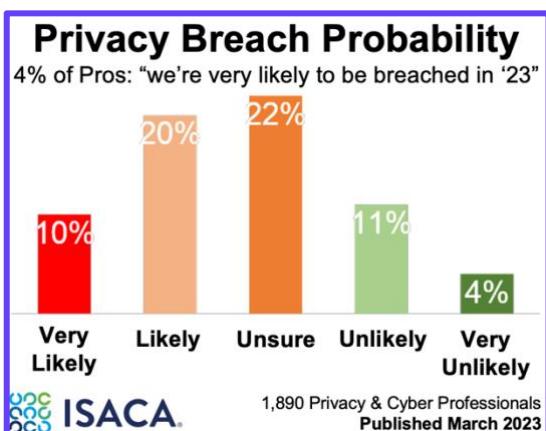
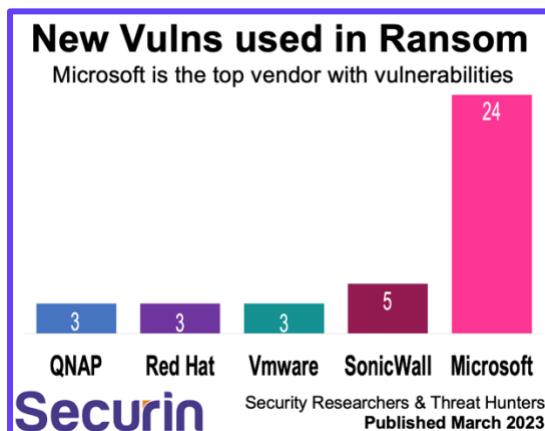
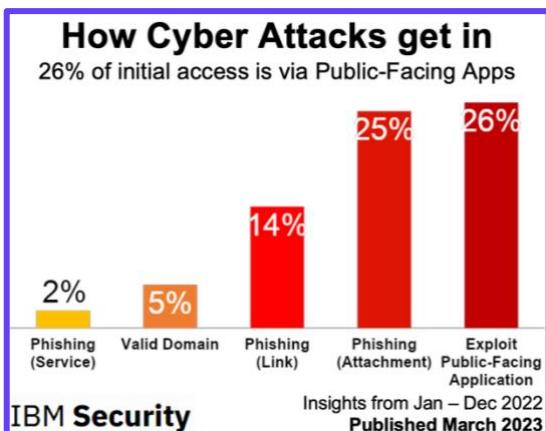
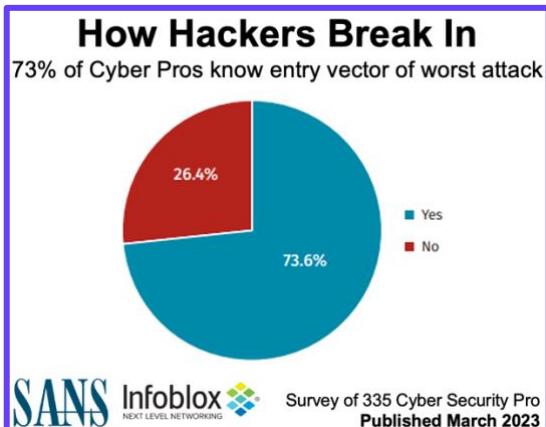
**Stolen Credentials in billions**

13.8 billion credentials stolen in Information Sector

Sector	Billion Credentials Stolen
Information	13.8
Professional Scientific	2.2
Retail	1.4
Manufacturing	0.8
Transport	0.3

# Cyber Insights: Cyber Initial Vectors

Click each image to see each report in full. All were published in month to April 2023

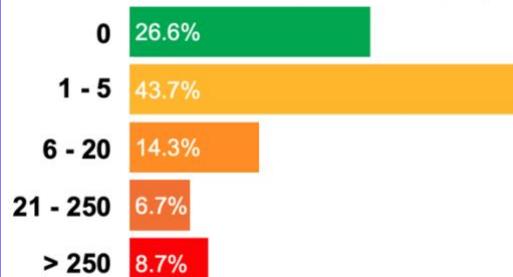


# Cyber Insights: *Cyber Disruption*

Click each image to see each report in full. All were published in month to April 2023

## Cyber Incident Frequency

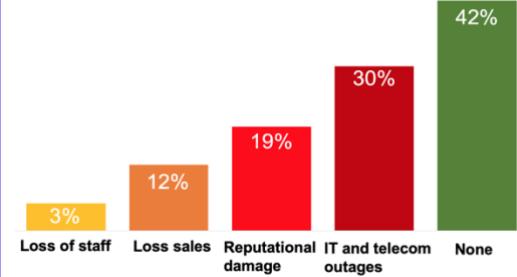
26.6% of Firms suffer Zero cyber incidents per year



Survey of 266 Risk & Continuity Leaders  
Published March 2023

## Harm from Cyber Incidents

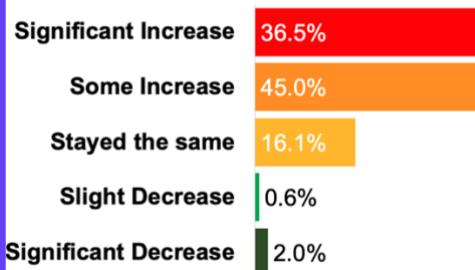
42% of Firms unharmed by Cyber Incident this year



Survey of 303 Risk & Continuity Leaders  
Published March 2023

## Cyber Incident Growth

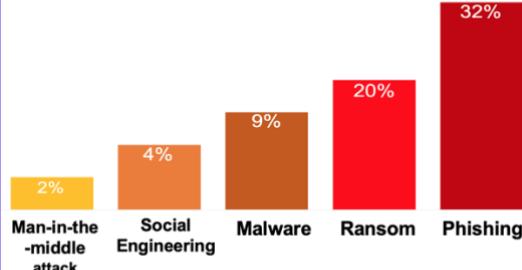
36.5% of Firms saw a big increase in Cyber Attacks



Survey of 275 Risk & Continuity Leaders  
Published March 2023

## Severe Cyber Disruption

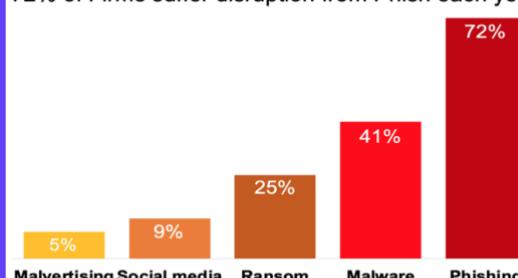
32% of the most severe disruption caused by Phish



Survey of 303 Risk & Continuity Leaders  
Published March 2023

## Disruption caused by Cyber

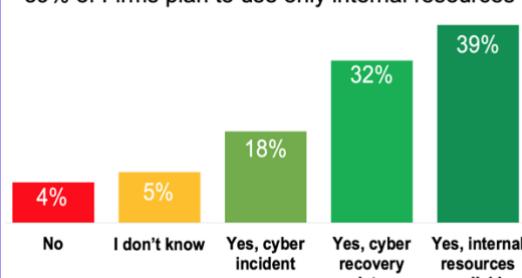
72% of Firms suffer disruption from Phish each year



Survey of 303 Risk & Continuity Leaders  
Published March 2023

## Plans for Cyber Disruption

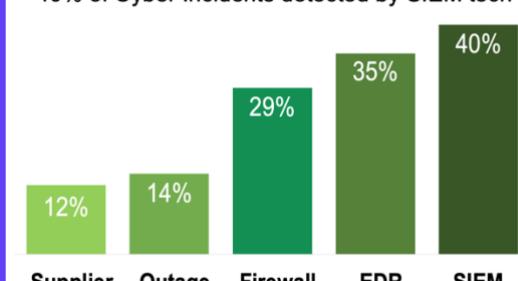
39% of Firms plan to use only internal resources



Survey of 303 Risk & Continuity Leaders  
Published March 2023

## Cyber Incident Detection

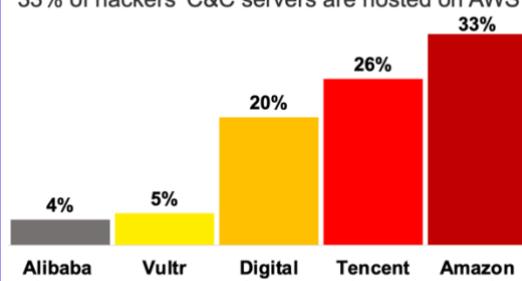
40% of Cyber Incidents detected by SIEM tech



Survey of 303 Risk & Continuity Leaders  
Published March 2023

## Cyber Command & Control

33% of hackers' C&C servers are hosted on AWS



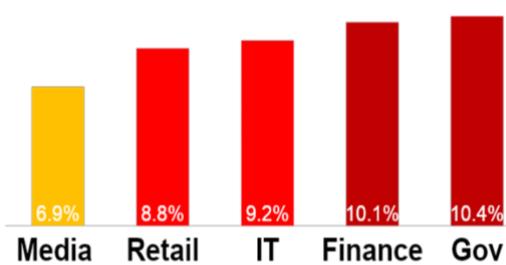
Analysis from IronNet ecosystem  
Published March 2023

# Cyber Insights: Phishing

Click each image to see each report in full. All were published in month to April 2023

## Phishing Attacks by Sector

10.4% of Phishing attacks target Government

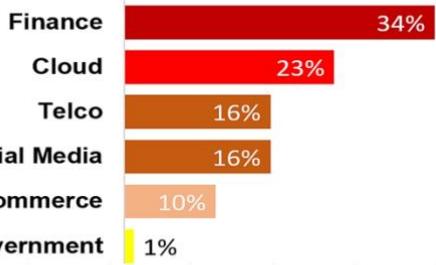


**SOCRadar**  
Your Eyes Beyond

SOCRadar analysis of attacks  
Published March 2023

## Top Phishing by Industry

34% of Phishing attacks target Financial Services

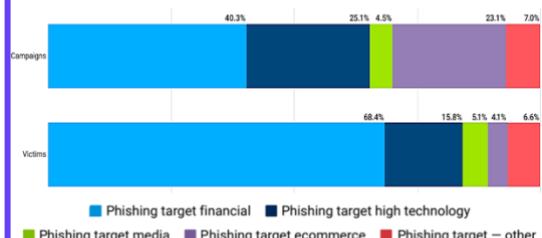


**vade**

Insights from Jan – Dec 2022  
Published March 2023

## Phishing Impersonation

68% of Phish pretended to be from Finance firms



**Akamai**

Insights from Jan – Dec 2022  
Published February 2023

## Top Impersonated Brands

Facebook is the Top Impersonated Brand

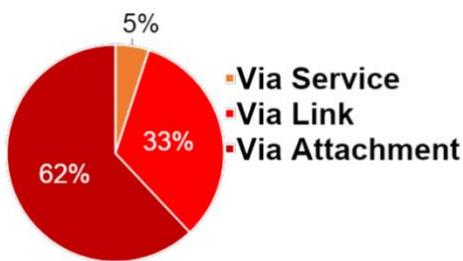
- #1 = Facebook
- #2 = Microsoft
- #3 = Google
- #4 = PayPal
- #5 = MTB

**vade**

Insights from Jan – Dec 2022  
Published March 2023

## Phishing Techniques

62% of Phishing Attacks use infected Attachments

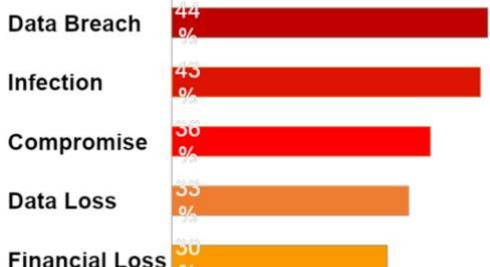


**IBM Security**

Insights from Jan – Dec 2022  
Published March 2023

## Successful Phishing Attacks

44% of successful Phish result in a Data Breach



Survey of 8,550 Employees & IT Pros.  
Published March 2023

## Fallout from Phishing Attack

54% suffered Financial Loss from Customer Churn



**egress**

Survey of 500 Cybersecurity Leaders  
Published March 2023

## Punishing of Phish Victims

11% of Firms terminate staff who fall victim to Phish

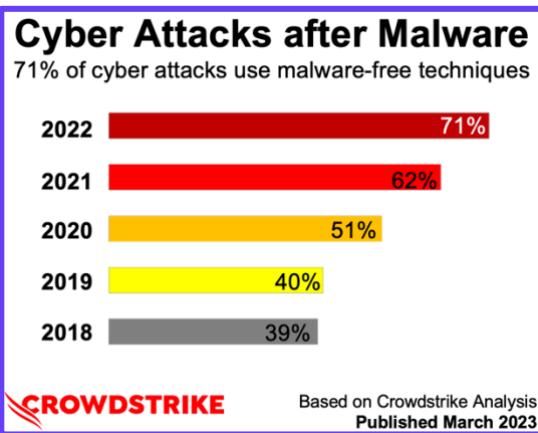
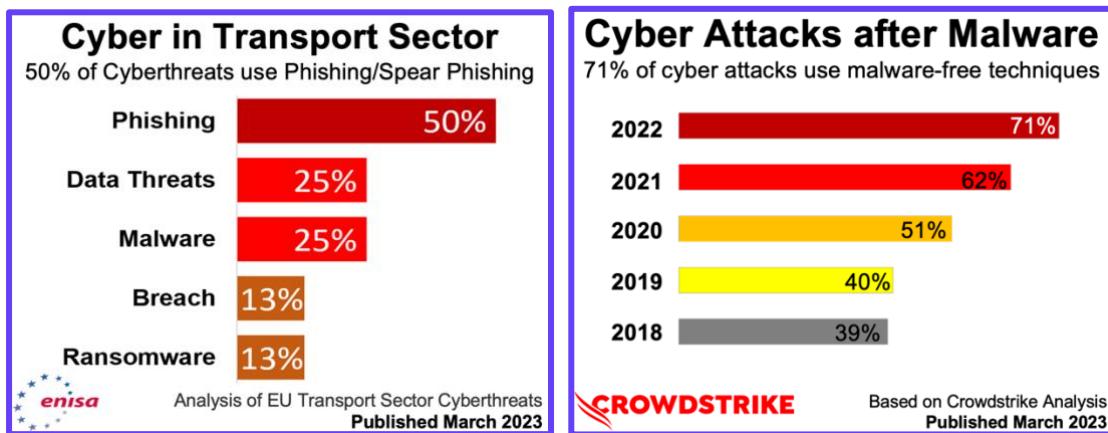
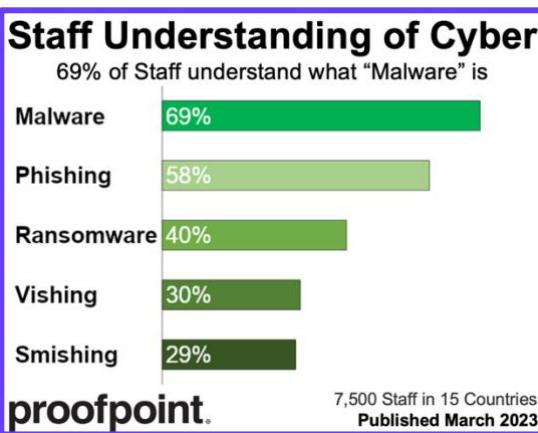
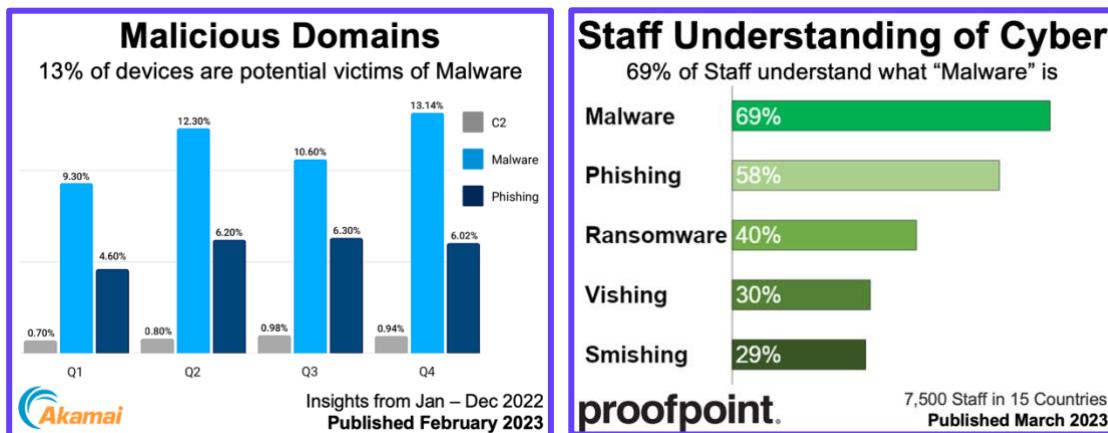
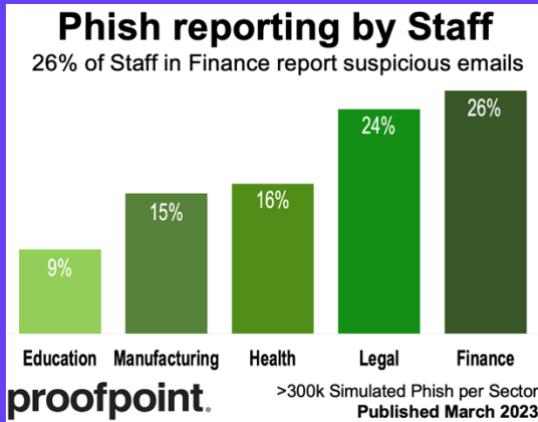
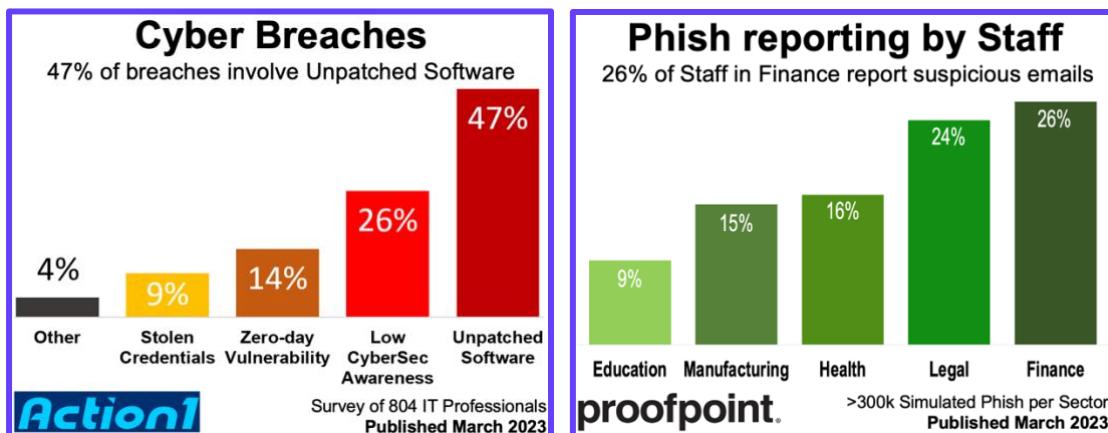


**proofpoint**

1,050 IT Pros in 15 Countries  
Published March 2023

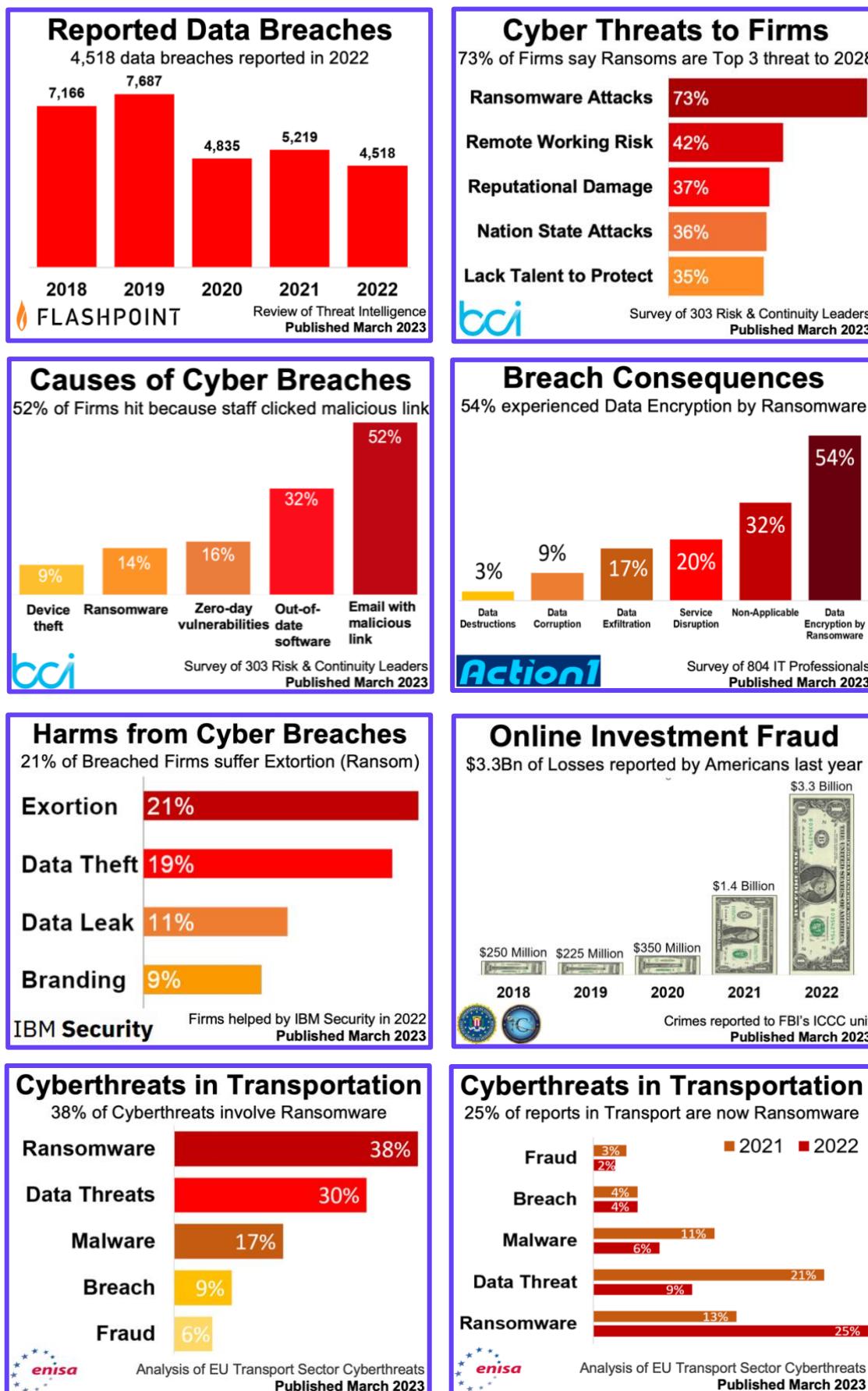
# Cyber Insights: Phish & Attacks

Click each image to see each report in full. All were published in month to April 2023



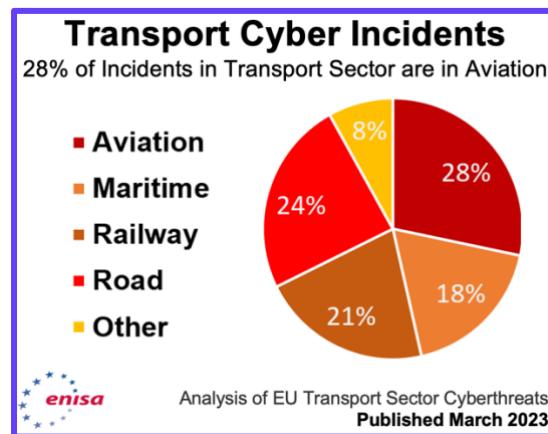
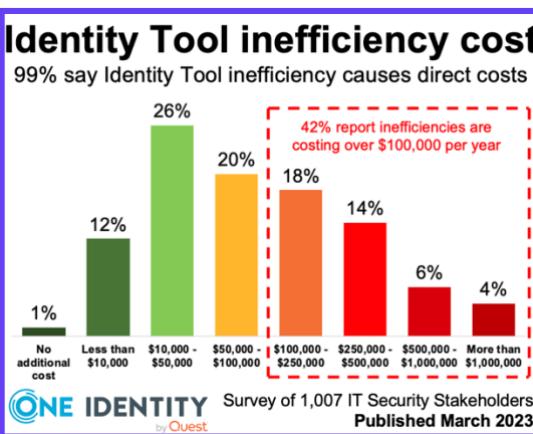
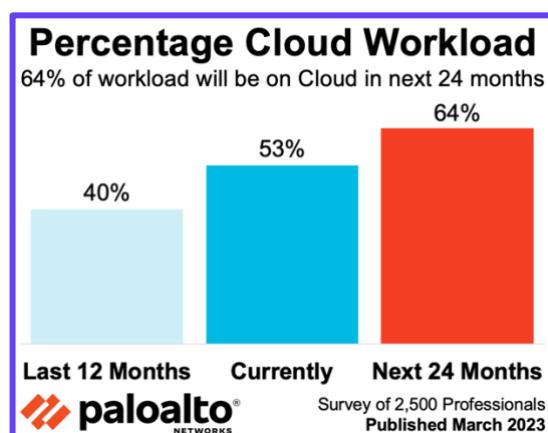
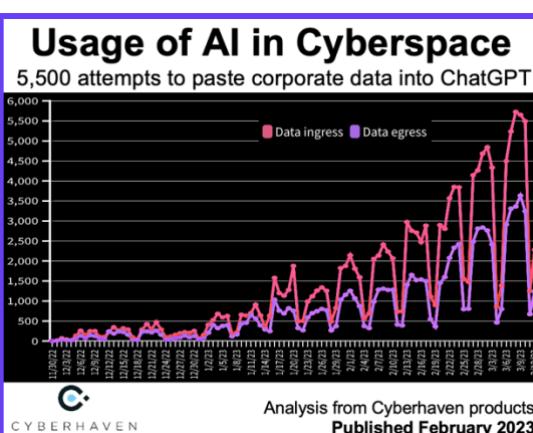
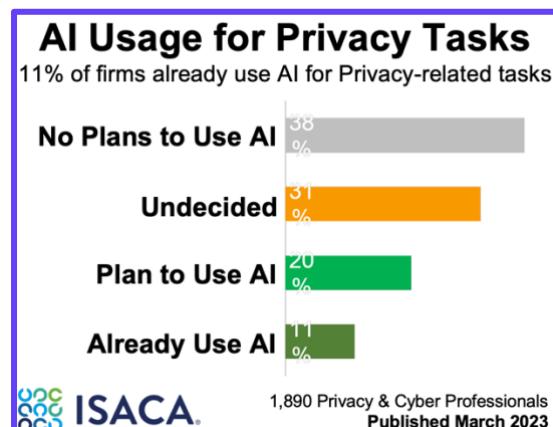
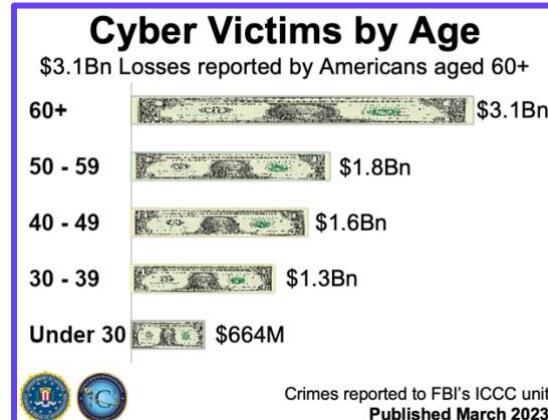
# Cyber Insights: Threats & Breaches

Click each image to see each report in full. All were published in month to April 2023



# Cyber Insights: Cybercrime & Identity

Click each image to see each report in full. All were published in month to April 2023

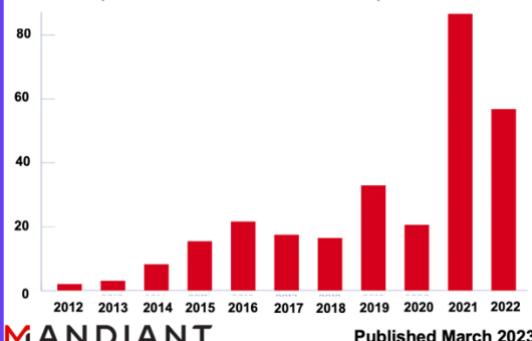


# Cyber Insights: Cyber Challenges & Exploits

Click each image to see each report in full. All were published in month to April 2023

## Zero-Day Exploits each Year

55 surprise new vulnerabilities exploited in '22

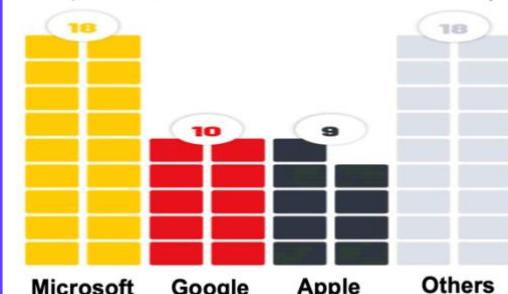


MANDIANT

Published March 2023

## Zero-Day Exploits by Vendor

18 surprise new vulnerabilities at Microsoft this year



MANDIANT

Published March 2023

## Zero-Day Exploit by Country

Chinese Groups lead Exploitation for Espionage



MANDIANT

Published March 2023

## Zero-Day Exploits by Spys

13 surprise new vulnerabilities used for espionage

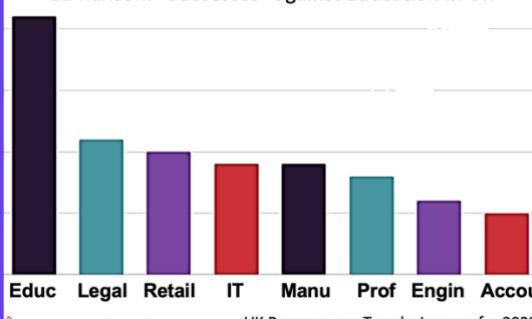


MANDIANT

Published March 2023

## Ransom “Successes” in UK

21 Ransom “Successes” against Education in UK

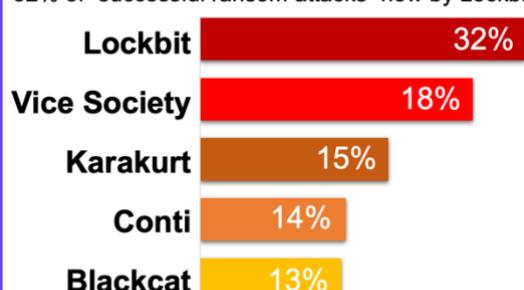


JUMPSEC

UK Ransomware Trends: Lessons for 2023  
Published March 2023

## Ransomware Gangs

32% of “successful ransom attacks” now by Lockbit

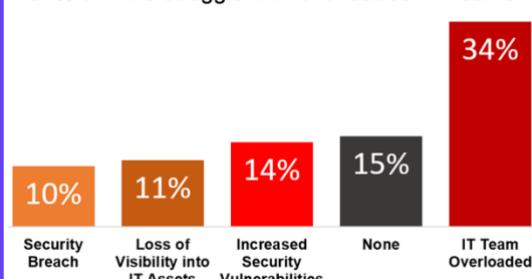


JUMPSEC

UK Ransomware Trends: Lessons for 2023  
Published March 2023

## Cyber Challenges in Firms

34% of firms struggle with overloaded IT Teams



Action1

Survey of 804 IT Professionals  
Published March 2023

## Insights on Cyber Threats

Combat Threats, Boost Cyber Security

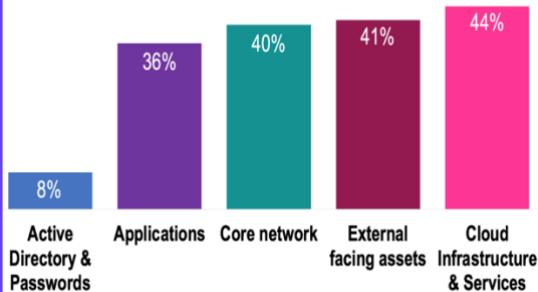


# Cyber Insights: Pen Tests

Click each image to see each report in full. All were published in month to April 2023

## Pen Tests: What's in Scope?

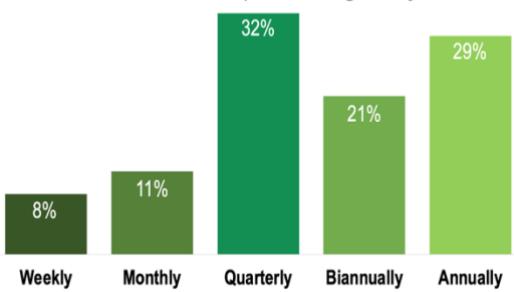
44% of Firms that Test include Cloud Infrastructure



Survey of 300 CISOs  
Published March 2023

## Pen Tests: How Often?

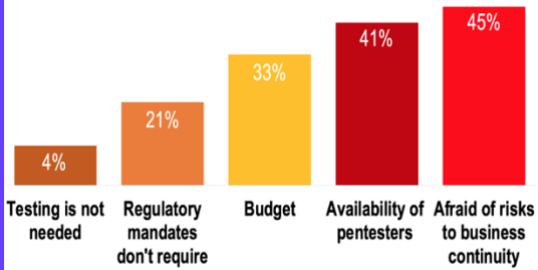
8% of Firms conduct pen-testing every week



Survey of 300 CISOs  
Published March 2023

## Pen Tests: Why not do them?

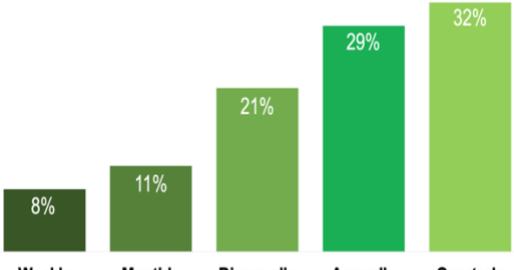
45% of Firms fear Tests will hit Business Continuity



Survey of 300 CISOs  
Published March 2023

## Pen Tests: Why do them?

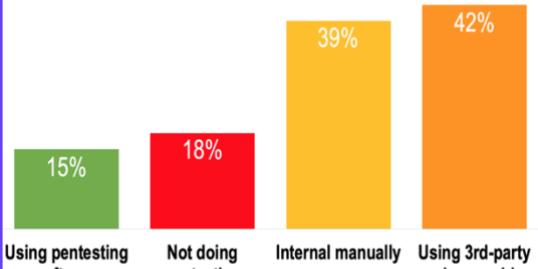
22% of Firms do Tests for Regulatory Compliance



Survey of 300 CISOs  
Published March 2023

## Pen Tests: Who does them?

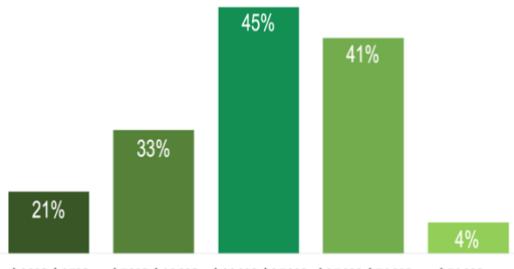
42% of Firms use 3rd Party Pen-testing providers



Survey of 300 CISOs  
Published March 2023

## Pen Tests: Budgets

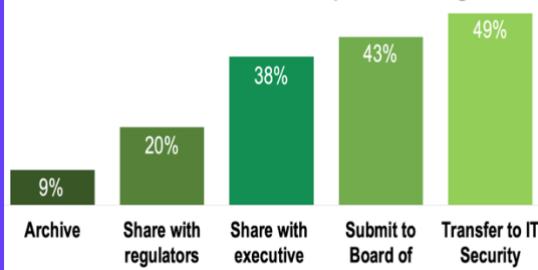
45% say their budget is \$100K - \$250K



Survey of 300 CISOs  
Published March 2023

## Pen Tests: Reporting

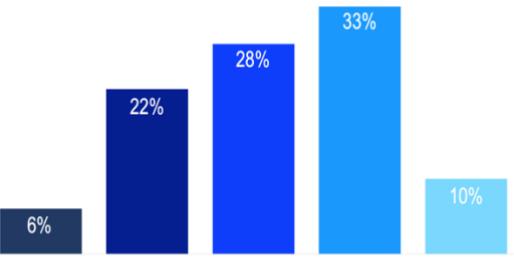
20% of Firms share Pen Test report with Regulators



Survey of 300 CISOs  
Published March 2023

## Cyber Tools: Number / Firm

10% of Firms use more than 75 cyber security tools



Survey of 300 CISOs  
Published March 2023

# Cyber Insights: Rankings in Cyber

Click each image to see each report in full. All were published in month to April 2023

## What Drives Growth of Cloud

Top 5 Reasons for Firms to Expand in the Cloud

- #1 = Expanding Products & Services
- #2 = Increasing Efficiency & Agility
- #3 = Creating new Processes & Workflows
- #4 = Mitigating Business & Regulatory Risk
- #5 = Expanding into New Markets



Survey of 2,500 Professionals  
Published March 2023

## Ensuring Cyber Resilience

Top 5 Practices by Firms to ensure Cyber Resilience

- #1 = Regularly back-up Critical Data
- #2 = Comply with good cyber practices
- #3 = Regularly Patch Software & Apps
- #4 = Regular Penetration Testing
- #5 = Align to Industry Regulations



Survey of 303 Risk & Continuity Leaders  
Published March 2023

## Cyber Security Incidents

Top 5 Cyber Security Incidents

- #1 = Early Risk in App Development
- #2 = Images with Vulnerabilities or Malware
- #3 = Vulnerable Web Apps & APIs
- #4 = Unrestricted Network Access
- #5 = Downtime due to Misconfiguration



Survey of 2,500 Professionals  
Published March 2023

## Cyber Response Planning

Top 5 ways Firms validate Cyber Response Plans

- #1 = Regularly Conduct Exercises
- #2 = Conduct Penetration Tests
- #3 = Run awareness-raising initiatives
- #4 = Outcome Reports & Action Plans
- #5 = Use External Specialists



Survey of 303 Risk & Continuity Leaders  
Published March 2023

## Finance Impersonation

PayPal most impersonated brand in Finance

- #1 = PayPal
- #2 = MTB
- #3 = Crédit Agricole
- #4 = La Banque Postale
- #5 = WellsFargo



Insights from Jan – Dec 2022  
Published March 2023

## Key Cyber Security Metrics

Top 5 Key Cyber Security Metrics

- #1 = Mean Time to Detect
- #2 = Mean Time to Remediate
- #3 = Number of Breaches
- #4 = Number of Intrusion Attempts
- #5 = Unplanned Downtime



Survey of 2,500 Professionals  
Published March 2023

## Top Security Principles

Priorities from Australia's Cyber Security Center

- #1 = Govern, eg manage risks
- #2 = Protect eg create controls
- #3 = Detect
- #4 = Respond

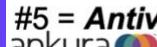


Australian Information Security Manual  
Published February 2023

## Top 5 Myths in Ransomware

Debunking Five Ransomware Misconceptions

- #1 = Sophisticated Hackers to blame
- #2 = Large firms are most targeted
- #3 = Contagion always spreads
- #4 = Paying guarantees data restored
- #5 = Antivirus stops all Ransomware



Published March 2023

# Cyber Insights: Cyber Strategies

Click each image to see each report in full. All were published in month to April 2023

## USA's New Cyber Strategy

Joe Biden announced five pillars in 39 page doc

- #1 = Defend Critical Infrastructure
- #2 = Disrupt & Dismantle Threat Actors
- #3 = Shape Market to Drive Security
- #4 = Invest in a Resilient Future
- #5 = Forge International Partnerships

 39 Page Document, with 27 Strategic Objectives  
Published March 2023

## New Governance Framework

For current EU member states  
Published Feb '23

## National Cyber Strategy for the UK

Published Feb 2023

## Cyber Risk Management by the Saudi Arabia Government

Published March '23

## ACSC InfoSec Manual

Cybersecurity Manual for Australia  
Published March '23

## RAPID Vulnerability Intelligence Report

Published Mar '23

## sosafe Cybercrime Trends

Latest threats & security practices  
Published March '23

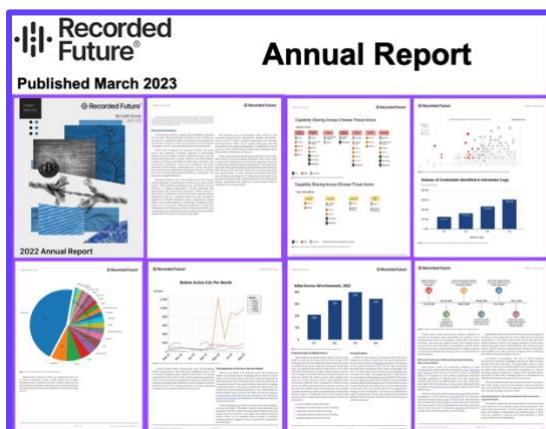
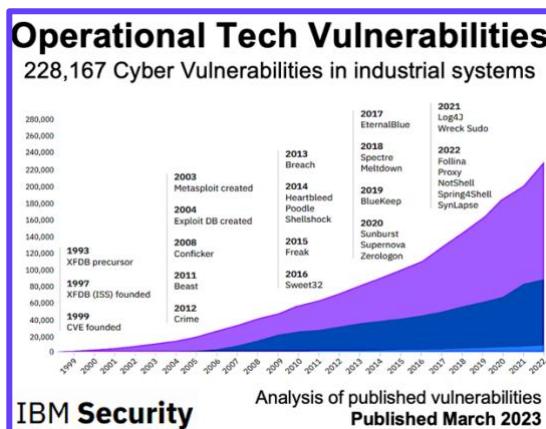
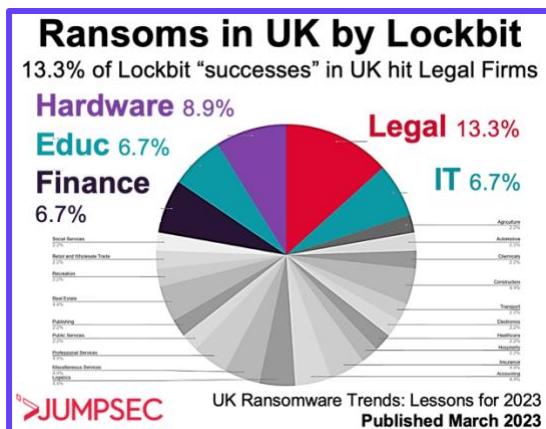
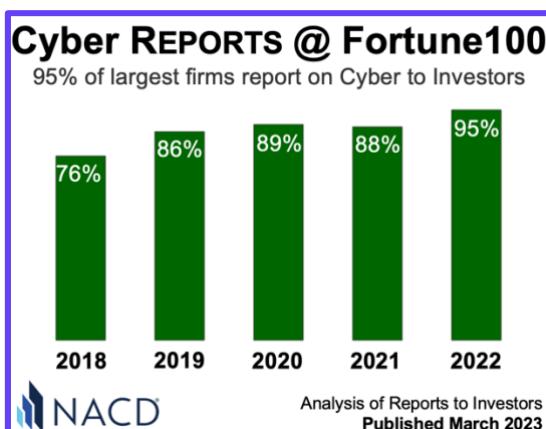
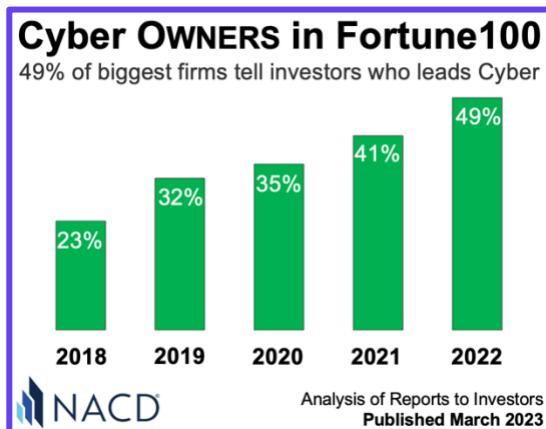
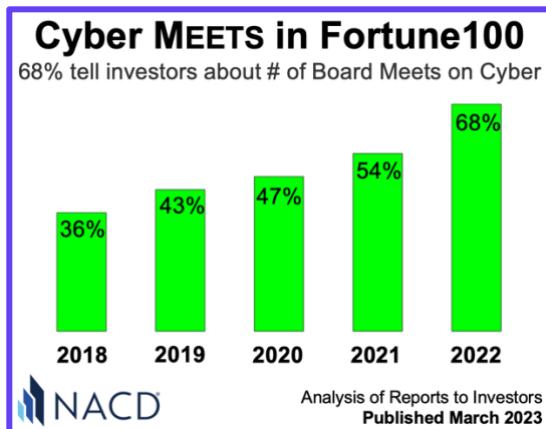
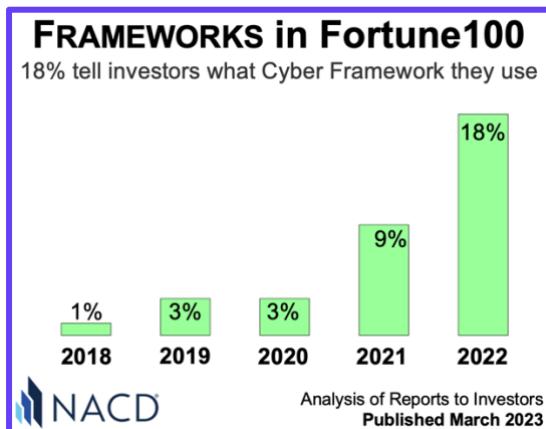
## OECD New Cyber Tools

for Protecting Data and Privacy  
Published March '23



# Cyber Insights: *Reporting on Cyber*

**Click each image** to see each report in full. All were published in month to April 2023

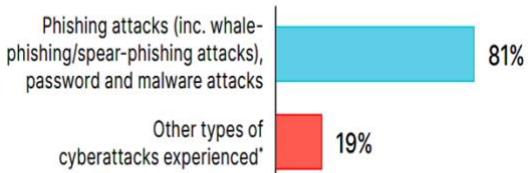


# Cyber Insights: Cyber Skills Gap

Click each image to see each report in full. All were published in month to April 2023

## Frequency of Cyber Attacks

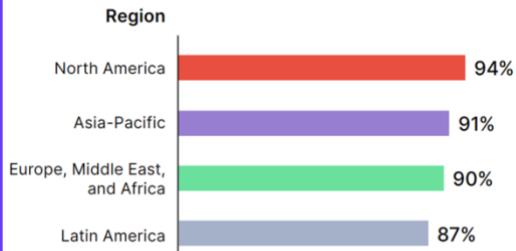
81% of organisations are hit by Phishing attacks



Survey of 1,855 IT Decision Makers  
Published March 2023

## Cyber Certifications

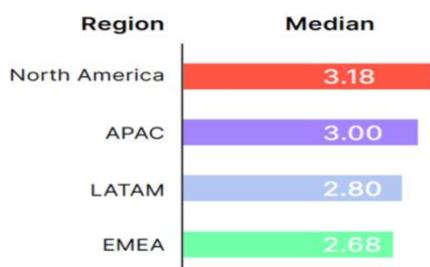
90% of firms prefer Cyber Staff with Certifications



Survey of 1,855 IT Decision Makers  
Published March 2023

## Where Firms Breached Most

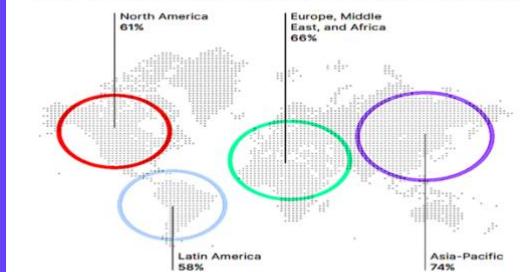
3.18 Breaches per Firm in North America



Survey of 1,855 IT Decision Makers  
Published March 2023

## Cyber Attacks per Firm

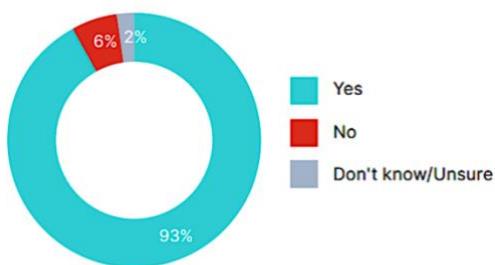
74% of firms in Asia-Pacific have been attacked



Survey of 1,855 IT Decision Makers  
Published March 2023

## Cyber Concerns in Boards

93% of Boards are concerned about Cyber Attacks



Survey of 1,855 IT Decision Makers  
Published March 2023

## Cyber Skills Firms Need

46% of Firms say Cloud Security skills most needed



Survey of 1,855 IT Decision Makers  
Published March 2023

## Cyber Skills left Unfilled

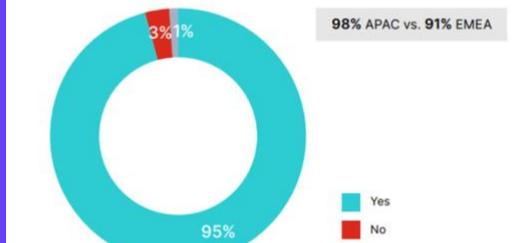
44% of Firms say Cloud Security is hardest to fill



Survey of 1,855 IT Decision Makers  
Published March 2023

## Cyber Certifications

90% of leaders prefer technical cyber certifications



Survey of 1,855 IT Decision Makers  
Published March 2023

# The Best Cyber Insights of 2023

Click each image to see each report in full. All were published in March 2023

### 3rd Party Cyber Attacks

63% of big firms get emails from breached suppliers

Staff Size Category	H2 2022 (%)	H1 2022 (%)	H1 2021 (%)	H1 2020 (%)
> 10,000 Staff	63.14%	61.14%	48.90%	16.60%
5,000 – 10,000	60.01%	53.85%	30.71%	21.74%
500 – 5,000	36.27%	33.09%	23.79%	14.67%
0 – 500 Staff	13.79%	6.22%	6.95%	6.94%

Abnormal

Published February 2023

### 3rd Party Data Breaches

Five 3rd party breaches suffered by typical big firm

Number of Breaches	Count
1 to 99 Staff	1
100 to 999 Staff	1
1,000 to 9,999	2
10,000 or More	5

CyberRisk ALLIANCE

Survey of breaches over last two years

Published February 2023

### 3rd Party Relationship Risks

14% of firms have Suppliers in > 10 countries

Percent of First Parties

Unique Countries in Third Parties

14% of firms have Suppliers in more than 10 countries

Security Scorecard Cyentia

Published February 2022

### 3rd Party Supplier Relations

23% of Suppliers to typical Firms are Prof. Services

Industry	Percentage
Prof. Services	22%
Retail/Wholesale	22.5%
Information	21.2%
Admin/Logistics	15.9%
Manufacturing	5.3%
Finance	2.8%
Hospitality	2.3%
Healthcare	1.5%
Real Estate	1.5%
Construction	1.5%
Public Admin	1.3%

Security Scorecard Cyentia

Published February 2022

### Third-party Ransomware

46% of Hospitals hurt by Ransom on Supplier

Response	2021 (%)	2022 (%)
Unsure	9%	9%
No	55%	45%
Yes	36%	46%

Ponemon INSTITUTE CENSINET

Survey of 579 IT Professionals

Published February 2023

### 3rd Party Breach Costs

1% of firms suffered \$5M cost from such breaches

Breach Cost Category	Percentage
No Costs	27%
<\$100K	38%
\$100K to <\$500K	19%
\$500K to <\$1M	5%
\$1M to \$5M	1%
\$5M or more	1%

CyberRisk ALLIANCE

Survey of 209 Security and IT Experts

Published February 2023

### 3rd Party Risk Management

49% of firms are concerned they lack qualified staff

Concern	Percentage
Lack of qualified staff	49%
Lack of visibility	45%
Insufficient budget	44%
Lack of technology	44%
Lack of 4th party visibility	41%

CyberRisk ALLIANCE

Survey of 209 Security and IT Experts

Published February 2023

### 3rd Party Risk Management

27% of large firms plan "significant" investment

Investment Level	Total (%)	1 to 99 (%)	100 to 999 (%)	1000 to 9999 (%)	> 10000 (%)
No Investment	14%	56%	58%	59%	50%
Limited Investment	23%	31%	21%	24%	21%
Some Investment	56%	13%	14%	5%	2%
Significant Investment	8%	13%	14%	5%	2%

CyberRisk ALLIANCE

Survey of 209 Security and IT Experts

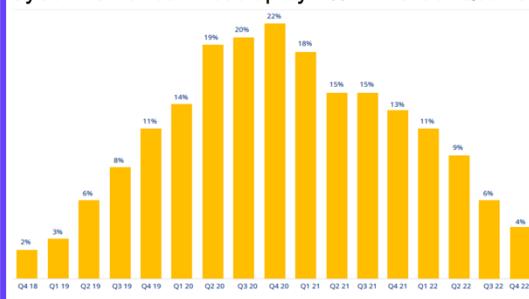
Published February 2023

# The Best Cyber Insights of 2023

Click each image to see each report in full. All were published in March 2023

## Cyber Insurance Inflation

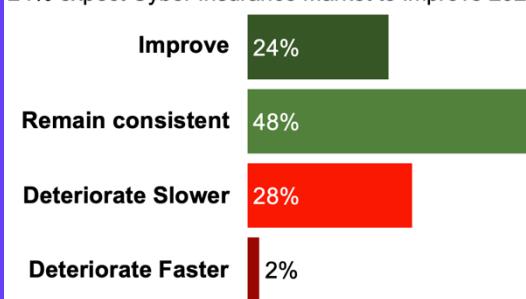
Cyber Insurance Prices up by 4% in the last Quarter



Based on Marsh Specialty & Global Placement  
Published February 2023

## Cyber Insurance Market

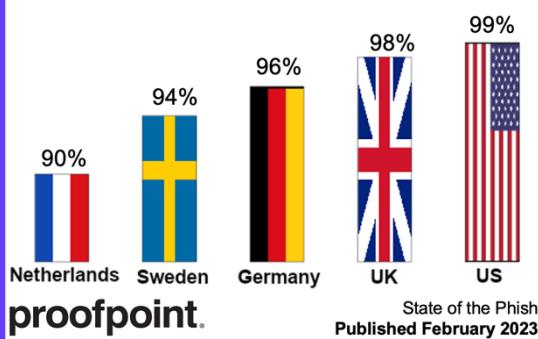
24% expect Cyber Insurance Market to improve 2023



Survey of Airmic members  
Published February 2023

## Cyber Insurance

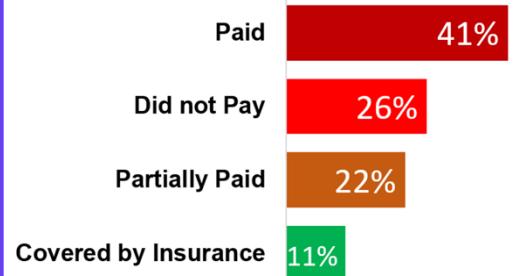
98% of insurers pay Cyber Ransoms in the UK



State of the Phish  
Published February 2023

## Ransom Paid by Insurers?

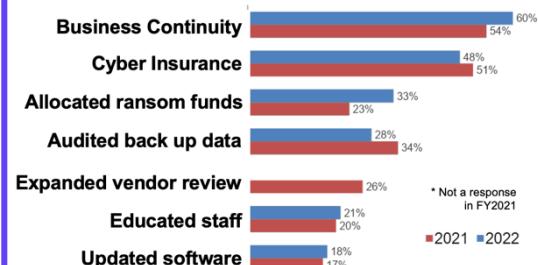
11% of Ransoms are paid by Cyber Insurance



Insights from over 701 experts  
Published February 2023

## Ransom Prep in Hospitals

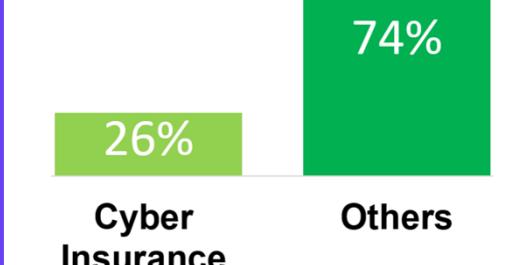
48% of Hospitals prepare with Cyber Insurance



Survey of 579 IT Professionals  
Published February 2023

## Risk Management Drivers

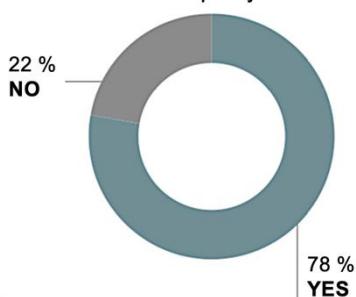
26% of firms use Cyber Insurance as a strategy



Insights from over 701 experts  
Published February 2023

## Cyber Insurance Risk

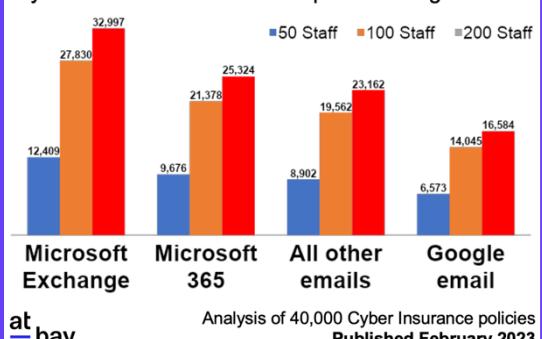
78% of Insurers consider quality of Risk Management



Survey of Airmic members  
Published February 2023

## Cost to Insure Email Services

Cyber Insurance is 50% cheaper for Google clients



# The Best Cyber Insights of 2023

Click each image to see each report in full. All were published in March 2023

### Cyber Security Budgets

39% of Firms increasing by >10%, vs 51% last year

Category	2022 (%)	2023 (%)
Decrease	15%	16%
Unchanged	12%	13%
+1% to +5%	18%	23%
+6% to +10%	25%	20%
11% or more	26%	19%

Data from 2023 Global Digital Trust Insights  
Published February 2023

### IT Security Budgets

Increased complexity of IT Infrastructure at 54%

Category	Percentage
New locations of business	23%
Compliance/Legal requirements	29%
Increased profits	30%
Improve level of security expertise	45%
Increased complexity of IT infrastructure	54%

kaspersky  
Published February 2023

### Risk Budget Less Prioritised

Risk Management Budget prioritized by Hospitals

Category	2021 (%)	2022 (%)
Unsure	5%	6%
No	45%	51%
Yes	50%	43%

Survey of 579 IT Professionals  
Published February 2023

### Privacy Spending by Firms

\$3.6m typical spend on Privacy by largest firms

Size (Number of Employees)	2019 (\$M)	2020 (\$M)	2021 (\$M)	2022 (\$M)
50-249	1.1	1.5	1.7	2.0
250-499	0.8	1.6	2.1	2.1
500-999	1.2	2.0	2.3	2.6
1,000-9,999	1.3	2.8	3.0	2.8
10,000+	1.9	3.7	3.5	3.6

CISCO  
Survey of 4,700 Security Professionals  
Published February 2023

### Cyber Budgets & SOCs

\$2M budget for Enterprises with Security Ops Centre

Revenue Category	Without SOC (\$)	With SOC (\$)
SMB (\$10M Revenue)	\$225,000	\$450,000
SMB (\$50M Revenue)	\$500,000	\$750,000
Enterprise (\$100M Revenue)	\$1,500,000	\$2,000,000

Data from Boardish Clients  
Published February 2023

### CFOs plan to invest in Cyber

39% of CFOs plan to invest in Cyber Tech Solutions

Investment Plan	Percentage
Invest in Cybersecurity Tech	39%
Focus on Operations Tech	37%
Upskill & Hire Talent	36%
Focus on GRC	33%
Cyber with Business Focus	27%

pwc  
Survey of 326 CFOs  
Published February 2023

### Cyber Budgeting Problems

Legacy Budgets make it hard to budget well for future

- #1 = Legacy Budget Structures
- #2 = Lack of Verification  
if expense tracking done internally
- #3 = Lack of Visibility on Resources

Boardish  
Data from Boardish Clients  
Published February 2023

### Typical Ransom Payments

Median Ransom actually paid is about \$180,000

Quarter	Average Ransom Payment (\$)	Median Ransom Payment (\$)
Q3 2018	~\$10,000	~\$5,000
Q4 2018	~\$15,000	~\$10,000
Q1 2019	~\$20,000	~\$15,000
Q2 2019	~\$30,000	~\$20,000
Q3 2019	~\$40,000	~\$25,000
Q4 2019	~\$50,000	~\$30,000
Q1 2020	~\$60,000	~\$35,000
Q2 2020	~\$80,000	~\$40,000
Q3 2020	~\$100,000	~\$50,000
Q4 2020	~\$120,000	~\$60,000
Q1 2021	~\$150,000	~\$70,000
Q2 2021	~\$180,000	~\$80,000
Q3 2021	~\$200,000	~\$90,000
Q4 2021	~\$220,000	~\$100,000
Q1 2022	~\$250,000	~\$120,000
Q2 2022	~\$280,000	~\$140,000
Q3 2022	~\$300,000	~\$160,000
Q4 2022	~\$350,000	~\$180,000

COVWARE  
Published February 2023

# The Best Cyber Insights of 2023

Click each image to see each report in full. All were published in March 2023

## Ransom Payments Escalate

Size of each known payment +58% from Q3/22



Average (Mean)  
Known Payout =

**USD \$408,644**

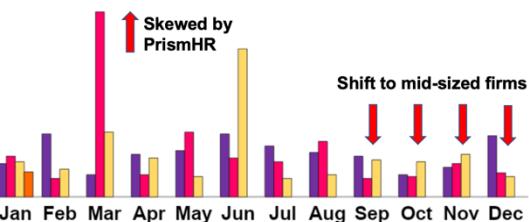


Published February 2023

## Size of Ransom Victims

Ransom Gangs keep targeting smaller sized firms

■ 2020 ■ 2021 ■ 2022 ■ 2023

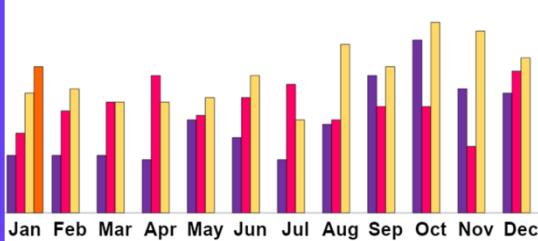


Published February 2023

## # of “Successful” Ransoms

The highest number of attacks in January on record

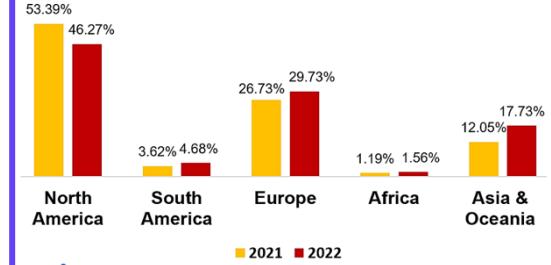
■ 2020 ■ 2021 ■ 2022 ■ 2023



Published February 2023

## Ransom Attacks by Region

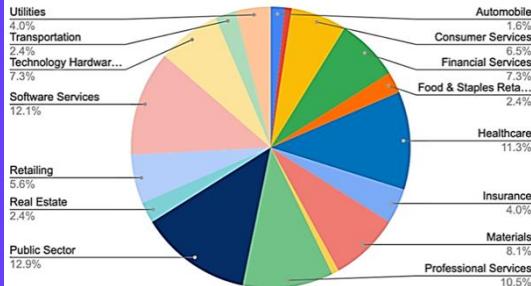
46% of Ransom attacks observed in North America



Extracted Attacks from the Dark Web analysis  
Published February 2023

## Ransom Attacks by Sector

Public Sector organizations hit most frequently



Published February 2023

## Ransom Victims by Sector

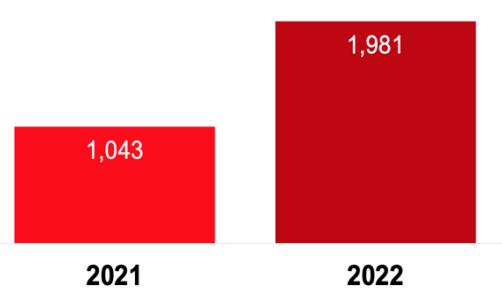
Education records the most incidents this month



Published February 2023

## Ransomware Impact

Increase in ransomware for Education in 2022



Published February 2023

## Top Ransomware Variants

Hive is now the most common ransom variant

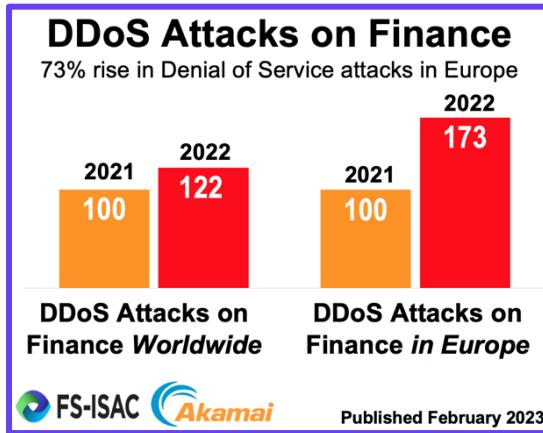
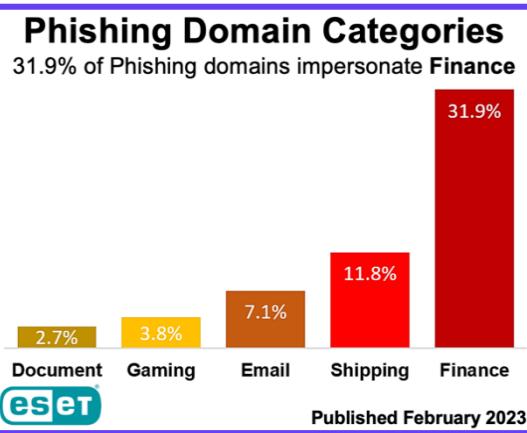
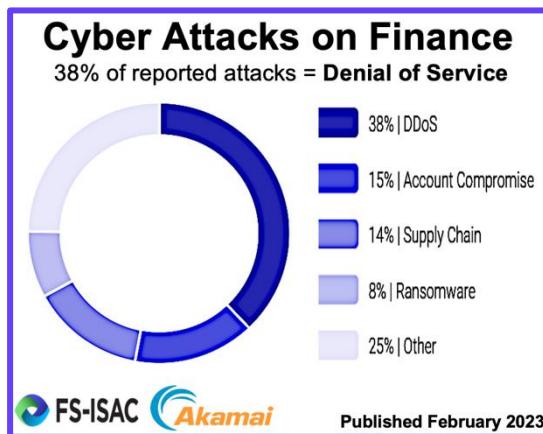
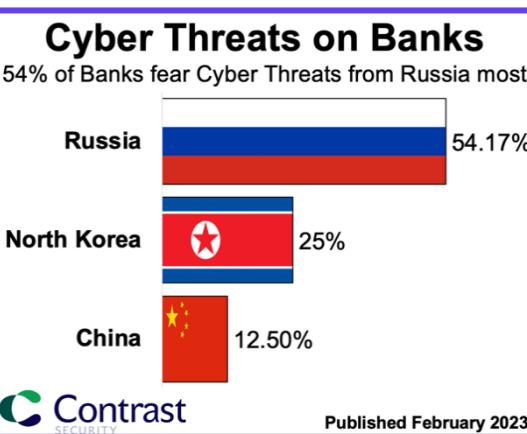
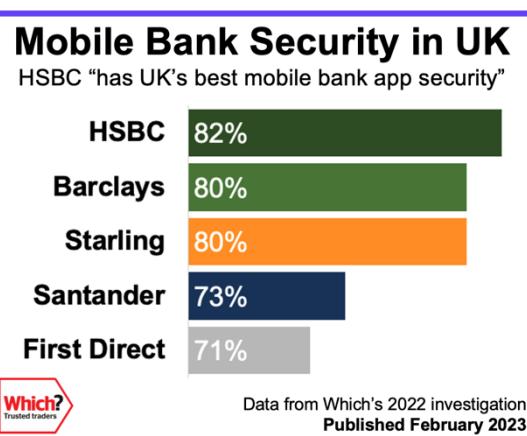
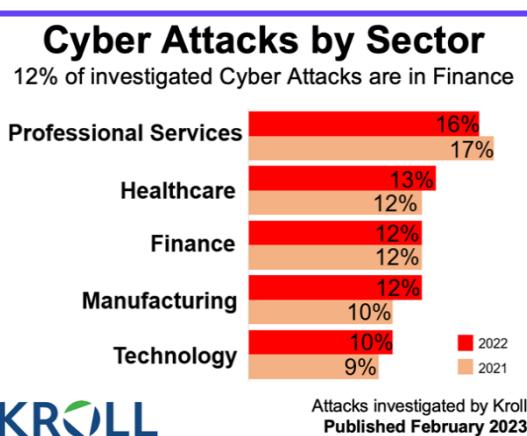
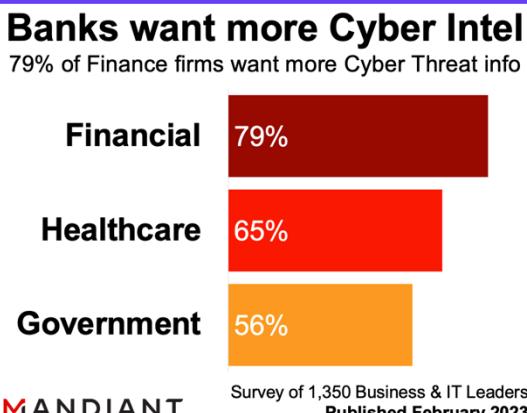
Rank	Ransomware Type	Market Share %
1	Hive	13.8%
2	Black Basta	12.2%
3	BlackCat	10.6%
4	Royal	8.9%
5	Phobos	6.5%
6	Quantum	4.8%
7	Diavol	3.2%
7	Lockbit 3.0	3.2%



Published February 2023

# The Best Cyber Insights of 2023

Click each image to see each report in full. All were published in March 2023

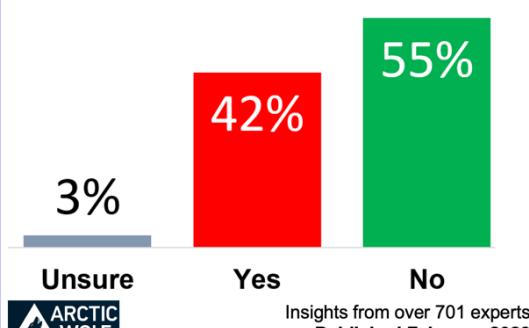


# The Best Cyber Insights of 2023

Click each image to see each report in full. All were published in March 2023

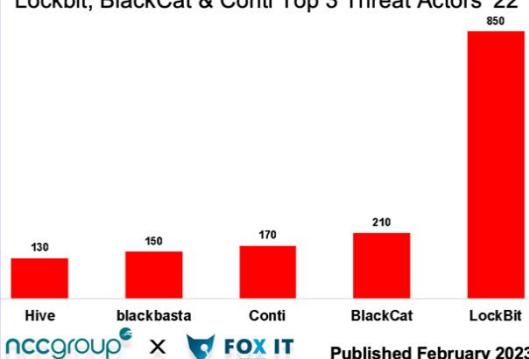
## Ransomware Attack Trends

42% of firms suffered a ransomware attack in 2022



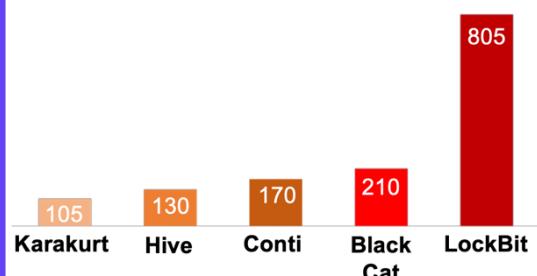
## Ransomware Threat Landscape

Lockbit, BlackCat & Conti Top 3 Threat Actors '22



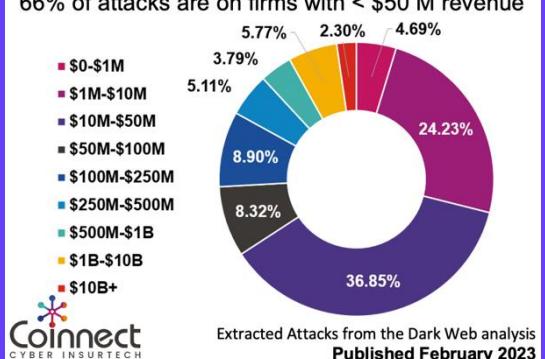
## "Successful" Ransom Gangs

805 known victims of Lockbit Ransomware in 2022



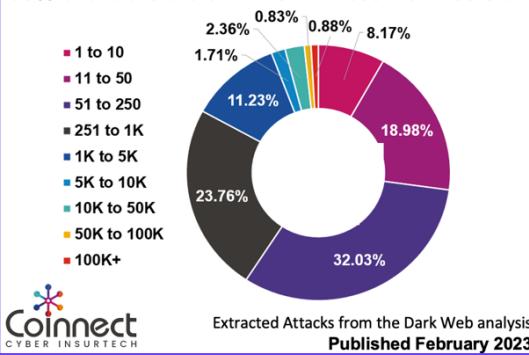
## Ransom by size of Firm

66% of attacks are on firms with < \$50 M revenue



## Ransom by size of Firm

59% of attacks are on firms with less than 250 staff



## Most Prolific Ransom Gangs

LockBit lists 1,320 victims on its extortion site

### LockBit

1,320

### Conti

880

### Pysa

300

### REvil

280

### Maze

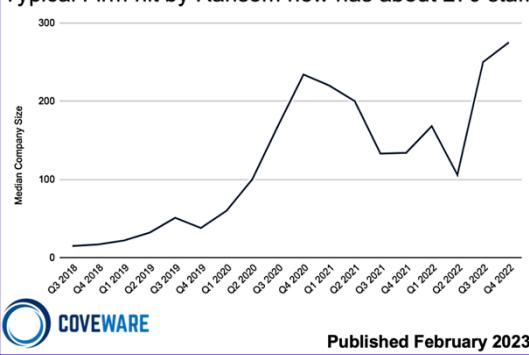
250

The Record.  
Recorded Future News

Data collected by Recorded Future  
Published February 2023

## Size of Firms hit by Ransom

Typical Firm hit by Ransom now has about 270 staff



## Top Ransom Gang

LockBit was most active Ransom Gang in last year

#1 = LockBit

#2 = BlackCat

#3 = Conti

#4 = Black Basta

#5 = Hive

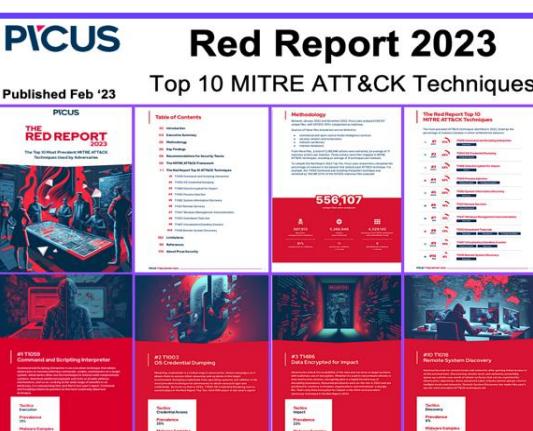
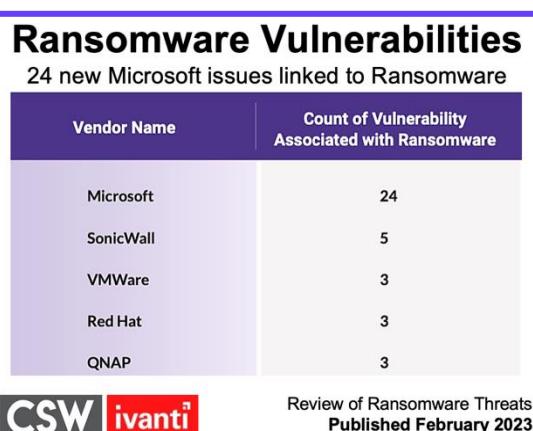
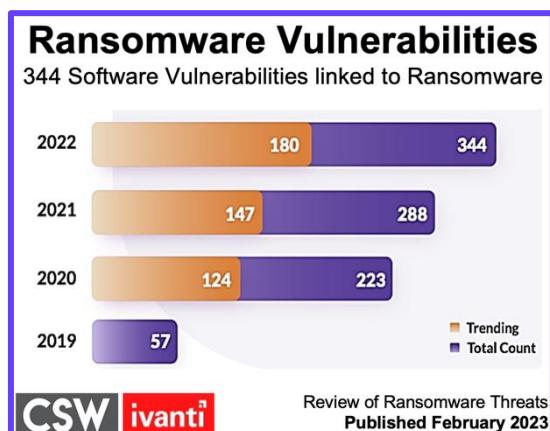
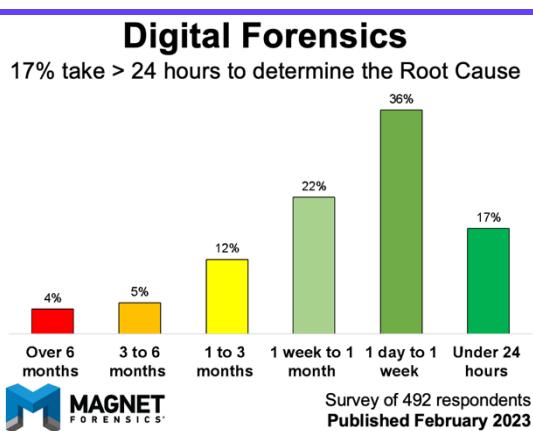
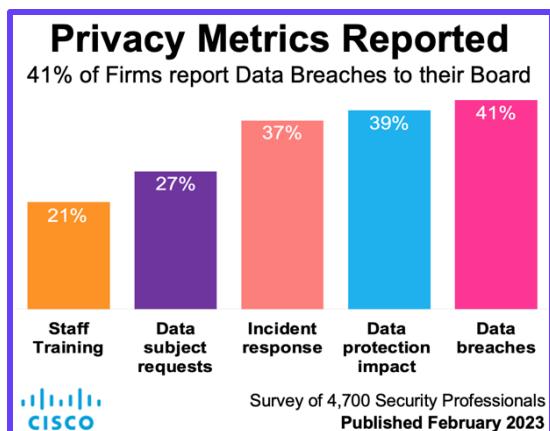
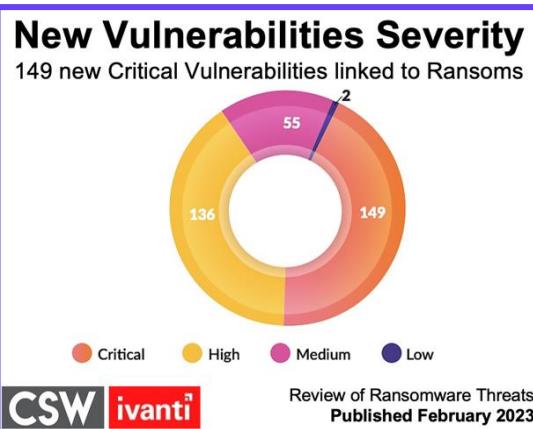
Coinnect CYBER INSURTECH

Extracted Attacks from the Dark Web analysis  
Published February 2023



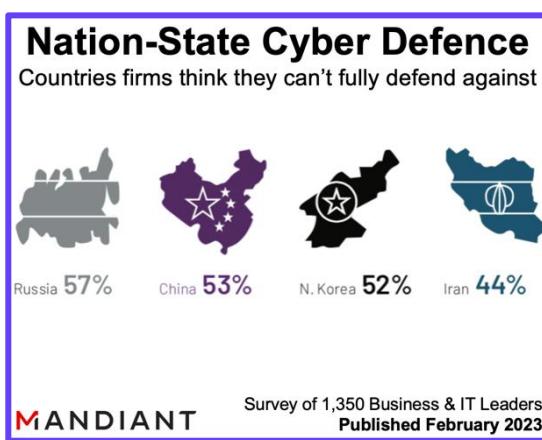
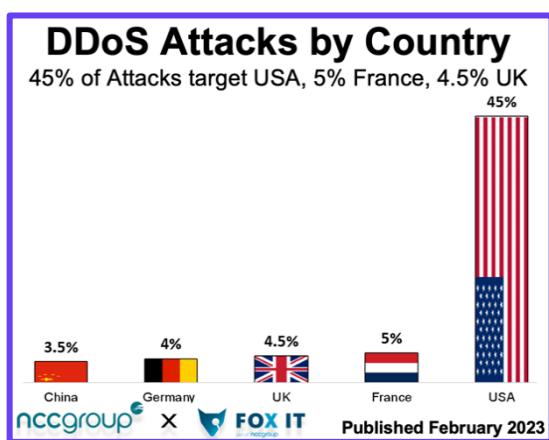
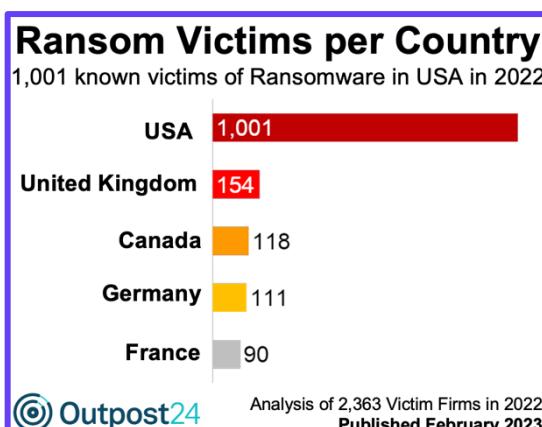
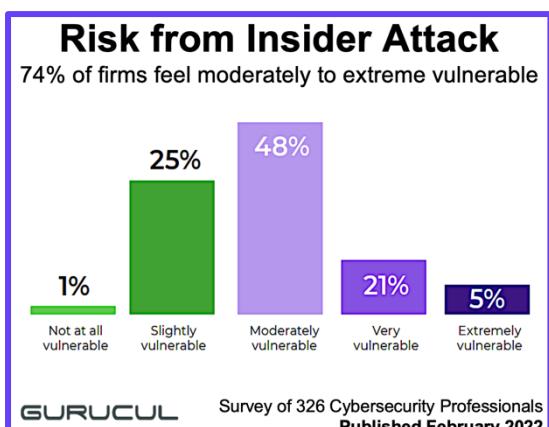
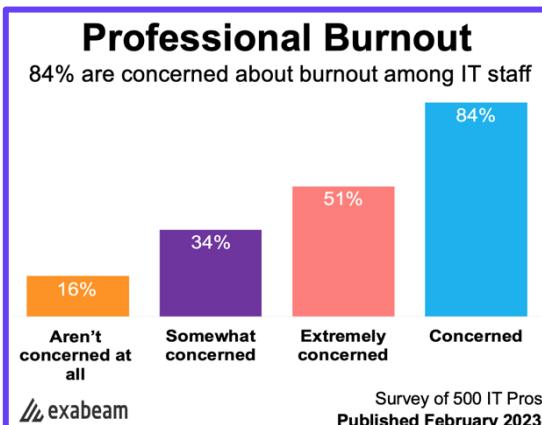
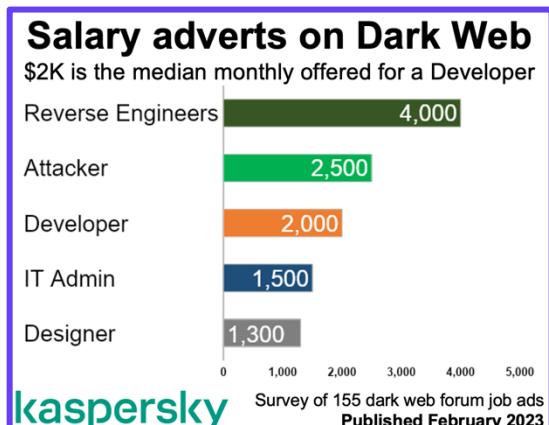
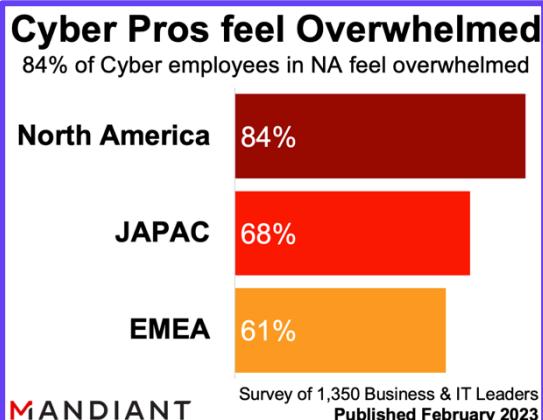
# The Best Cyber Insights of 2023

**Click each image** to see each report in full. All were published in March 2023



# The Best Cyber Insights of 2023

Click each image to see each report in full. All were published in March 2023



# The Best Cyber Insights of 2023

Click each image to see each report in full. All were published in March 2023

### Trends in Cyber Attacks

60% of FIs hit by Destructive Attacks last year

Application Attacks	64%
Watering-hole Attacks	60%
Destructive Attacks	60%

**Contrast SECURITY**

Published February 2023

### Frequency of Cyber Attacks

10% suffer Data Exfiltration attacks Very Frequently

Attack Type	Very Frequently (%)	Somewhat Frequently (%)
Data Exfiltration or IP Theft	10%	25%
BEC Scams	14%	20%
Employee Misconduct	10%	23%
Misuse of Assets or Policy Violations	9%	21%
Internal Fraud	11%	18%
Ransomware	8%	20%

**MAGNET FORENSICS**

Survey of 492 respondents  
Published February 2023

### Data Breaches Reported

512 Data Breaches reported in USA in Q4 of 2022

Period	Number of Breaches
Jan to Mar	404
Apr to Jun	413
Jul to Sep	473
Oct to Dec	512

**ITRC | IDENTITY THEFT RESOURCE CENTER**

Review of all breach reports in USA  
Published February 2023

### Breaches Reported in USA

1,802 breaches reported by firms in USA in 2022

Year	Number of Breaches
2018	1,175
2019	1,279
2020	1,108
2021	1,862
2022	1,802

**ITRC | IDENTITY THEFT RESOURCE CENTER**

Review of all breach reports in USA  
Published February 2023

### Compromised Cloud Credentials

Long-term credentials most compromised at 75%

Credential Type	Percentage
Console Credentials	25%
Long-term Access	75%

**expel**

Insights from Jan – Dec 2022  
Published February 2023

### Ransomware Threat Landscape

800 Ransom "Successes" at Industrial Firms in '22

Industry Sector	2021	2022
Industrials	890	800
Consumer Cyclicals	440	490
Technology	280	270
Healthcare	190	180
Basic Materials	180	170

**nccgroup** x **FOX IT**

Published February 2023

### Less Info about Breaches

Only 58% of breach reports include details of attack

Year	Percentage
2018	98%
2019	100%
2020	100%
2021	93%
2022	58%

**ITRC | IDENTITY THEFT RESOURCE CENTER**

Review of all breach reports in USA  
Published February 2023

### Less Info about Breaches

Only 34% of reports give detail on attack & victims

Year	Percentage
2018	58%
2019	72%
2020	60%
2021	58%
2022	34%

**ITRC | IDENTITY THEFT RESOURCE CENTER**

Review of all breach reports in USA  
Published February 2023

# The Best Cyber Insights of 2023

Click each image to see each report in full. All were published in March 2023

## Cybersecurity Discussions

Leaders discuss Cyber with investors every 7 weeks



**MANDIANT**

Survey of 1,350 Business & IT Leaders  
Published February 2023

## Cybersecurity Data Sources

56% of firms use ISACs to follow Threat Landscape

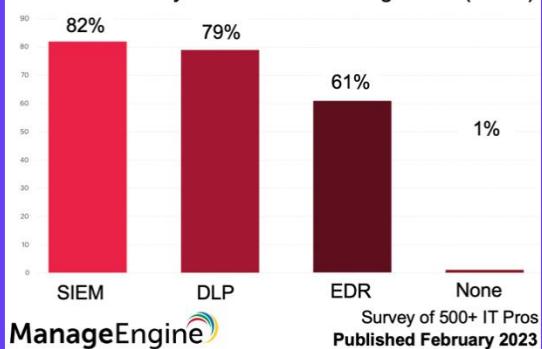


**MANDIANT**

Survey of 1,350 Business & IT Leaders  
Published February 2023

## Use of Security Solutions

82% use Security Info & Event Management (SIEM)

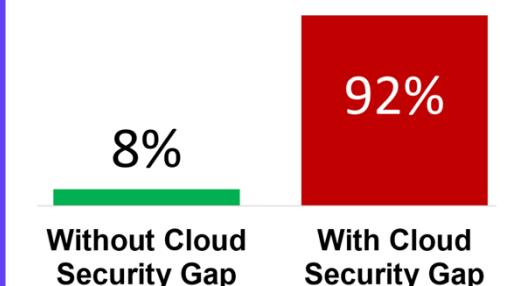


**ManageEngine**

Survey of 500+ IT Pros  
Published February 2023

## Cloud Security

92% of firms have an active Cloud Security Gap

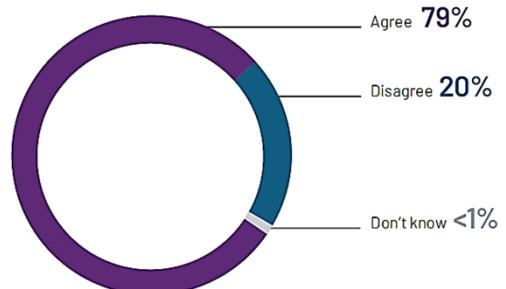


**ARCTIC WOLF**

Insights from over 701 experts  
Published February 2023

## Cyber Security Focus

79% of Leaders feel they can focus more on threats

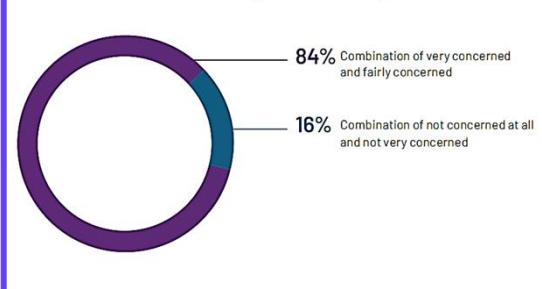


**MANDIANT**

Survey of 1,350 business and IT leaders  
Published February 2023

## Cyber Security Data Alerts

84% of Leaders feel they are missing out on threats

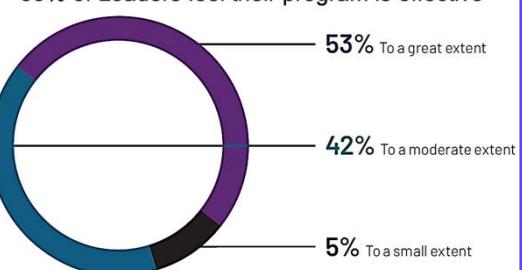


**MANDIANT**

Survey of 1,350 business and IT leaders  
Published February 2023

## Cyber Security Confidence

53% of Leaders feel their program is effective



**MANDIANT**

Survey of 1,350 business and IT leaders  
Published February 2023

## Cyber Security Pros & Stress

43% worry about "inability to prevent bad things"



**exabeam**

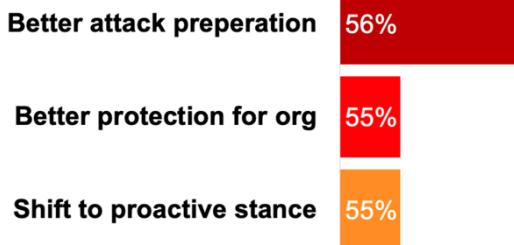
Survey of 500 IT Pros  
Published February 2023

# The Best Cyber Insights of 2023

Click each image to see each report in full. All were published in March 2023

## Threat Actor Understanding

Importance of understanding threats targeting you

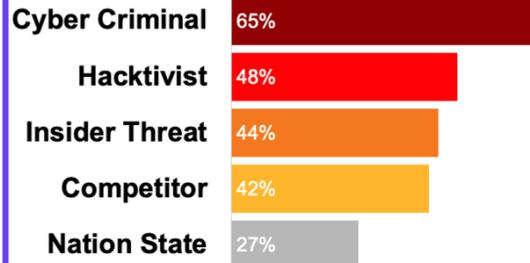


**MANDIANT**

Survey of 1,350 Business & IT Leaders  
Published February 2023

## Cyber Threat Actors in 2023

65% think cyber criminals will significantly affect them

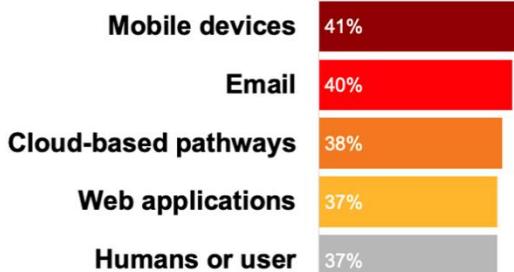


**pwc**

Survey of 3,552 C-Suite Execs  
Published February 2023

## Pathways for Cyber Attacks

41% think threats via Mobile Devices will affect them

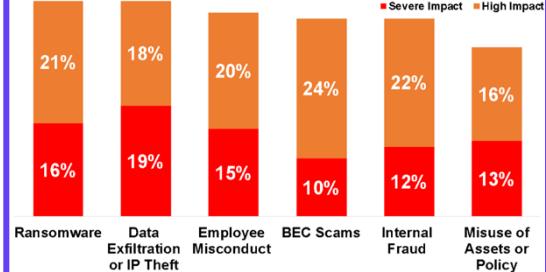


**pwc**

Survey of 3,552 C-Suite Execs  
Published February 2023

## Impact of Cyber Attacks

16% suffer Ransomware attacks with severe impact

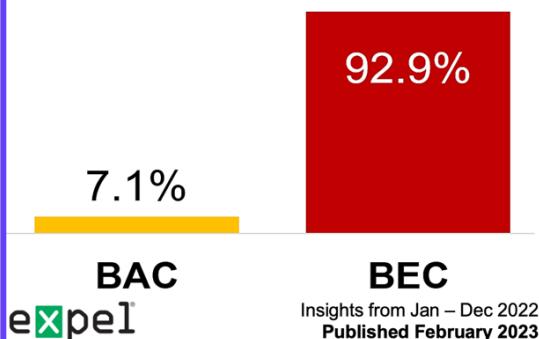


**MAGNET FORENSICS**

Survey of 492 respondents  
Published February 2023

## Business Email Compromise

BECs highest threat at 92.9%

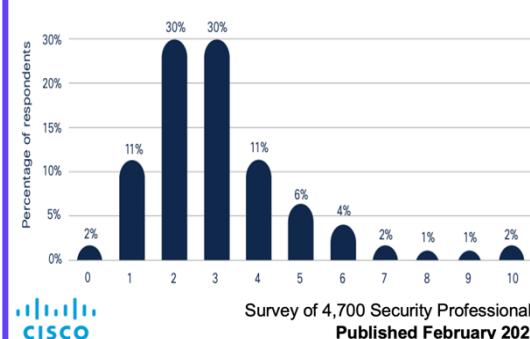


**expel**

Insights from Jan – Dec 2022  
Published February 2023

## Privacy Metrics Reported

2% of Firms report 10(!) privacy metrics to Board



**CISCO**

Survey of 4,700 Security Professionals  
Published February 2023

## Impact of Email Threats

98% of firms are not prepared to deal with risks



**Barracuda**

Survey of 1,350 IT Staff  
Published February 2023

## Ransomware Vulnerabilities

152 Microsoft issues are linked to Ransomware

Vendor	Vulnerability Count
Microsoft	152
Red Hat	89
Novell	82
Gentoo	73
Oracle	61

**CSW ivanti**

Review of Ransomware Threats  
Published February 2023

# The Best Cyber Insights of 2023

Click each image to see each report in full. All were published in March 2023

### TPRM: Prioritisation

15% of Firms with 10K staff say it's a Critical Priority

Firm Size	Not a priority	Low priority	Moderate priority	High priority	Critical priority
1 to 99	19%	44%	25%	13%	
100 to 999	2%	38%	35%	2%	
1000 to 9999	5%	25%	48%	1%	
> 10000	15%	44%	30%	11%	

**CyberRisk ALLIANCE** Survey of 209 Security and IT Experts Published February 2023

### 3rd Party Attack Assessment

21% of firms can assess attacks in several hours

Time to Assess	Percentage
Within several hours	21%
1 to 6 days	45%
1 to 2 weeks	10%
More than 2 weeks	10%
Don't know	14%

**CyberRisk ALLIANCE** Survey of 209 Security and IT Experts Published February 2023

### 3rd Party Breach Effects

31% of Firms hit by Outage caused by a 3rd Party

Effect	Percentage
Network Outage	31%
Service Disruption	26%
Business Disruption	27%
Data Theft	24%
Nothing	21%
Financial Loss	20%

**CyberRisk ALLIANCE** Survey of breaches over last two years Published February 2023

### 3rd Party Risk Management

20% say it has become much more important

Importance	Percentage
Much more important	20%
Somewhat important	48%
No change	26%
Less important	5%
Much less important	1%

**CyberRisk ALLIANCE** Survey of 209 Security and IT Experts Published February 2023

### Sectors Cyber Overwhelms

91% of Cyber Gov employees feel overwhelmed

Sector	Percentage
Government	91%
Healthcare	79%
Retail/Hospitality	71%
Financial Services	69%
Manufacturing	64%

**MANDIANT** Survey of 1,350 Business & IT Leaders Published February 2023

### Email Compromise Attacks

16% of Transport staff Reply to "BEC" Email Attacks

Industry	Percentage
Transportation	16.07%
Automotive	9.42%
Healthcare	8.22%
Infrastructure	7.74%
Retail	6.16%

**Abnormal** Published February 2023

### Ransomware Threat Landscape

269 known Ransom "Hack & Leak" Victims in 12/22

Month	Victims
Jan-21	127
Feb-21	190
Mar-21	200
Apr-21	230
May-21	225
Jun-21	220
Jul-21	155
Aug-21	300
Sep-21	310
Oct-21	324
Nov-21	180
Dec-21	180
Jan-22	120
Feb-22	280
Mar-22	289
Apr-22	225
May-22	200
Jun-22	140
Jul-22	159
Aug-22	210
Sep-22	190
Oct-22	260
Nov-22	269

**nccgroup X FOX IT** Published February 2023

### Causes of 3rd Party Breaches

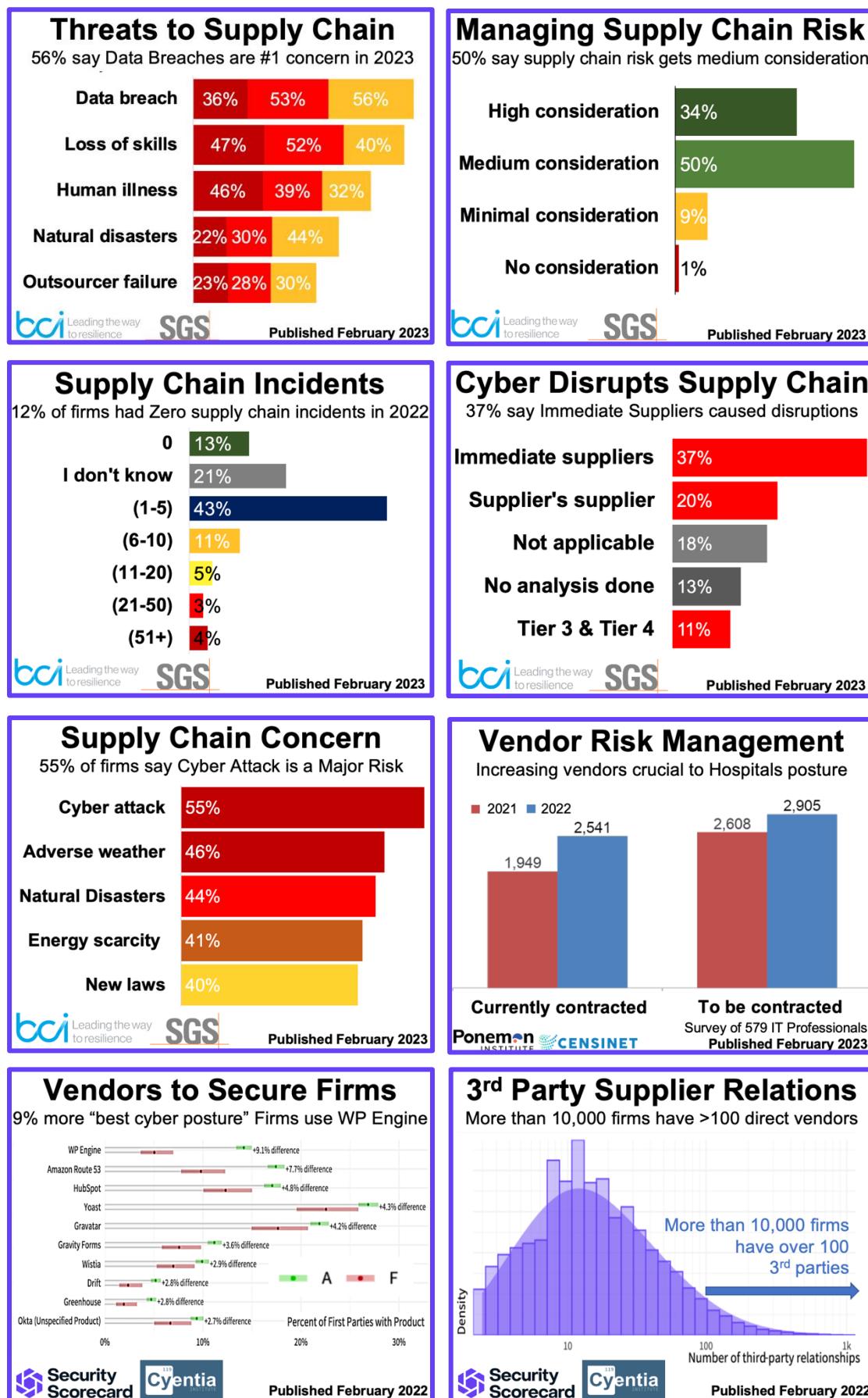
27% of reported 3rd Party Breaches = Ransomware

Cause	Percentage
Ransomware	27%
Unauthorized Network Access	39.7%
Unsecured Servers	10%
Other	8%
Human Error	6%
Phishing	3%
Malware	3%

**BLACK KITE** Published February 2023

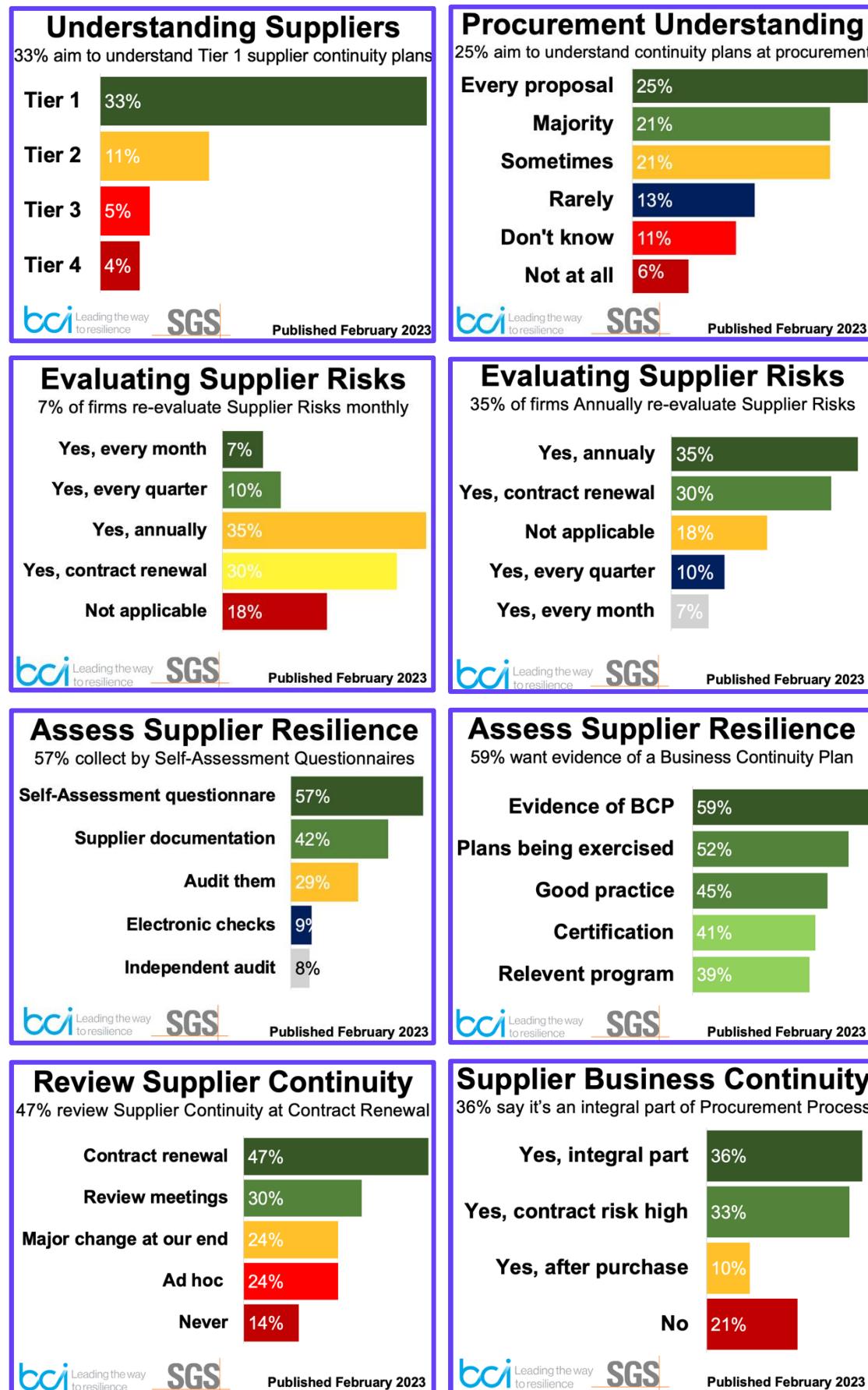
# The Best Cyber Insights of 2023

Click each image to see each report in full. All were published in March 2023



# The Best Cyber Insights of 2023

Click each image to see each report in full. All were published in March 2023



# The Best Cyber Insights of 2023

Click each image to see each report in full. All were published in March 2023

## Why Insider Threats are Up

54% of insiders already have credential access



**54%**

Insiders already have credentialled access to the network and services



**44%**

Increased use of applications that can leak data (e.g., Web email, DropBox, social media)



**42%**

Personal device access to corporate resources

GURUCUL

Survey of 326 Cybersecurity Professionals  
Published February 2022

## Causes of Data Breach

71% of firms fear Compromised Accounts the most



**71%**

Compromised accounts/machines (i.e., user system taken over without knowledge)



**64%**

Negligent data breach (i.e., user willfully ignoring policy, but not malicious)



**66%**

Inadvertent data breach/leak (i.e., user unknowingly violates policy without malicious intent)



**54%**

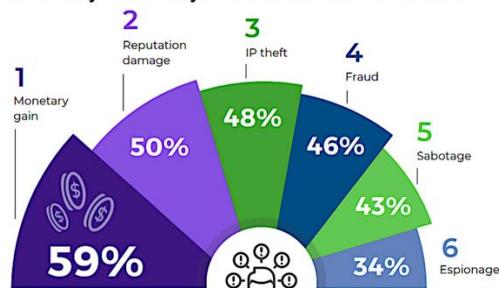
Malicious data breach (i.e., user willfully causing harm)

GURUCUL

Survey of 326 Cybersecurity Professionals  
Published February 2022

## Motivations of Insider Attack

59% say Monetary Gain is the main motivation

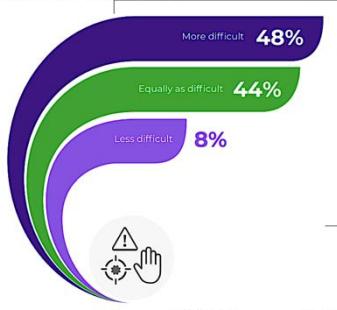


GURUCUL

Survey of 326 Cybersecurity Professionals  
Published February 2022

## Internal vs External Threats

48% say "Internal threats are more difficult to detect"



GURUCUL

Survey of 326 Cybersecurity Professionals  
Published February 2022

## Frequency of Insider Attacks

74% of Firms say Insider Attacks now more frequent

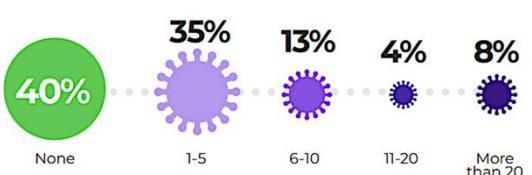


GURUCUL

Survey of 326 Cybersecurity Professionals  
Published February 2022

## Frequency of Insider Attacks

40% of Firms report zero Insider Attacks in last year



GURUCUL

Survey of 326 Cybersecurity Professionals  
Published February 2022

## Top Impact of Insider Attacks

#1 impact of Insider Attacks is "Loss of Critical Data"

- #1 = Loss of Critical Data
- #2 = Brand Damage
- #3 = Operation disruption
- #4 = Loss in Revenue
- #5 = Legal Liabilities

GURUCUL

Survey of 326 Cybersecurity Professionals  
Published February 2022

## Ransomware Software

7 Advanced Threat Groups (APTs) use Maze code

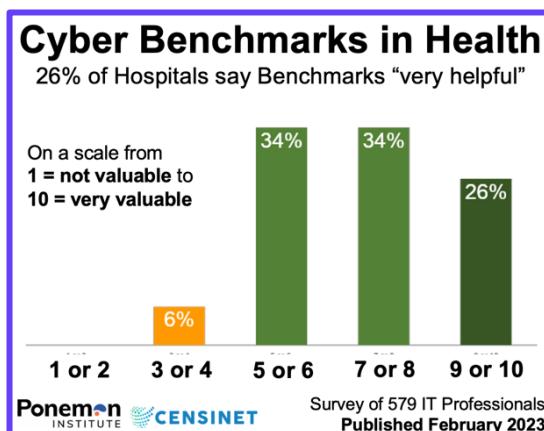
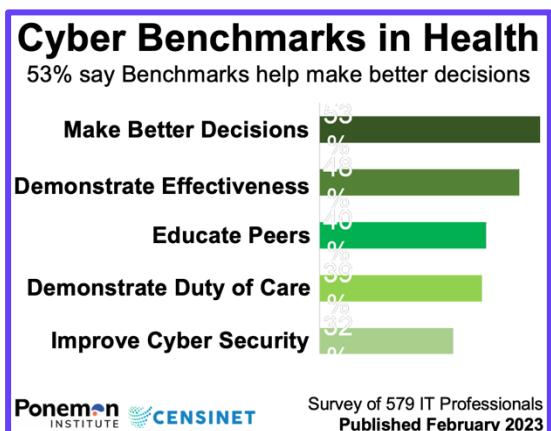
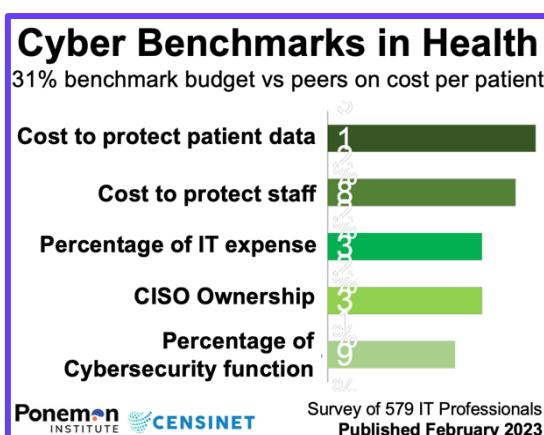
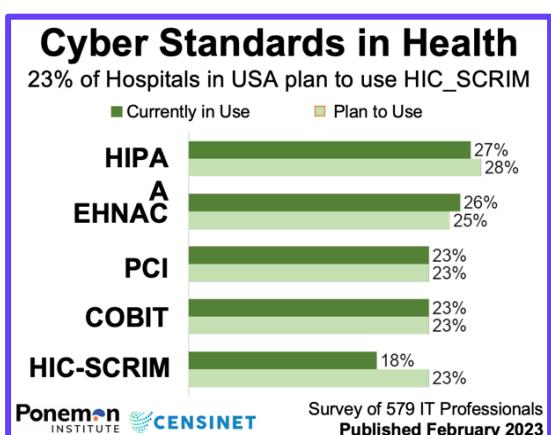
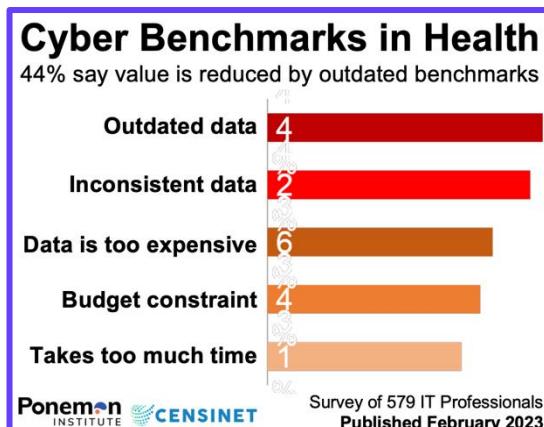
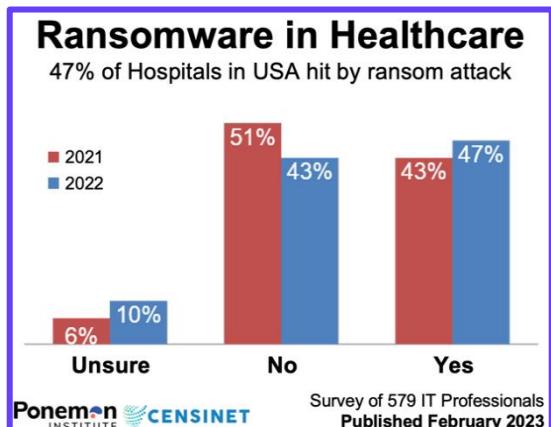
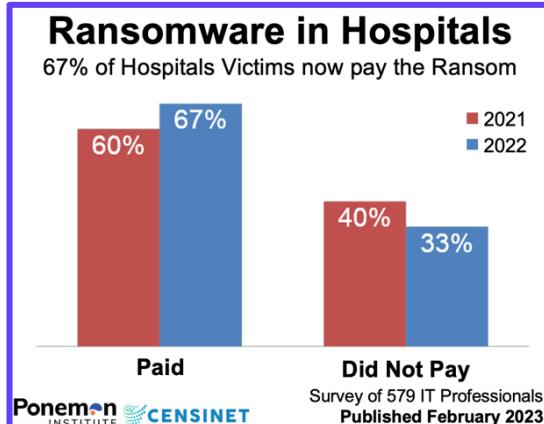
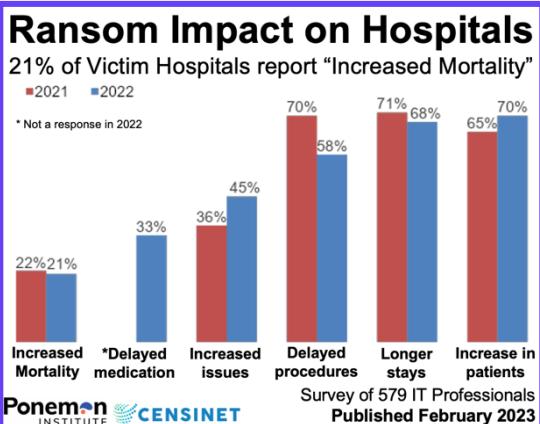
Name of the Ransomware	Count of APT Groups Using the Ransomware
Maze	7
DarkSide	5
Gimemo	4
WannaCry	4
BlackCat	3

CSW | ivanti

Review of Ransomware Threats  
Published February 2023

# The Best Cyber Insights of 2023

Click each image to see each report in full. All were published in March 2023

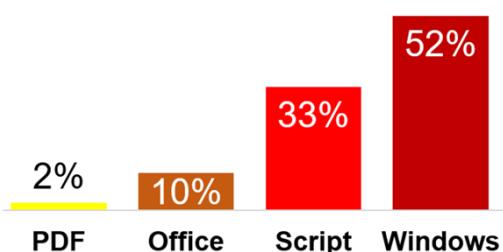


# The Best Cyber Insights of 2023

Click each image to see each report in full. All were published in March 2023

## Malicious Email Attachments

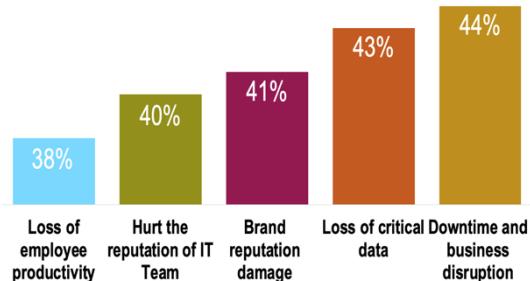
Windows Executables most used at 52%



Published February 2023

## Email-based Attacks Impact

44% cause downtime and business disruption



Survey of 1,350 IT Staff  
Published February 2023

## Email Compromise Attacks

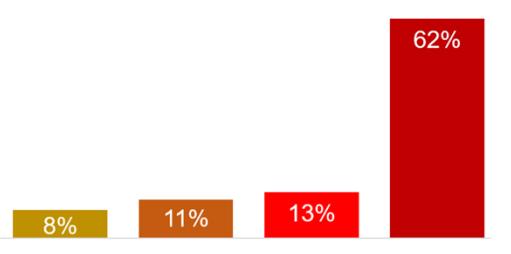
4.33 BEC Attacks / Mailbox / Week at Small Firms



Published February 2023

## Email Platforms hit by Phish

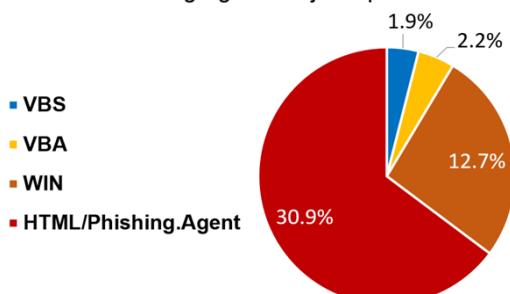
13% of Phish Emails target Outlook email system



Detections on Trellix's Telemetry  
Published February 2023

## Top Email Threats in T3 2022

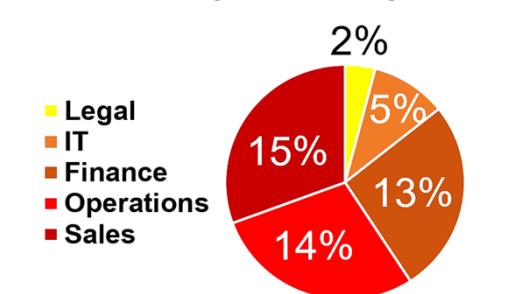
"HTML/Phishing.Agent" Trojan tops at 30.9%



Published February 2023

## Business Email Compromise

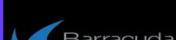
15% of BEC emails go to staff working in Sales



Insights from Jan – Dec 2022  
Published February 2023

## Email-based Attacks

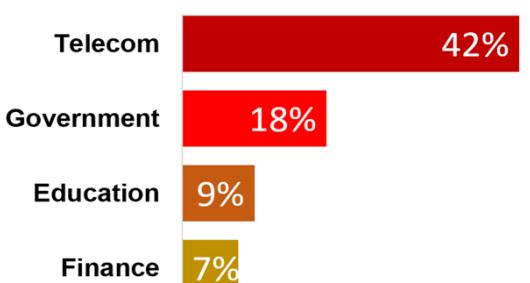
75% of email-based attacks are successful



Survey of 1,350 IT Staff  
Published February 2023

## Sectors hit by Malicious Emails

42% of Malicious Email now targets Telecom Firms



Analysis of Threat Actors in Q4 2022  
Published February 2023

# The Best Cyber Insights of 2023

Click each image to see each report in full. All were published in March 2023

### Consumer Trust in AI

36% say to "Give me an Opportunity to Opt Out"

Action	Percentage
Adopt AI ethics	16%
Audit for bias	23%
Involve human in decision-making	28%
How applications make decisions	28%
Provide opportunity to opt out	36%

**CISCO** Survey of 4,700 Security Professionals Published February 2023

### Hackers using the AI Chatbot

Improving phishing email authenticity is top concern

Goal	Percentage
Refining Phishing	53%
Enhancing skills	49%
Spreading Disinformation	49%
Malware Creation	48%
Sophisticating Attacks	46%

**BlackBerry** Survey of 1,500 IT Pros. in UK, US & Aus. Published February 2023

### Love Letters from ChatGPT

69% of adults unable to differentiate AI vs Human

Ability to Spot AI Love Letter	Percentage
Unable to spot a love letter written by ChatGPT	69%
able to spot a love letter written by ChatGPT	31%

**McAfee** businesswire A BERKSHIRE HATHAWAY COMPANY Survey of 5,109 people in nine countries Published February 2023

### ChatGPT on Dark Web

Multiple discussions of ChatGPT began in Nov 2022

**Recorded Future** Published February 2023

### Cyber Attacks on API Sites

61% of Attacks on API Sites are API Violations

Attack Type	Percentage
API Violation	61.4%
XSS	5.3%
RCE/RFI	8.7%
Protocol Manipulation	2.4%
LFI	5.9%
MISC	1.7%
Data Leakage	6.3%
Trojan	1.0%

**imperva** Data from Financial Services Industry Published February 2023

### ChatGPT's Threats to Cyber

10 Cyber Security Challenges AI could accelerate

Challenge	Challenge
- Fake Chatbots	- Social Engineering
- Malicious Text	- Two-way Dialogue
- Supply Chain	- Availability Attacks
- Insider Attacks	- Malware Generation
- Military Use	- Output Corruption

**TAG CYBER** As assessed by TAG Cyber Published February 2023

### Shadow API Requests

34% of API Requests are Shadow APIs

Type	Percentage
Shadow API	33.5%
Documented API	66.5%

**imperva** Data from Financial Services Industry Published February 2023

### Developing National Vulnerability Programmes

Published Feb 2023

**enisa** Published Feb 2023

# The Best Cyber Insights of 2023

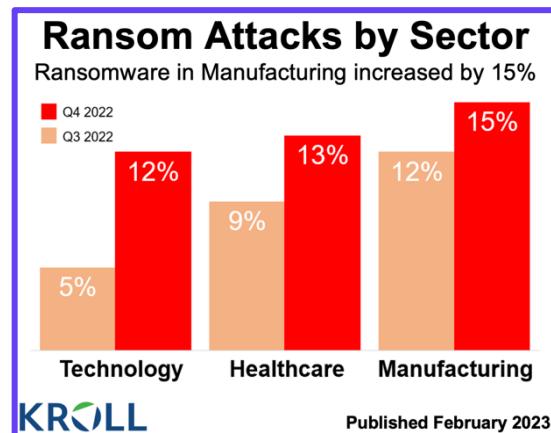
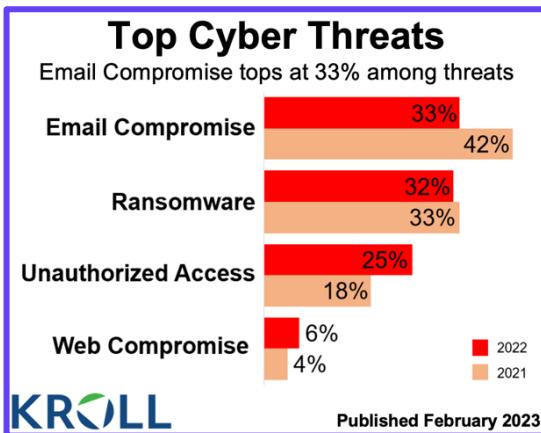
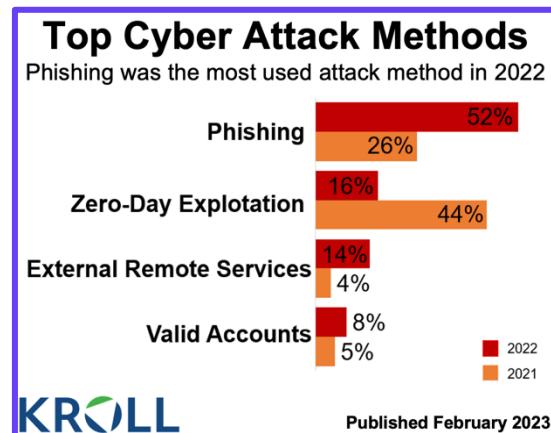
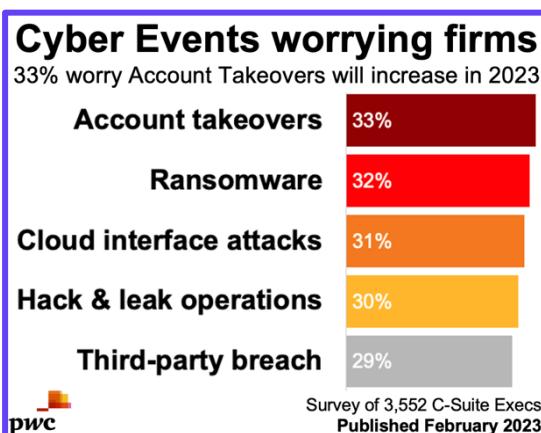
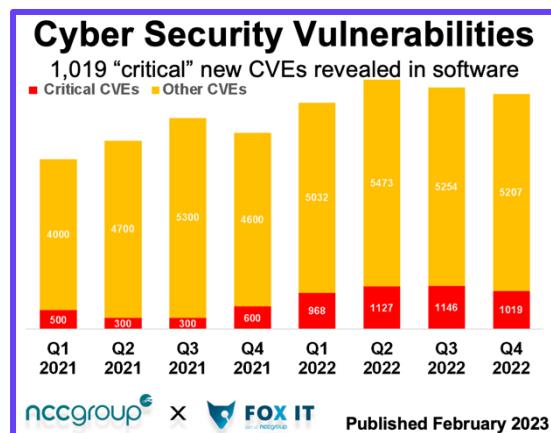
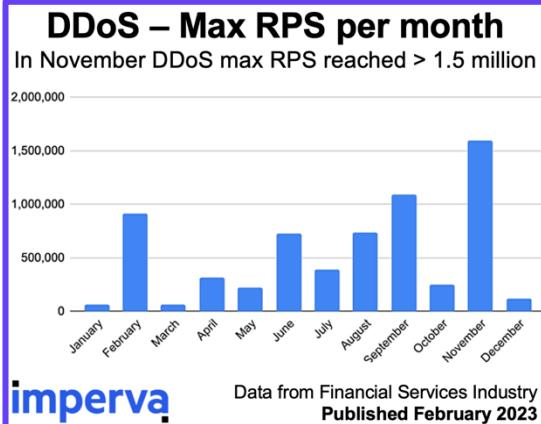
Click each image to see each report in full. All were published in March 2023

## Commonly used ransomware

Maze ransomware used by 7 global threat groups

Name of the Ransomware	Count of APT Groups Using the Ransomware
Maze	7
DarkSide	5
Gimemo	4
WannaCry	4
BlackCat	3

**CSW | ivanti** Review of Ransomware Threats Published February 2023



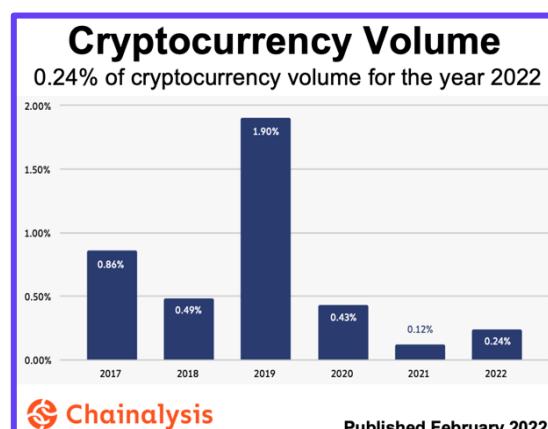
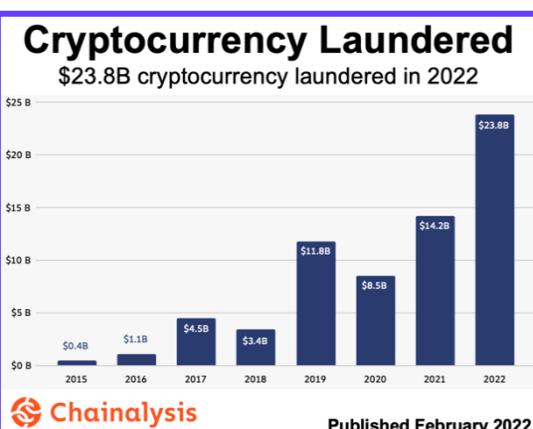
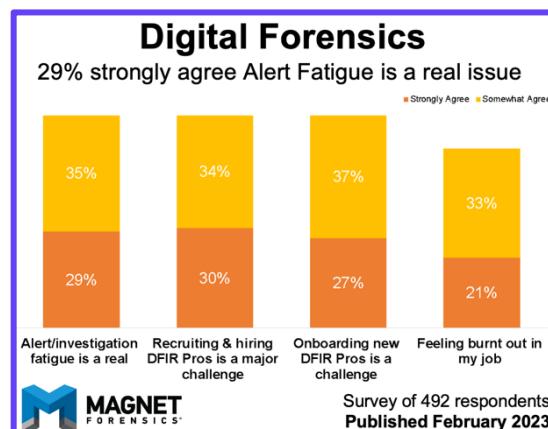
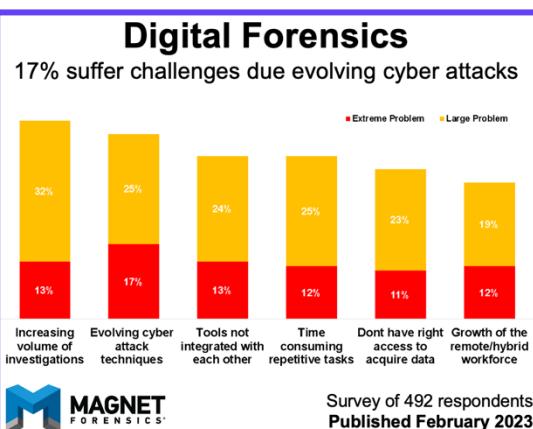
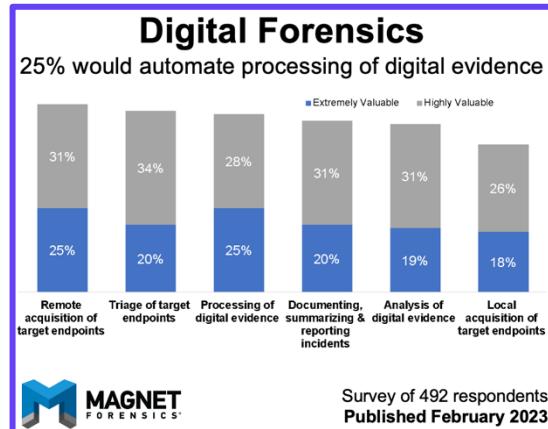
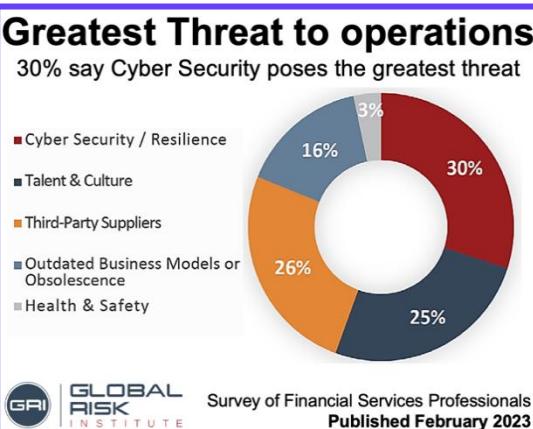
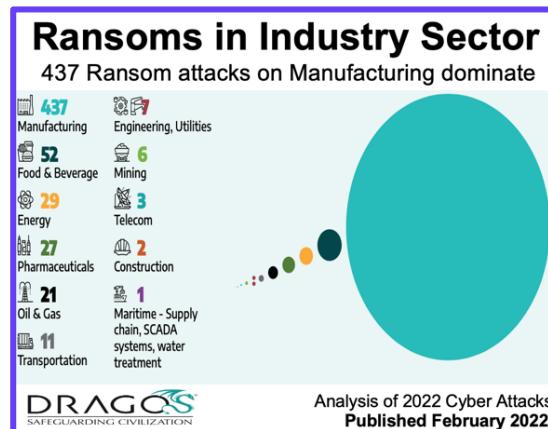
## Cybersecurity Trends

Cybersecurity, Automation &

Published Feb '23

# The Best Cyber Insights of 2023

Click each image to see each report in full. All were published in March 2023



# The Best Cyber Insights of 2023

Click each image to see each report in full. All were published in March 2023

## Cyber Risk Quantification

Top Five reasons that Firms implement CRQ

- #1 = Assess ROI of cyber security
- #2 = Prioritise Risk Remediations
- #3 = Quantify risk from cyber threats
- #4 = Calibrate risk transfer strategies
- #5 = Justify budget for cyber security

FORRESTER®

Report on 15 CRQ vendors  
Published February 2023

## Cyber Risk Quantification

Top three reasons for CISOs to implement CRQ

- #1 = Standardise taxonomy of risks
- #2 = Reframe conversation about risk
- #3 = Cement CISO's role as a partner

FORRESTER®

Report on 15 CRQ vendors  
Published February 2023

## Cyber Risk Quantification

Choose your Use Case column to find best Vendor

Vendor	Articulate ROI of current cybersecurity investment	Prioritize risk treatment and remediation strategies	Quantify current cybersecurity risk to boards of directors	Rationalize and calibrate risk transfer strategies	Justify current cybersecurity budget and future investment
Accenture	●		●		
Axio	●		●	●	●
Balbix	●	●	●		
Boston Consulting Group (BCG)	●	●	●		●
Cyberwrite			●	●	
Deloitte	●	●	●		●
EY	●			●	●
IBM	●	●	●		●
Kovrr	●	●	●	●	●
KPMG	●	●	●		●

FORRESTER®

Report on 15 CRQ vendors  
Published February 2023

## Cyber Risk Quantification

Choose your Use Case to see needed Functionality

Functionality	Articulate ROI of current cybersecurity investment	Prioritize risk treatment and remediation strategies	Quantify current cybersecurity risk to boards of directors	Rationalize and calibrate risk transfer strategies	Justify current cybersecurity budget and future investment
Model software interface	●	●	●	●	●
CRQ modeling methodology	●	●	●	●	●
Threat information capture	●	●	●	●	●
Financial impact capture	●	●	●	●	●
Model visualization	○	○	●	●	○
Risk loss exposure reporting	●	●	●	●	●
Security budget portfolio optimization	●	○	○	○	●
Cyber Insurance risk coverage analysis	●	○	●	●	●
Executive reporting and dashboards	○	○	●	●	○
Analytics and benchmarking data	○	○	●	○	○

FORRESTER®

Report on 15 CRQ vendors  
Published February 2023

## Cyber Attacks on Devices

21% of Cyber Attacks on Devices target Hikvision

Hikvision

21%

D-Link

14%

Apple

7%

Samsung

5%

RaySharp

3%



Data from CUJO AI Sentry & AI Explorer  
Published February 2023

## Cyber Attacks on Devices

63% of attacked Audio-Video Devices are Dahua

Dahua

63%

Meta

11%

Samsung

9%

Lorex

6%

Denon

3%



Data from CUJO AI Sentry & AI Explorer  
Published February 2023

## Cyber Attacks on Devices

Computers are most threatened device with 31.6%

Desktops & Laptops

32%

IP Cameras

25%

Smartphones

14%

Network-Attached Storage Devices

10%

DVRs

7%



Data from CUJO AI Sentry & AI Explorer  
Published February 2023

## Cyber Attacks on Devices

58% of attacked IP Camera Brands are Hikvision

Hikvision

58%

D-Link

37%

Other

3%

Amcrest

1%

ClareVision

0%



Data from CUJO AI Sentry & AI Explorer  
Published February 2023

# The Best Cyber Insights of 2023

Click each image to see each report in full. All were published in March 2023

## Progression of Cybersecurity

79% focused on improving Operational Tech Security

Operational Tech Security	79%
Defence against ransomware	77%
Incorporating Sec & Priv	75%
Resource value & efficiency	75%
Collaboration with OT	73%

Survey of 3,552 C-Suite Execs  
Published February 2023

## Cyber Security Culture

Best Practices to Strengthen Cybersecurity Culture

- #1 = Treat Staff as Part of Solution
- #2 = Develop a Structured Roadmap
- #3 = Gain Leadership Support
- #4 = Boost Cybersecurity Knowledge

**Forbes**

Published February 2023

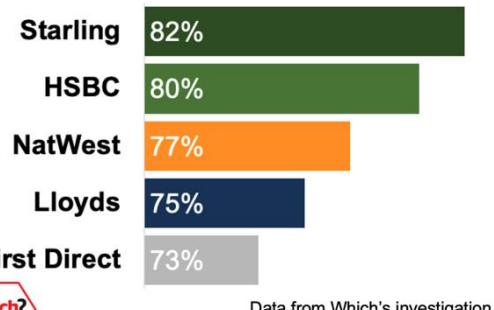
## UpGuard Cyber in Australia

Top 200 Australian firms Cybersecurity

Published Feb '23

## Online Bank Security in UK

Starling "has best UK online security for customers"



## Top Perceived Risk for 2023

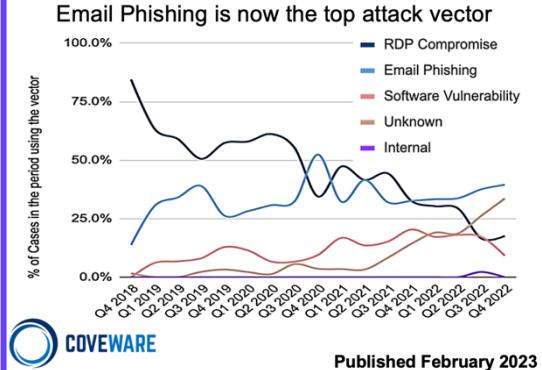
#2 Risk for Financial Services firms is Economic

- #1 = Economic
- #2 = Cyber
- #3 = Credit
- #4 = Geopolitical
- #5 = Talent

Survey of Financial Services Professionals  
Published February 2022

## How Firms hit by Ransom

Email Phishing is now the top attack vector



## Insuring Essential Services

% of Essential Services Firms with Cyber Insurance

Western & Northern EU	45%	55%
Southern EU	39%	61%
Eastern EU	12%	88%

262 Essential Services Operators  
Published February 2023

## It's time for Cyber ILS

Insurance-Linked Securities are here!

# The Best Cyber Insights of 2023

Click each image to see each report in full. All were published in month to February 2023

## Top Global Business Risks

Experts list Cyber Incidents as key a risk

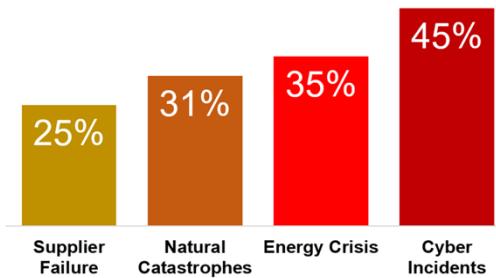
- #1 = Cyber Incidents
- #2 = Business Interruption
- #3 = Macroeconomic developments
- #4 = Energy Crisis
- #5 = Legislation & Regulation changes



Insights from over 2,712 respondents  
Published January 2023

## Business Interruption Risks

Cyber Incidents most feared interruption at 45%



Insights from over 917 respondents  
Published January 2023

## Chief Risk Officer Top Priorities

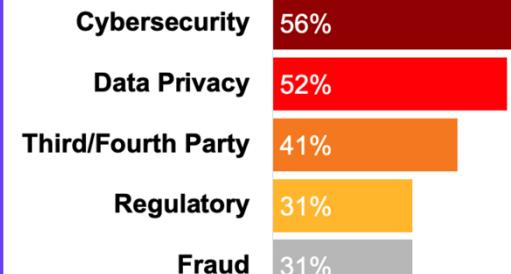
Cybersecurity Risk is Top Priority for next 12 months



Data from Annual Survey of Bank CROs  
Published January 2023

## Risks needing C-Level Attention

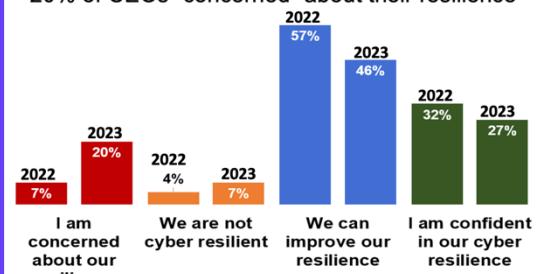
Cybersecurity will require most attention in next 3 years



Data from Annual Survey of Bank CROs  
Published January 2023

## Cyber Resilience Confidence

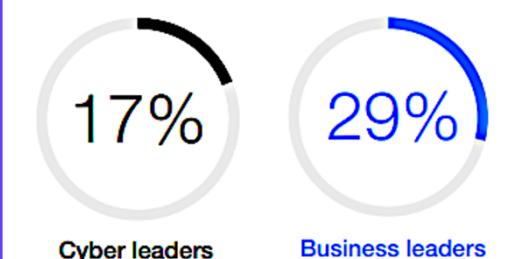
20% of CEOs "concerned" about their resilience



Survey of 117 firms  
Published January 2023

## CEOs want Cyber Regulation

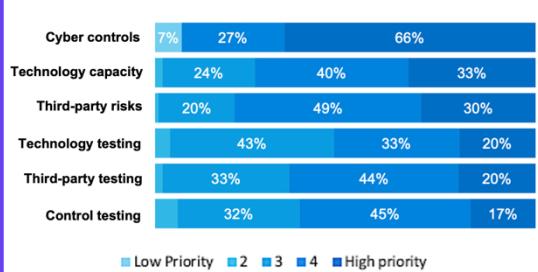
29% of Business Leaders say Regs help Resilience



Survey of 117 firms  
Published January 2023

## Priorities for Cyber Resilience

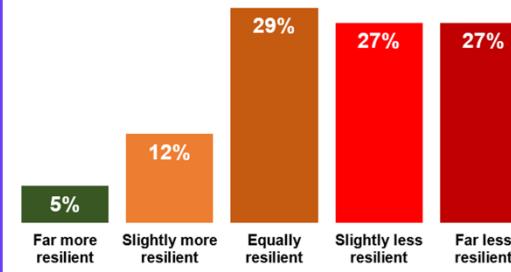
Cyber Controls are Highest Priority Enhancement



Data from Annual Survey of Bank CROs  
Published January 2023

## Cyber Risk at Third Parties

27% of CEOs say Suppliers are "Far Less Resilient"



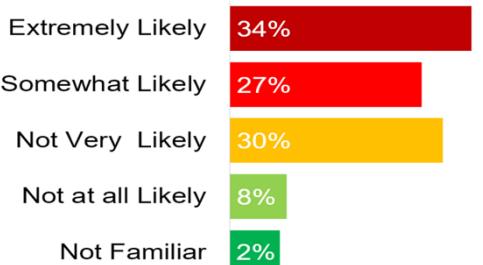
Survey of 117 firms  
Published January 2023

# Cyber Insights: Ransomware Attacks

Click each image to see each report in full. All were published in month to February 2023

## Ransom at Small Suppliers

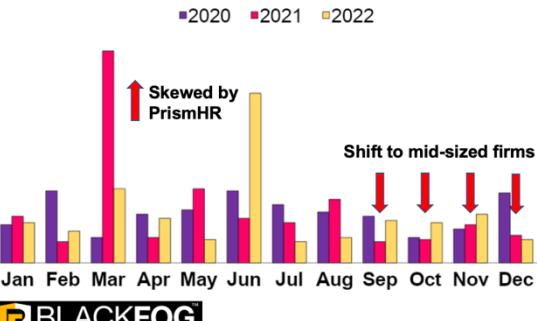
64% of small firms say it's likely they'll be hit this year



2,913 IT decision-makers at small firms  
Published January 2023

## Ransom Victims get Smaller

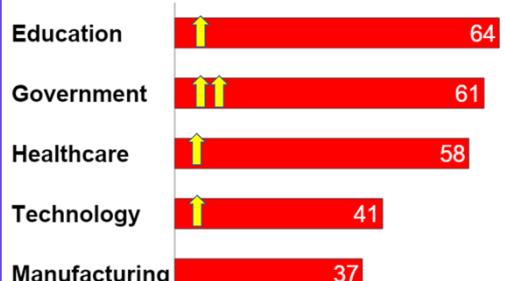
Ransom Gangs continue to focus on smaller firms



Published January 2023

## Ransom Victims by Sector

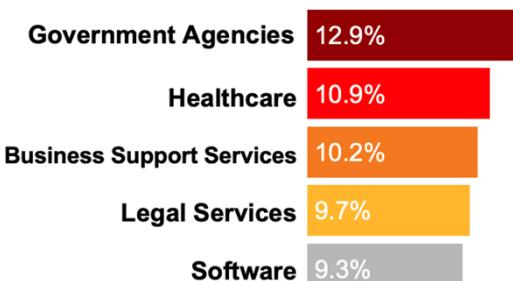
Government Agencies see fastest growth in Ransom



Published January 2023

## Ransom Victims by Sector

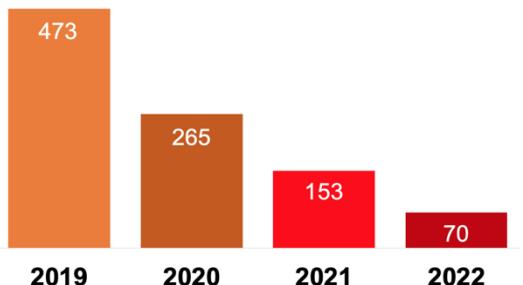
Government Agencies account for 12.9% of Victims



Data from open sources intelligence  
Published January 2023

## Mutation Speed of Ransom

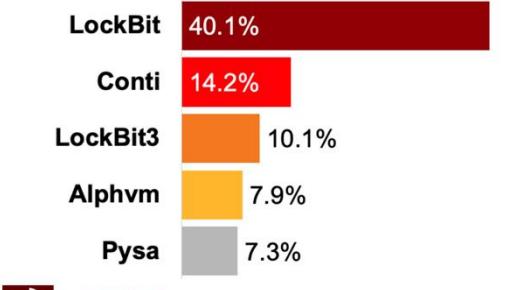
Average life of each Ransom strain now 70 days



Analysis of Crypto Payments  
Published January 2023

## Top Ransomware Gangs

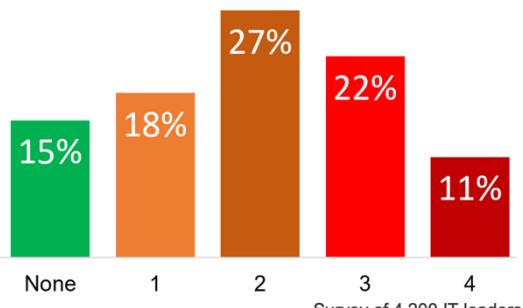
LockBit cause 40.1% of observed Cyber Attacks



Data from open sources intelligence  
Published January 2023

## Repeated Ransom Attacks

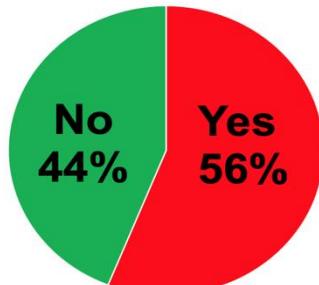
11% of firms attacked 4 times in the last 12 months



Survey of 4,200 IT leaders  
Published January 2023

## Victims of Ransomware

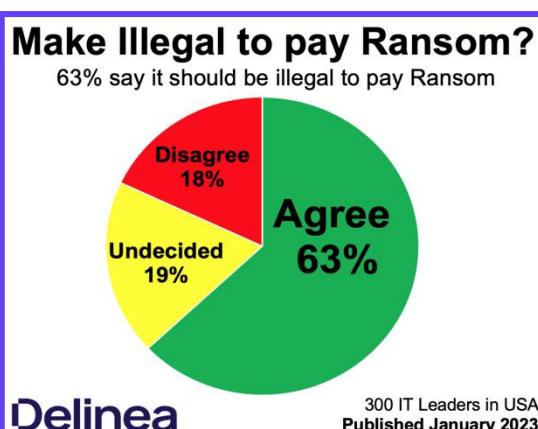
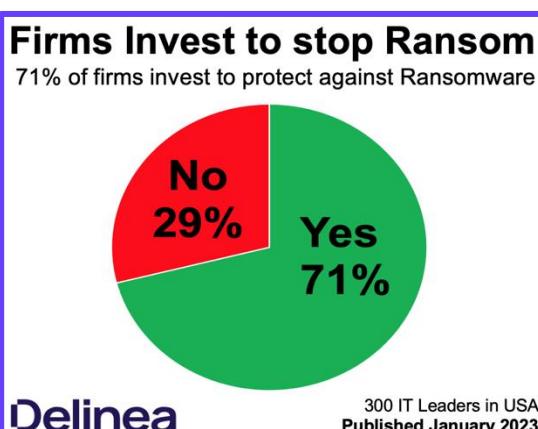
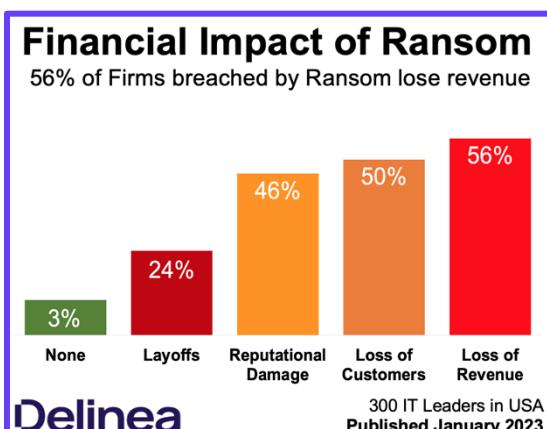
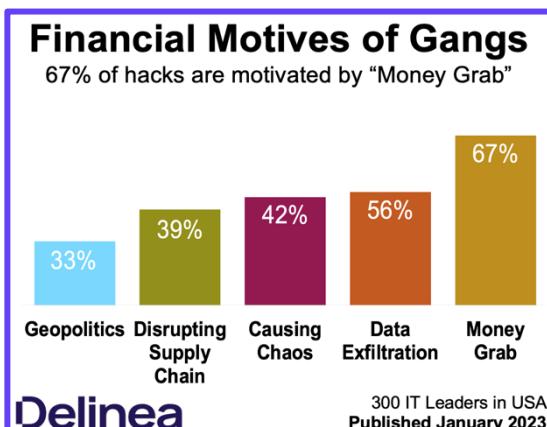
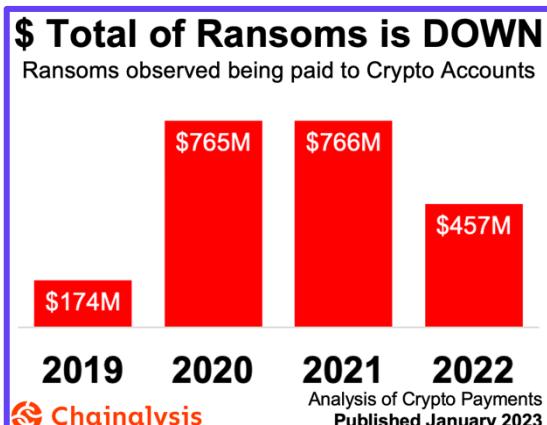
56% of firms have been "hit" by Ransomware



300 IT Leaders in USA  
Published January 2023

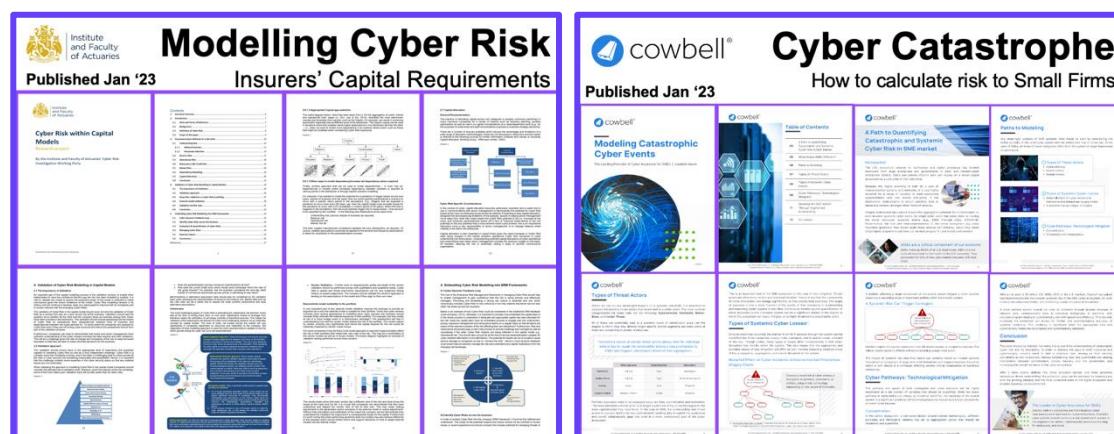
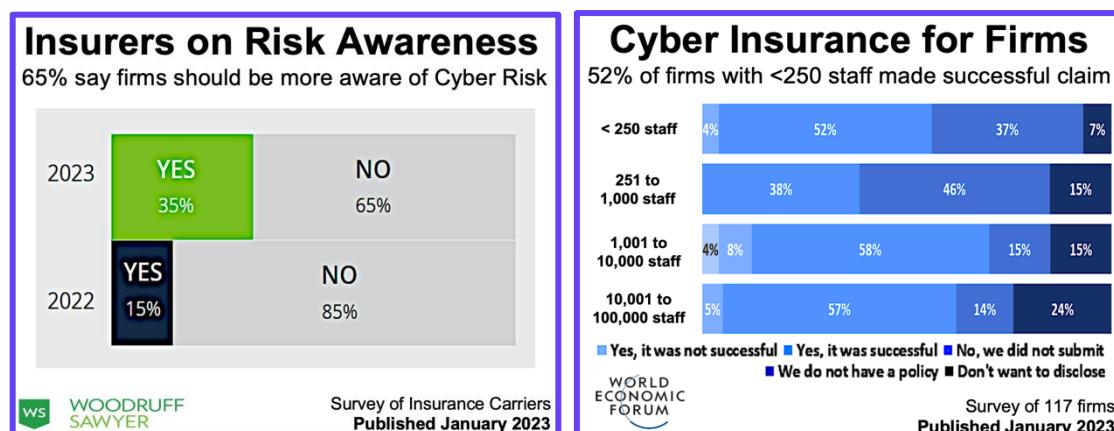
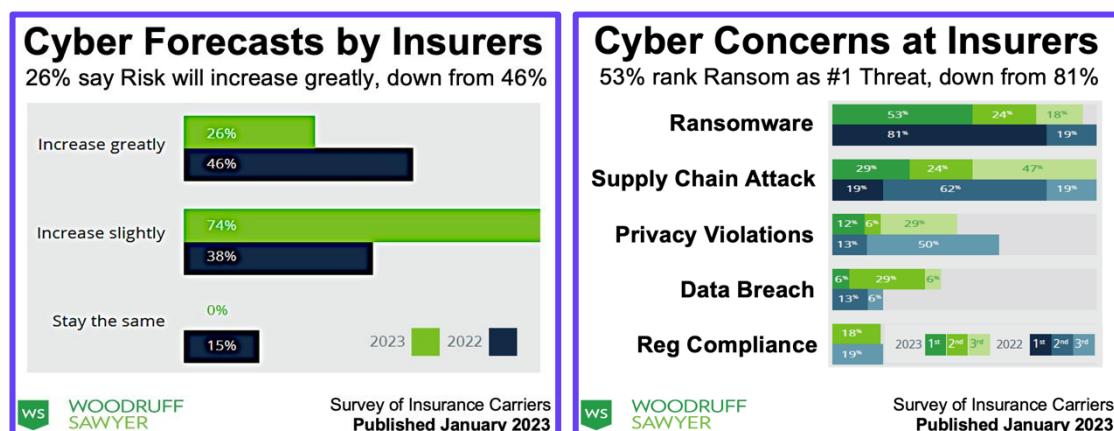
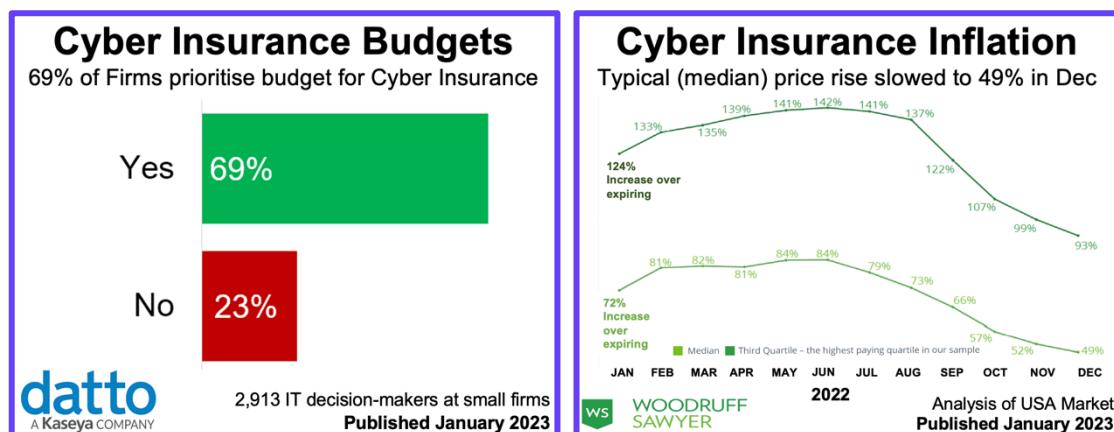
# Cyber Insights: Cyber Financials

Click each image to see each report in full. All were published in month to February 2023



# Cyber Insights: Cyber Insurance

Click each image to see each report in full. All were published in month to February 2023



# Cyber Insights: Cyber AI

Click each image to see each report in full. All were published in month to February 2023

**W / T H<sup>®</sup> SECURE**

**Malicious AI**  
How to engineer AI for Cyber Attacks

Published Jan '23

**GPT-3 vs GPT-4**  
GPT4 will have 500x more parameters than GPT3

**GPT-4**

**GPT-3**

↓

175,000,000,000 Parameters

100,000,000,000,000 Parameters

The CYBER RESCUE Alliance

Published January 2023

**The CYBER RESCUE Alliance**

**Best New AI Services**  
See Tomorrow, by using these Today

Published Jan 2023

Cleanup.pictures Removes Unwanted Objects	RESUME WORDED Instantly Scores Resumes	SOUNDRAW AI Music Generator	Looka Design Logos, Websites, Brands	copy.ai AI-Powered Copywriter
ELSA Artificial Speaking Coach	Socrative Personal Robotic Tutor	craiyon AI Image Generator	GLaMDA AI-Powered Chatbot	QuillBot Breakthrough Conversation Technology
tome Generates & Builds Presentations	Superhuman Automatically Organizes Emails	Notion Writes Notes & Builds	YOU Rephrases Your AI Search Engine	

**480 AI Firms Categorised**  
159 build AI for Text & Chat (Grammarly, ChatGPT)

<b>Text + Chat</b>	159
<b>Image</b>	71
<b>Audio</b>	59
<b>Video</b>	57
<b>ML Ops Platform</b>	42

**NFX**

Published January 2023

**The CYBER RESCUE Alliance**

**ChatGPT for Coding**  
How hackers & coders already use AI

Published Jan 2023

**ChatGPT & Cyber**  
23 ChatGPT Functions for Cyber

Published Jan 2023

<b>ChatGPT for CyberSecurity #1</b> <a href="https://www.chatgpt.com/cybersecurity">https://www.chatgpt.com/cybersecurity</a>	<b>What is ChatGPT</b> • ChatGPT is a large language model developed by OpenAI in November 2022. It is built on top of GPT-3 & GPT-3.5 family of language models, and ChatGPT was launched as a prototype on November 30, 2022, and quickly became one of the most popular AI models, accessible across many domains of knowledge. Its uneven factual knowledge has been widely criticized.
<b>Create Incident Response process</b>	<b>Containment Malware</b>
<b>Threat Correlation</b>	<b>Useful Volatility Commands</b>
<b>Identify Threat</b>	<b>Create Script .bat to Triage Forensic</b>

**ChatGPTs Risk to Cybersecurity**  
41% think ChatGPT poses a significant risk to Cyber

<b>Yes</b>	41%
<b>Not sure</b>	31%
<b>No</b>	28%

CSH

Data from LinkedIn Poll with > 14,000 votes

Published January 2023

**NIST** NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY U.S. DEPARTMENT OF COMMERCE

**Artificial Intelligence Risk Management Framework**

Published Jan 2023

# Cyber Insights: Cyber Governance

Click each image to see each report in full. All were published in month to February 2023

**Davos Global Risks Report**  
Cyber is #4 for Firms  
Published Jan 2023

The Global Risks Report 2023, 19th Edition

Year	No Cyber Laws	Some	Laws against most crimes
2013	32%	32%	36%
2018	19%	33%	48%
2020	12%	33%	55%
2023	8%	25%	67%

WORLD ECONOMIC FORUM

**Davos Report on Risks to Firms**  
Experts list Cyber Insecurity as key a risk to 2025  
#1 = Cost of Living Crisis  
#2 = Natural Disasters  
#3 = Geo-Economic confrontation  
#4 = Cyber Insecurity  
#5 = Environmental Damage  
Insights from over 1,200 experts  
Published January 2023

WORLD ECONOMIC FORUM

**Cyber Laws in Each Country**  
67% of UN Member States have substantive laws

Survey of 94% UN Member States  
Published January 2023

CSH

**10 Laws of Cyber Security**  
Microsoft's "Immutable Laws of Cyber Security"

- **Define Success** Ruin your attacker's ROI
- **Keep Up** Patch continuously
- **Productivity Wins** Automate for efficiency
- **Attackers don't care** Understand options
- **Prioritize to Survive** Know what's important
- **Cyber is Team Sport** Outsource to experts
- **Zero Level Trust** Don't Trust Network
- **Isolated Networks** aren't always secure
- **Encryption Protects** But it isn't enough
- **Tech doesn't solve** Invest: People & Process

Microsoft

Published January 2023

**Top 5 Cyber Posture Metrics**  
Asset Inventory Coverage is the Top Posture Metric

- #1 = Asset Inventory Coverage
- #2 = Software Inventory Coverage
- #3 = Security Controls Coverage
- #4 = Vulnerability Assessment Coverage
- #5 = Mean Age of Open Vulnerabilities

Balbix® Based on ability to link Security to Business  
Published December 2022

**Cyber Threat Intelligence Services**  
Why should they be part of your cybersecurity strategy?

Correlated Security

Published January 2023

**Trust Deficit in Cyber**  
Cyber Transparency is Key  
Published Jan '23

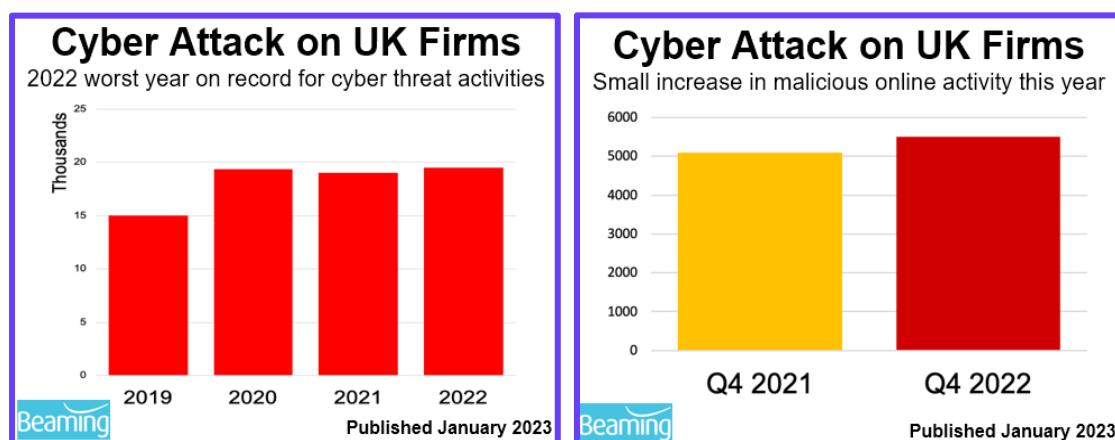
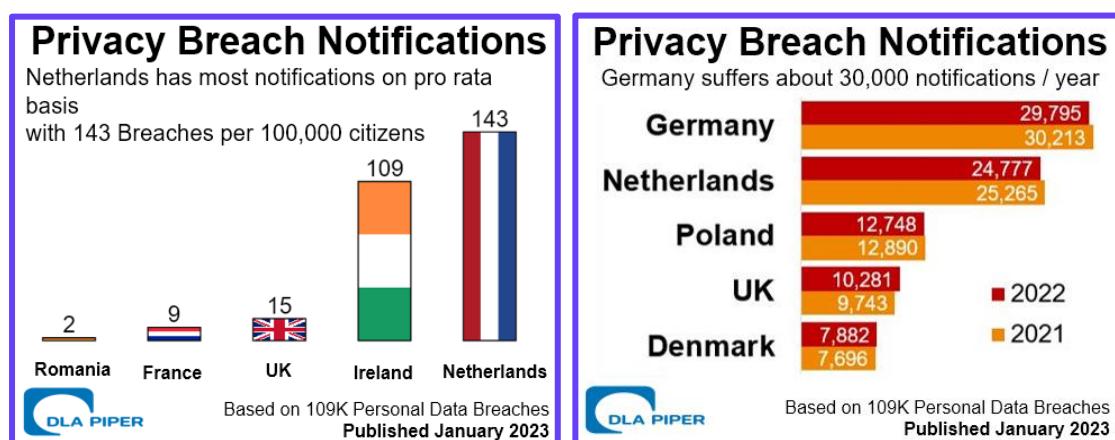
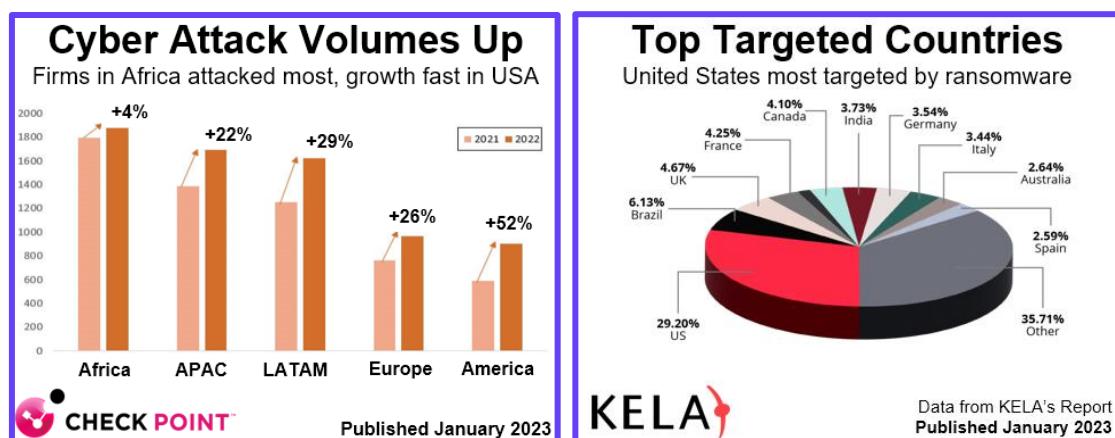
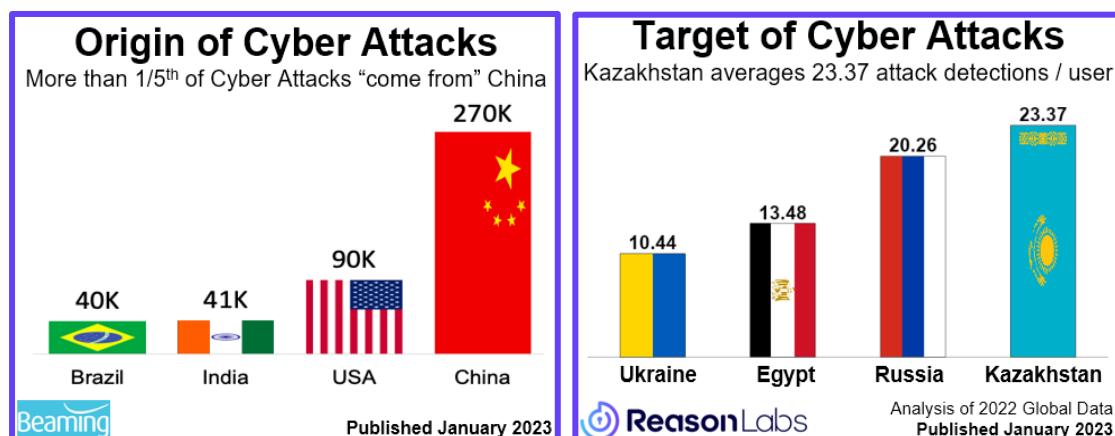
Addressing the Trust Deficit in Critical Infrastructure  
Cyber Resilience is Necessary for Building and Sustaining Trust  
Geopolitical Forces Compound Critical Infrastructure Vulnerabilities  
Policymakers Intensify Focus on Critical Infrastructure  
Trust Requires Measurement and Transparency

**Publish your Strategy**  
Cyber Strategy at a Medical Firm  
Published Jan 2023

2022 Cybersecurity Annual Report  
Transparency helps protect patient safety and privacy  
The state of healthcare cybersecurity  
Emerging cybersecurity developments  
Cybersecurity at BD  
Collaborating to strengthen cybersecurity in healthcare  
Coordinated vulnerability disclosure  
Investing in cybersecurity

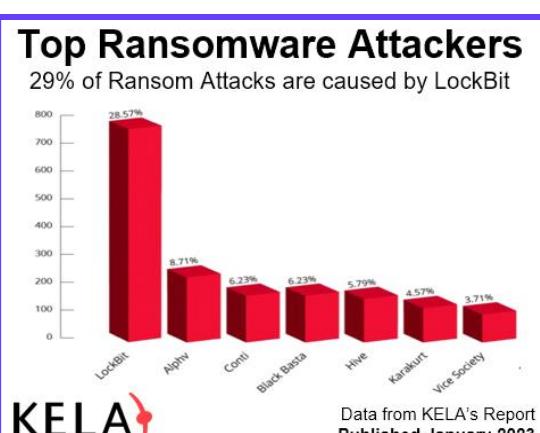
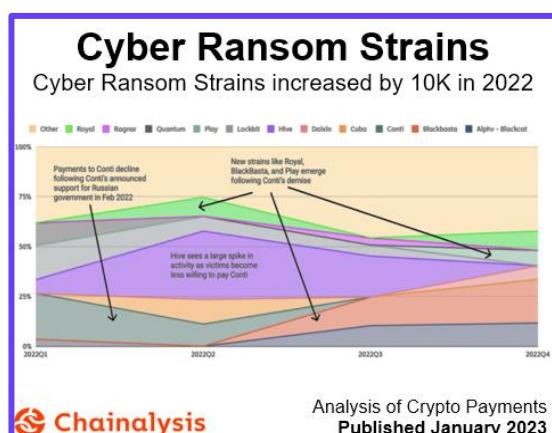
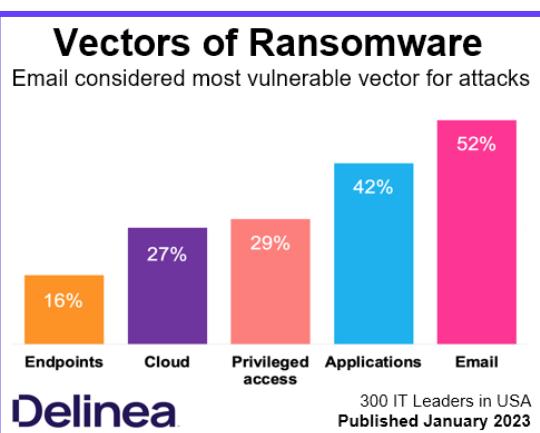
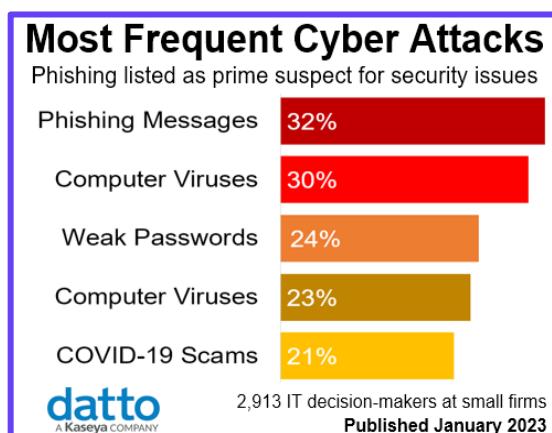
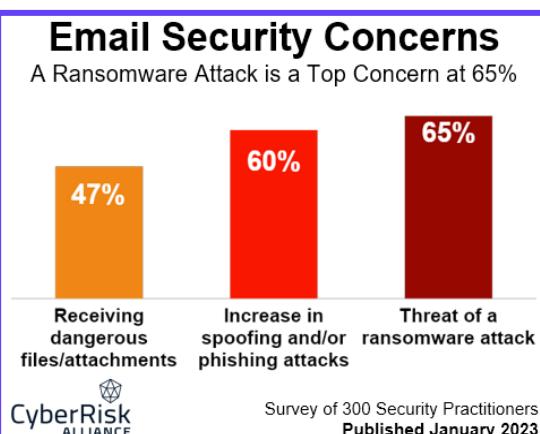
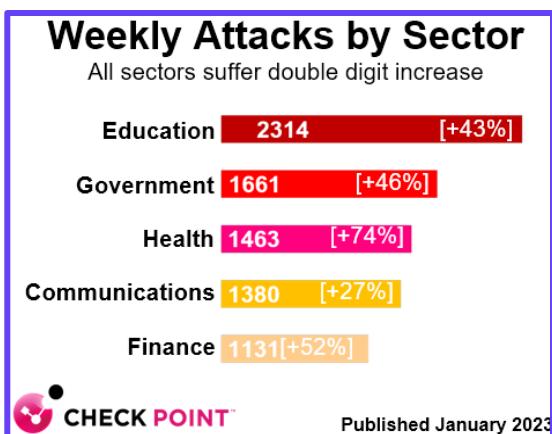
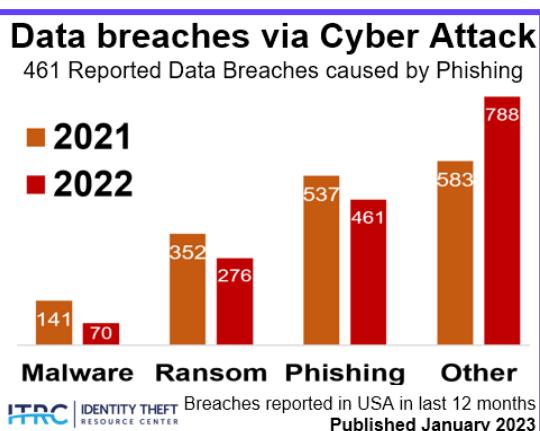
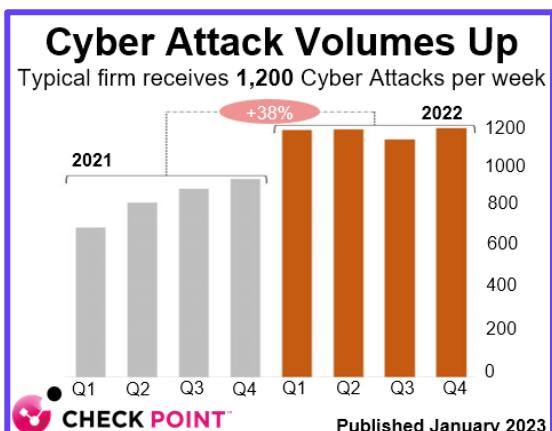
# Cyber Insights: Cyber by Country

Click each image to see each report in full. All were published in month to February 2023



# Cyber Insights: Cyber Attack Volumes

Click each image to see each report in full. All were published in month to February 2023

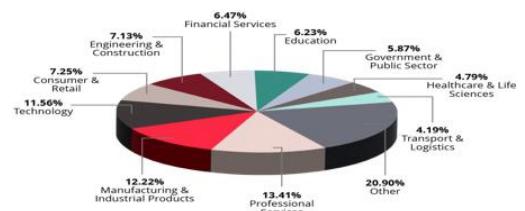


# Cyber Insights: Cyber by Sector

Click each image to see each report in full. All were published in month to February 2023

## Sectors attacked most often

Manufacturing most targeted sector at 17%

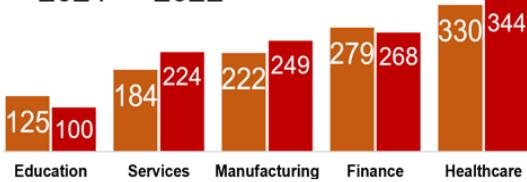


Data from KELA's Report  
Published January 2023

## Sectors breached most often

344 Reported Data Breaches at USA Health Firms

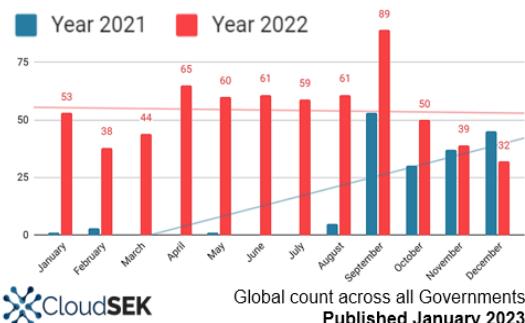
■ 2021 ■ 2022



ITRC IDENTITY THEFT RESOURCE CENTER Breaches reported in USA in last 12 months  
Published January 2023

## CyberAttacks on Government

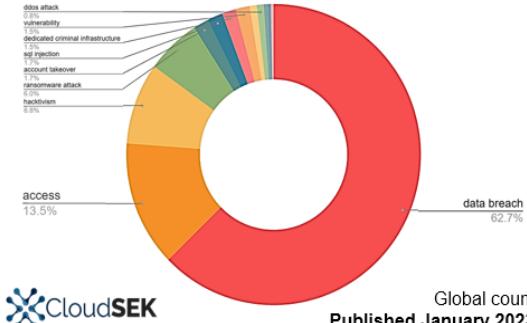
Number of attacks up 95% in H2 2022 vs H2 2021



Global count across all Governments  
Published January 2023

## CyberAttacks on Government

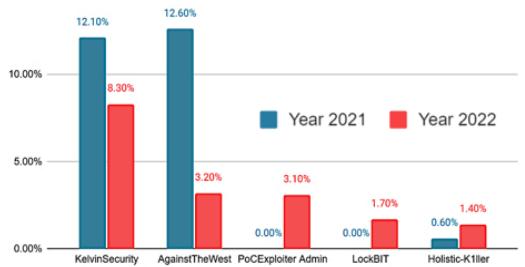
63% of reports by Governments are of Data Breach



Global count  
Published January 2023

## CyberAttacks on Government

KelvinSecurity & AgainstTheWest claim most attacks

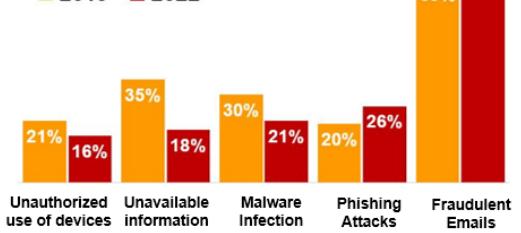


Global count across all Governments  
Published January 2023

## UK Schools Cyber Incidents

Fraudulent Emails now account for 73% of Incidents

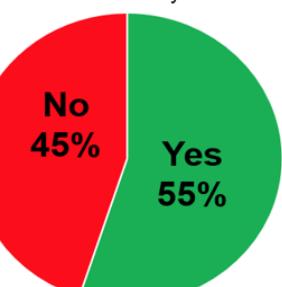
■ 2019 ■ 2022



Survey of 805 UK Schools  
Published January 2023

## UK Schools Cyber Training

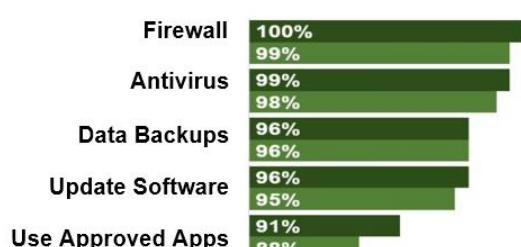
55% Non-IT Staff Received Cyber Security Training



Survey of 805 UK Schools  
Published January 2023

## Cyber Security in Schools

100% of UK Schools have implemented Firewalls



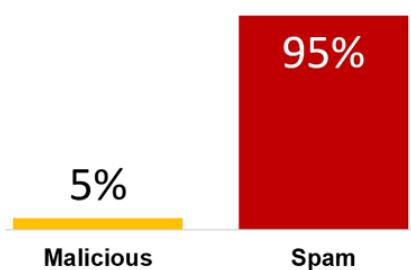
Survey of 805 UK Schools  
Published January 2023

# Cyber Insights: Microsoft & Remote Workers

Click each image to see each report in full. All were published in month to February 2023

## Security of Microsoft 365

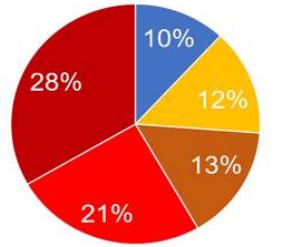
95% of unwanted emails are Spam



Analysis of 2 billion emails/month  
Published January 2023

## Security of Microsoft 365

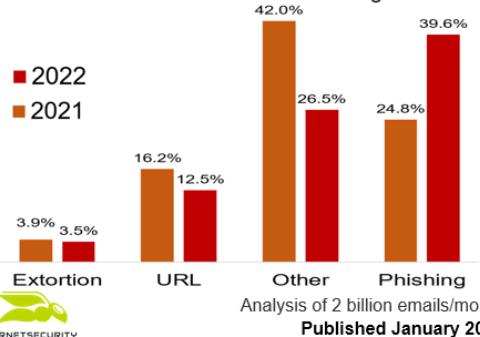
28% of cyber attacks use Archive files in emails



Analysis of 2 billion emails/month  
Published January 2023

## Security of Microsoft 365

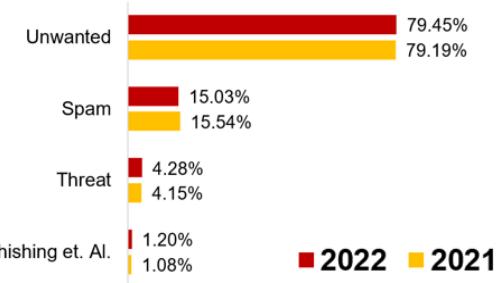
39.6% of email attacks use Phishing in 2022



Analysis of 2 billion emails/month  
Published January 2023

## Security of Microsoft 365

Unwanted Emails remain prevalent in the past year

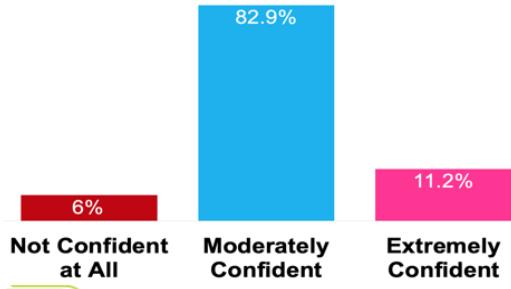


■ 2022 ■ 2021

Analysis of 2 billion emails/month  
Published January 2023

## Security of Remote Workers

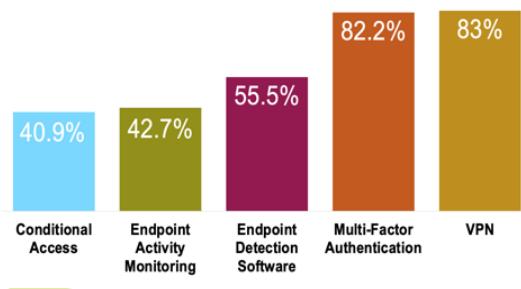
6% are not confident at all in security



900 IT & Security Managers  
Published January 2023

## Security of Remote Workers

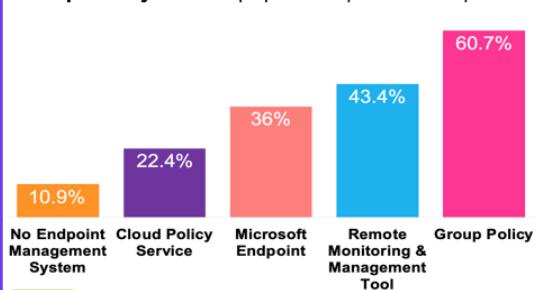
VPN commonly used as security feature



900 IT & Security Managers  
Published January 2023

## Security of Remote Workers

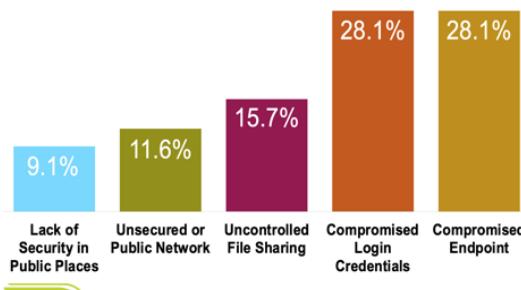
Group Policy is most popular to protect Endpoints



900 IT & Security Managers  
Published January 2023

## Security of Remote Workers

Compromised Endpoint is main source of incident



900 IT & Security Managers  
Published January 2023

# Cyber Insights: Respond & Recover

Click each image to see each report in full. All were published in month to February 2023

**NIST** Published Jan '23

## Respond and Recover

Cybersecurity for Manufacturers

**CYBER THEORY** Published Jan '23

## Cyber Sector Review

Performance of Defence Vs Attack

**CRN**

## Hottest 10 Cyber Tools

As assessed by CRN

- **Arctic Wolf** MyCyber
- **Beyond Identity** Secure Customers
- **Cybersixgill** DVE Intelligence
- **Fortinet** FortiRecon
- **Huntress** EDR
- **Island** Enterprise Browser
- **Palo Alto Networks** Autonomous SOC
- **SentinelOne** XDR Ingest
- **Sophos** X-Ops
- **Tenable** One Platform

Published December 2022

**datto** A Kaseya COMPANY

## Cyber Fears at Small Firms

Phishing Emails Top Concern of small firms at 37%

Fear	Percentage
Phishing Emails	37%
Malicious Websites	27%
Poor User Practices	24%
Weak Passwords	24%
Lack of Training	23%

2,913 IT decision-makers at small firms  
Published January 2023

**datto** A Kaseya COMPANY

## Defences vs Ransomware

Most popular defence used is Antivirus Software

Defence	Percentage
Antivirus Software	57%
Spam Protection	53%
Managed Firewall	49%
File Backup	49%
Security Training	43%

2,913 IT decision-makers at small firms  
Published January 2023

**Delinea**

## Firms Invest to stop Ransom

43% of small firms invest in Network Security

Investment Area	Percentage
Endpoint security	15%
Application security	21%
Identity and access management	22%
Cloud security	35%
Network security	43%

300 IT Leaders in USA  
Published January 2023

**CyberRisk ALLIANCE**

## Email Security Strategy

Current and planned strategies on email security

Strategy	Planned (%)	Currently Included (%)
Vulnerability Management	26%	65%
Spoofing/ Phishing Protection	18%	79%
Email backup	14%	80%
Security Awareness	16%	80%
Attachment Scanning	12%	85%

Survey of 300 Security Practitioners  
Published January 2023

**datto** A Kaseya COMPANY

## Top Recovery Method

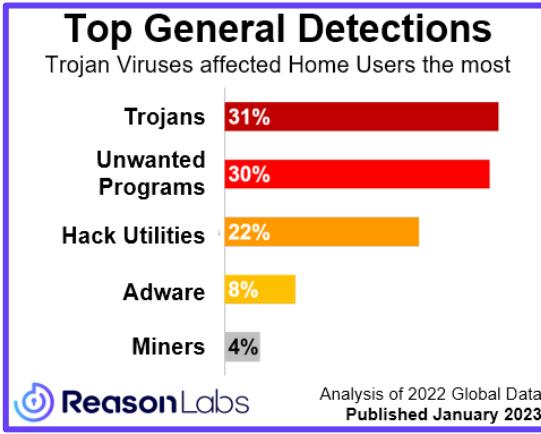
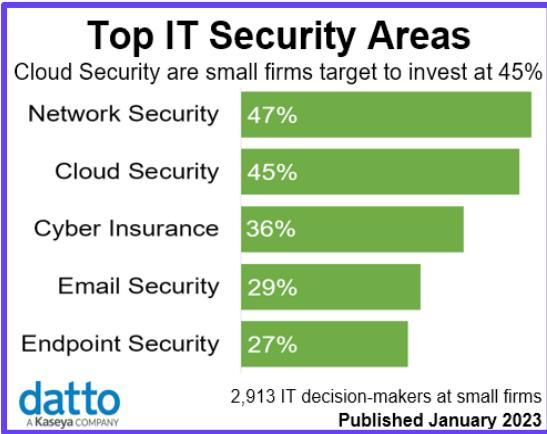
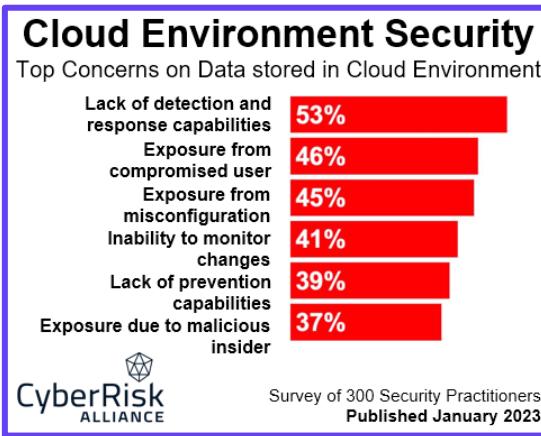
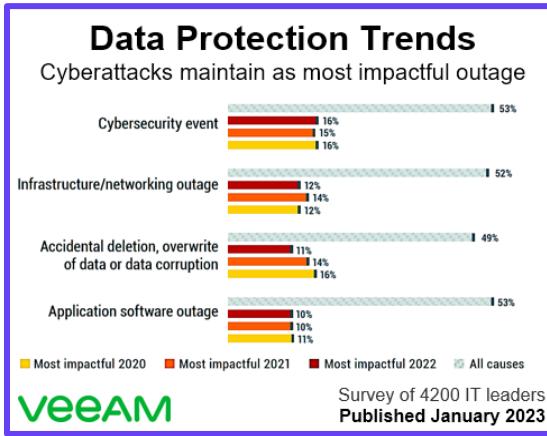
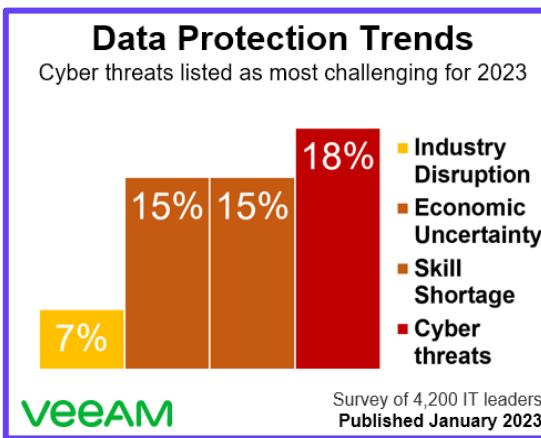
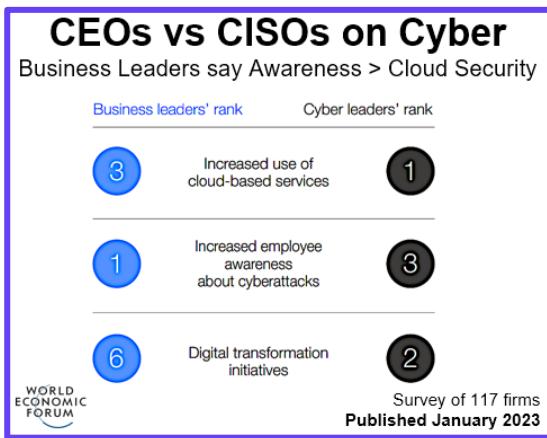
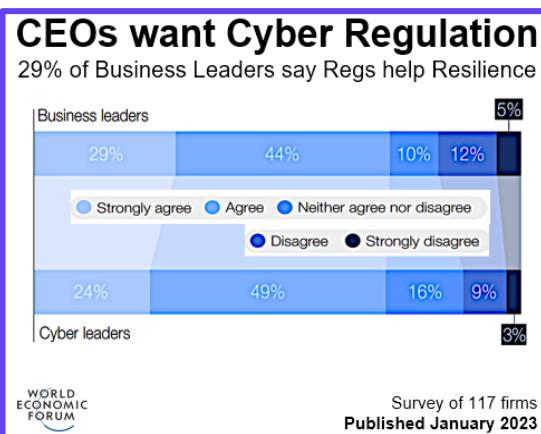
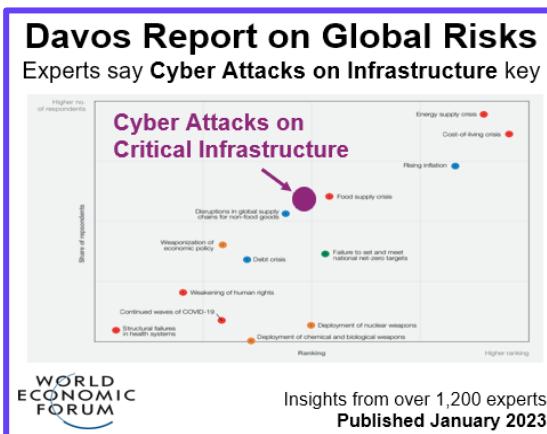
Manual Backup is Top Method for next 12 months

Method	Percentage
Manual Backup	49%
Continous Availability	36%
Old Systems Backup	36%
Third-Party Recovery	32%
No data loss	13%

2,913 IT decision-makers at small firms  
Published January 2023

# Cyber Insights: Cyber Developments

Click each image to see each report in full. All were published in month to February 2023



# The Best Cyber Insights of 2023

Click each image to see each report in full. All were published in month to January 2023

## Cyber AI Predictions for 2023

Top 5 Causes for Cyber Concern from AI

- #1 = Transform security, risk & fraud
- #2 = Innovate attacks with generative AI
- #3 = Spear-phishing personalised by AI
- #4 = Social engineer with Deep Fakes
- #5 = Disinformation with Chatbots



Predictions from Experts quoted by SC  
Published December 2022

## AI Cyber Attacks

Cyber Must Adapt to New Threats

TRAFCOM

Likennetehtävät ja viestintävirasto

Published Dec 2022



## Open AI generates InfoSec

InfoSec Policies made by ChatGPT

Published Dec 2022



## Open AI in Cyber

ChatGPT's AI Cyber Potential

CYFIRMA

DECODING THREATS

Published December 2022



## AI & ML use in Cyber Attacks

How Artificial Intelligence & Machine Learning helps

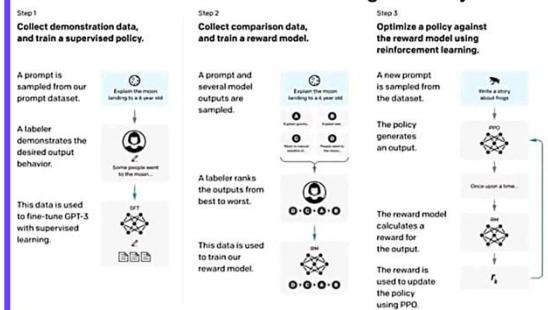


MITRE

Based on observations & security groups  
Published December 2022

## How Open AI is Trained

ChatGPT learns from its dialogue with you



kenovy OpenAI

Published December 2022

## Cyber Predictions for 2023

Top 5 Causes for Cyber Concern in 2023

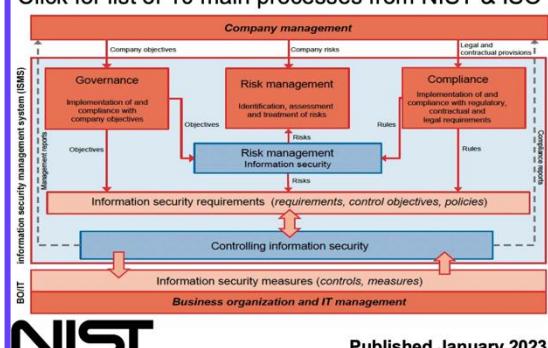
- #1 = Shadow APIs lead to breaches
- #2 = MFA becomes ineffective
- #3 = Cloud Apps unsecured
- #4 = Open Source Software targeted
- #5 = Ransomware rise up political agendas



Predictions from Industry Experts at F5  
Published December 2022

## Managing Cyber Security

Click for list of 10 main processes from NIST & ISO



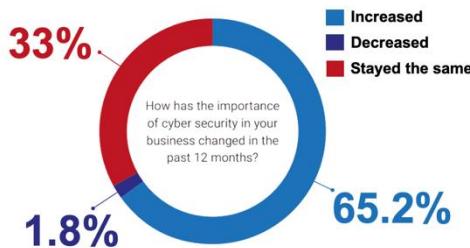
Published January 2023

# Cyber Insights: Cyber & Finance Dept

Click each image to see each report in full. All were published in month to January 2023

## Importance of Cyber is up

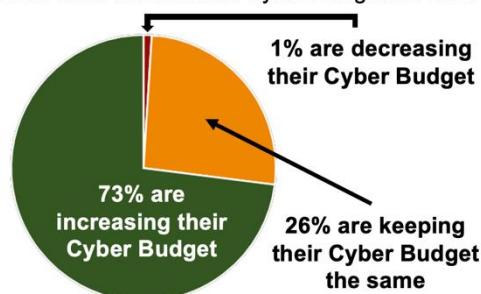
65.2% say that importance of cyber has increased



Survey of 20,000 Manufacturers  
Published December 2022

## Cyber Budgets are Growing

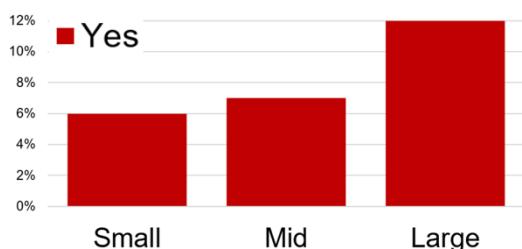
73% of firms will increase Cyber Budgets in 2023



Survey of over 6,550 Cybersecurity Professionals  
Published December 2022

## Ransom Impacting Firms

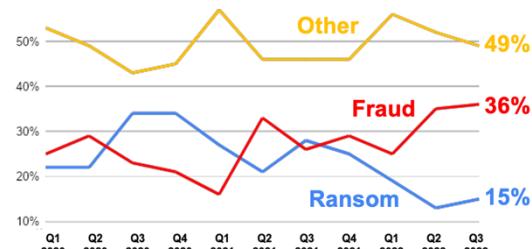
12% of Large firms "directly affected" last year



Survey of 343 Cyber Directors  
Published December 2022

## Claims on Cyber Insurance

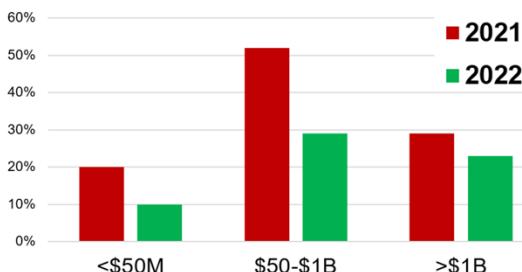
15% of Claims now for Ransom (vs 34% in Q3 '20)



Published December 2022

## Willingness to pay Ransom

29% of Medium-sized firms would consider paying



Survey of 343 Cyber Directors  
Published December 2022

## Ransom Payments increase

Size of each known payment +13.2% from Q2/22



Published December 2022

## Audit Teams say Cyber is Top

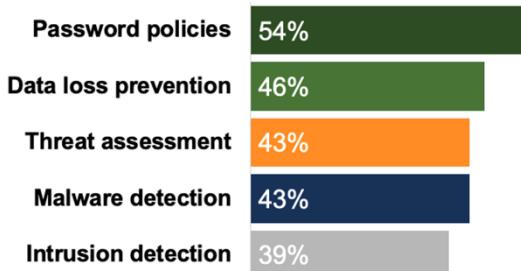
43% of Audit Executives Focus on Cyber in 2022



Survey of U.S. Internal Audit Executives  
Published December 2022

## Cyber Issues for Audit Team

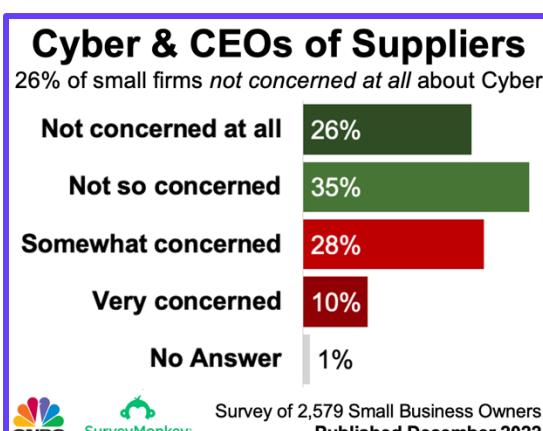
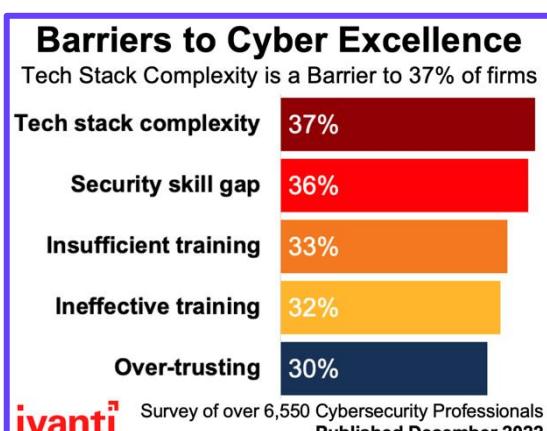
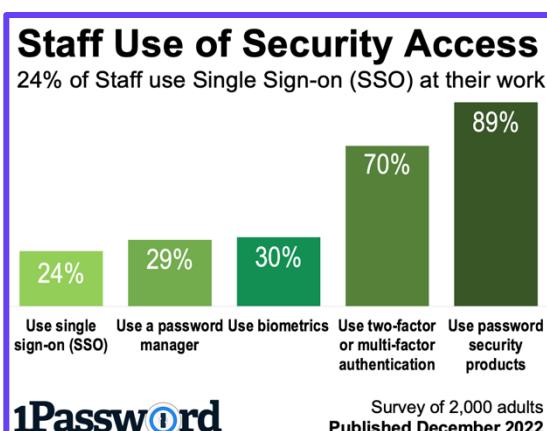
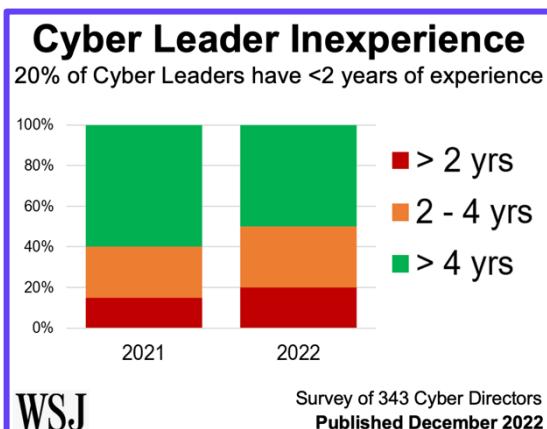
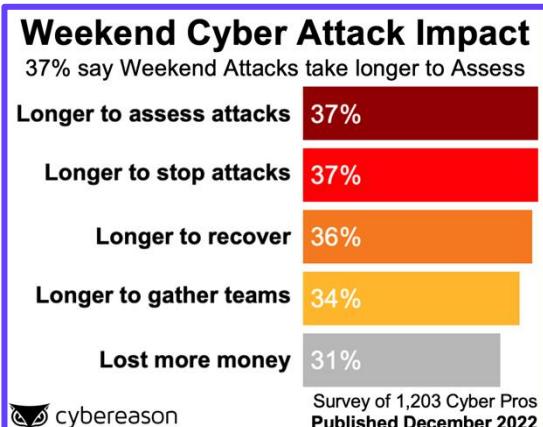
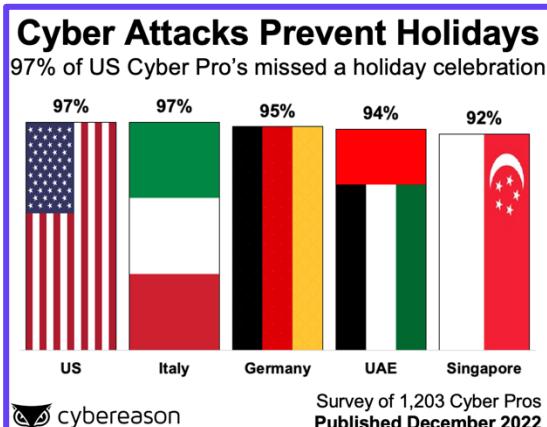
54% of Internal Auditors focus on Password Policies



Survey of U.S. Internal Audit Executives  
Published December 2022

# Cyber Insights: Cyber Humans

Click each image to see each report in full. All were published in month to January 2023



# Cyber Insights: Cyber Trends

Click each image to see each report in full. All were published in month to January 2023

### Cyber Threat Nations

75% of UK Manufacturers fear threat from Russia

Nation	Percentage
EU	25%
UK	38%
China	74%
Russia	75%

**MAKE uk**  
The Manufacturers' Organisation

Survey of UK Manufacturers  
Published December 2022

### Insecure Security Cameras

# of Surveillance Cameras with default password

Country	Count
Russian Federation	74,573
Republic of Korea	159,964
China	160,206
United Kingdom	248,933
United States	458,022

**cybernews**

Published December 2022

### Phishing & Malicious Emails

19% of Email-borne Attacks in Construction

Sector	Percentage
Construction	19%
Retail	18%
Real Estate	18%
Services	15%
Finance	11%
Manufacturing	6%
Computers & IT	6%
Other	7%

**Acronis**

From July to November 2022  
Published December 2022

### Most Frequent Cyber Incidents

49% say Ransomware is the Most Frequent incident

Incident Type	Percentage
Ransomware	49%
Supply Chain Attack	46%
Targeted Attack	31%

**cybereason**

Survey of 1,203 Cyber Pros  
Published December 2022

### Threat Vectors

Phishing continues to be the top threat at 76%

Threat Vector	Percentage
Phishing	76%
Malware	18%
Advanced Attack	3%
BEC	3%

**Acronis**

From July to November 2022  
Published December 2022

### Cyber Challenges of Firms

49% of firms lack Security for Digital Supply Chain

Challenge	Percentage
Increasing number of threats	43%
Employees circumventing protocols	47%
Expanded defense perimeter	48%
Increasing complexity of threats	48%
Digital supply chain	49%

**LogRhythm**

1,175 Security Pros & Executives  
Published December 2022

### Risk from Links to Suppliers

Finance Firms typically have 5 "critical" risky links

Industry	Links
Finance	2
Retail	4
Industry	18
Health	23
Food	28

**Cyberpion**

Published December 2022

### Demands for Cyber "Proof"

91% of firms must prove their security to Customers

Party	Percentage
Customers	91%
Partners	85%

**LogRhythm**

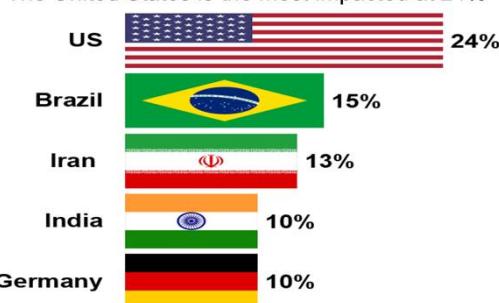
1,175 Security Pros & Executives  
Published December 2022

# Cyber Insights: *Ransomware*

Click each image to see each report in full. All were published in month to January 2023

## Top 5 Countries hit by Ransom

The United States is the most impacted at 24%



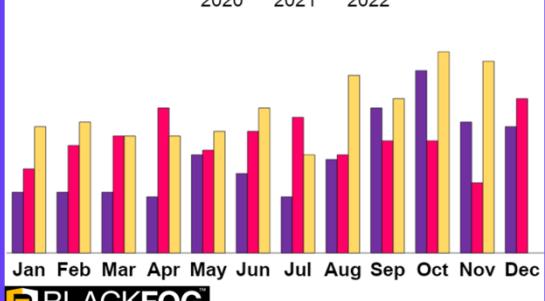
Bitdefender

Published December 2022

## # of “Successful” Ransoms

November had the 2<sup>nd</sup> highest number in 3 years

■ 2020 ■ 2021 ■ 2022



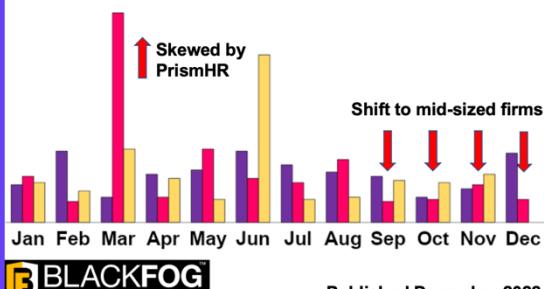
BLACKFOG  
Privacy. Security. Prevention.

Published December 2022

## Size of Ransom Victims

Active Hackers continue to focus on smaller firms

■ 2020 ■ 2021 ■ 2022



BLACKFOG  
Privacy. Security. Prevention.

Published December 2022

## Ransom Gangs in Finance

LockBit cause 41% of Ransom Attacks in Finance

LockBit

41%

Corp Leaks

13%

Conti

7%

BlackCat

7%

Other

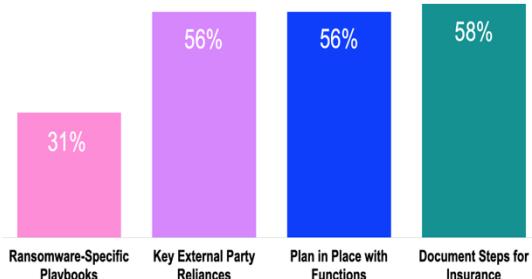
32%

FLASHPOINT

Data based on leak site data (Flashpoint)  
Published December 2022

## Ransom Risk Reduction

Firms reduce Ransom Risk by Better Documents

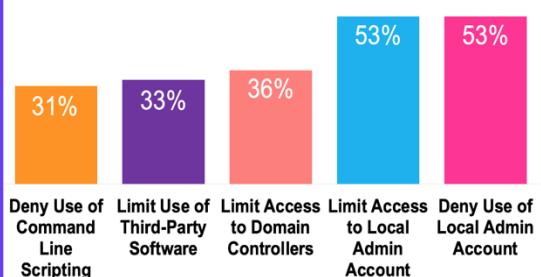


axio

Survey of 65 core practices arranged in 8 domains  
Published December 2022

## Ransom Risk Reduction

Firms reduce Ransom Risk by Restricting Access



axio

Survey of 65 core practices arranged in 8 domains  
Published December 2022

## Addressing Rise in Ransom

38% of firms implementing new detection capability

New detection capabilities

38%

Augmenting staff

31%

Automate detection/response

29%

Learn to negotiate ransoms

27%

Making crypto wallets to pay

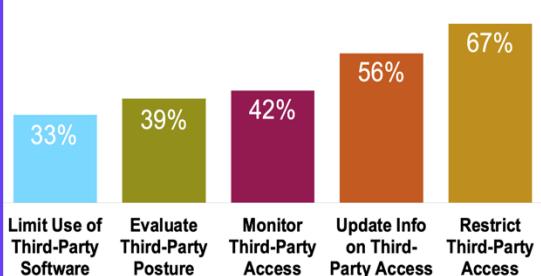
27%

cybereason

Survey of 1,203 Cyber Pros  
Published December 2022

## Ransom Risk Reduction

Firms reduce Ransom Risk by Manage 3rd Parties

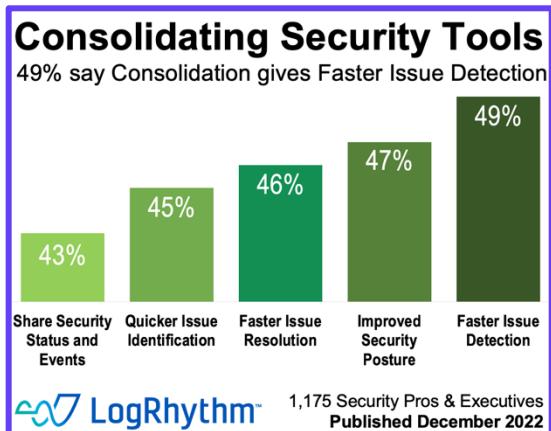
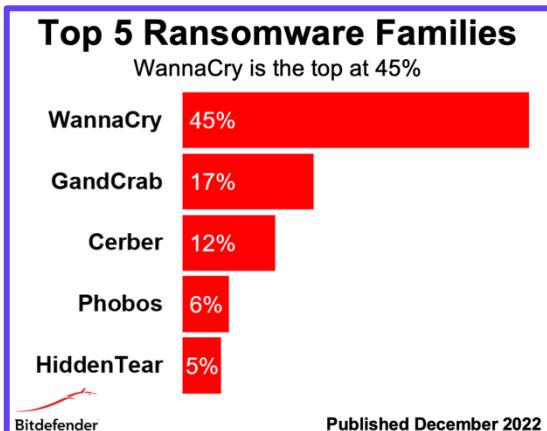
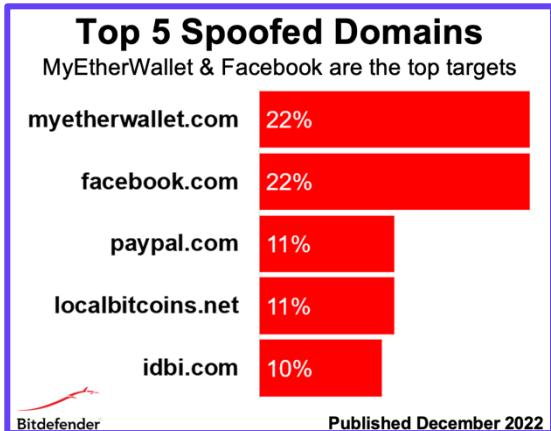
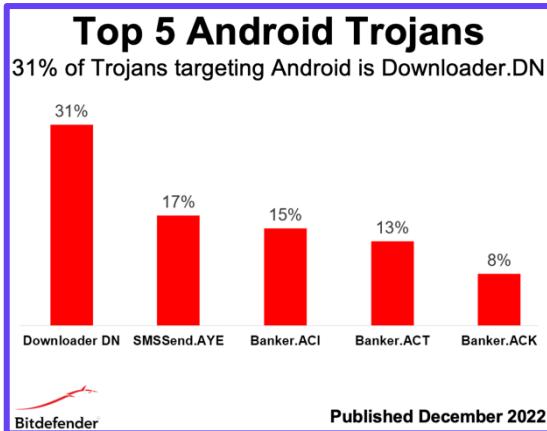
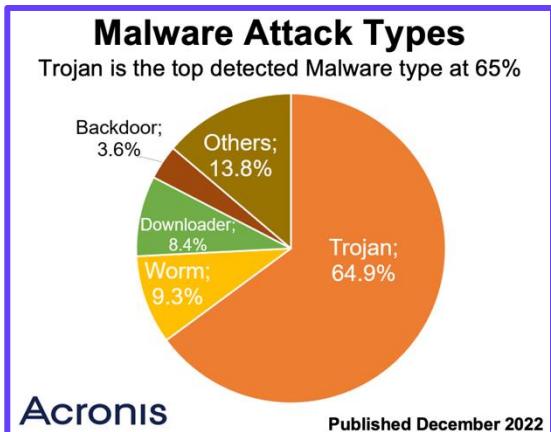
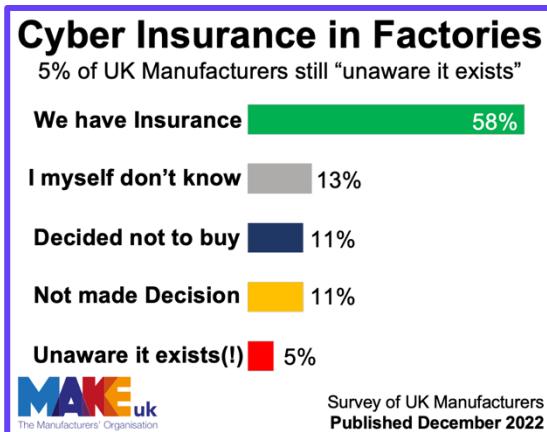
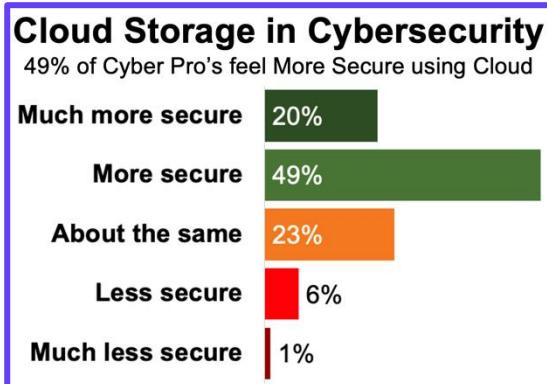


axio

Survey of 65 core practices arranged in 8 domains  
Published December 2022

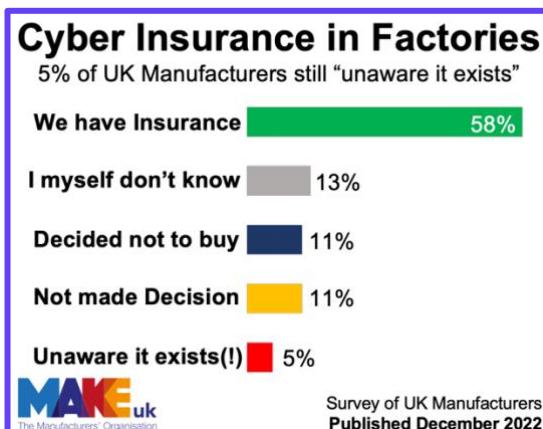
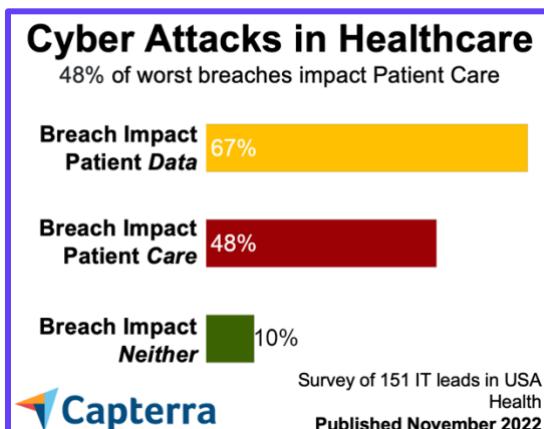
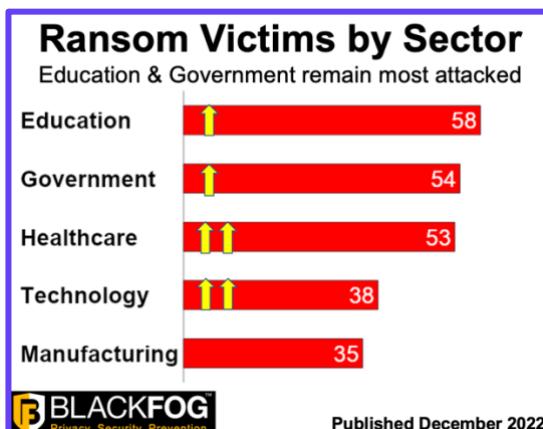
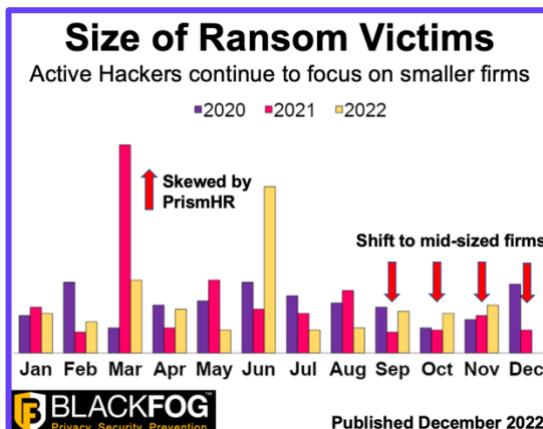
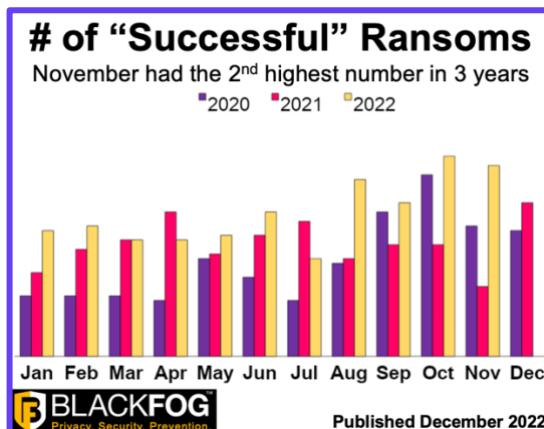
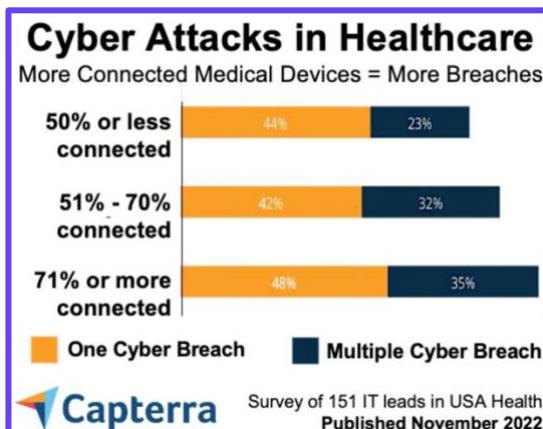
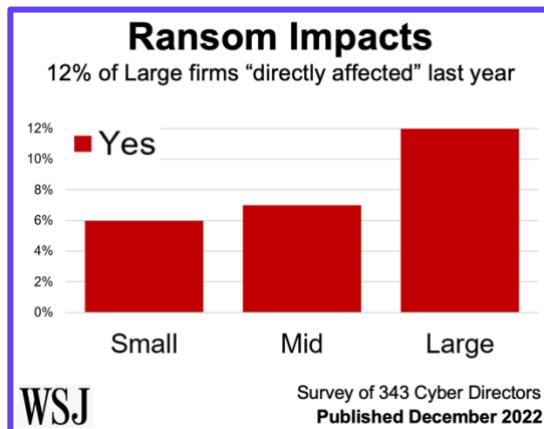
# Cyber Insights: Cyber Trends

Click each image to see each report in full. All were published in month to January 2023



# The Best Cyber Insights of 2022

Click each image to see each report in full. All were published in month to Dec 2022



# The Best Cyber Insights of 2022

Click each image to see each report in full. All were published in month to December 2022

## INTERPOL's Crime Forecast

Ransomware is "crime most likely to increase"

#1 = Ransomware

#2 = Phishing & Online Scams

#3 = Online Child Sexual Abuse

#4 = Business Email Compromise

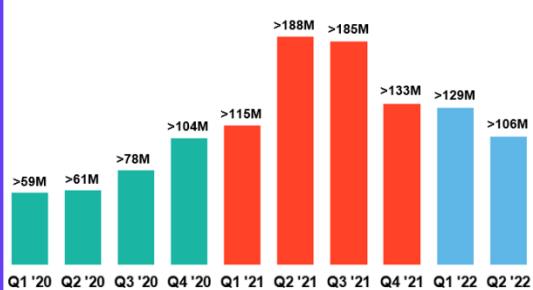
#5 = Computer Intrusion



Global Survey of Police Forces  
Published November 2022

## Ransom "Attacks" Volume

Good News as ransom attack volumes are declining

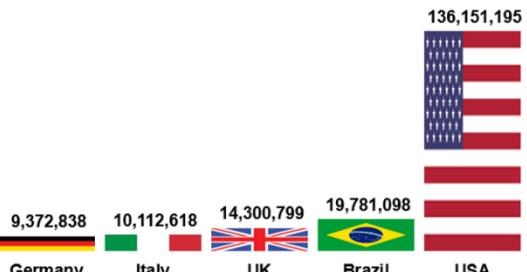


SONICWALL

Published November 2022

## Ransom "Attacks" Volume

136 million Ransom attempts on US Firms this year

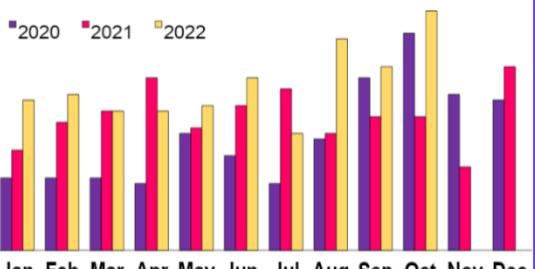


SONICWALL

Published November 2022

## Ransom "Success" Volume

Last month had most Ransom "successes" ever

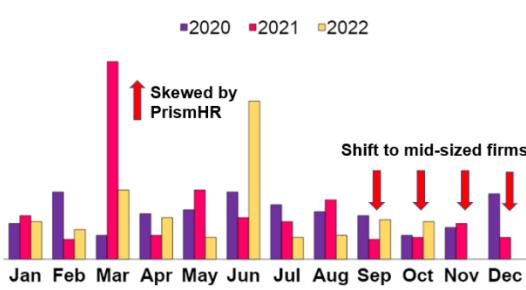


BLACKFOG

Published November 2022

## Size of Ransom Victim Firms

Active Hackers continue to focus on smaller firms

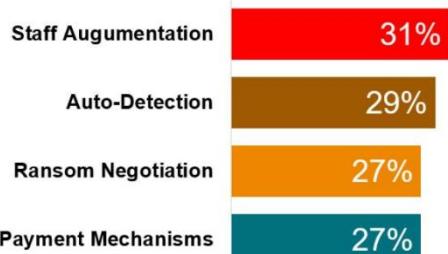


BLACKFOG

Published November 2022

## Ransom Redress

27% are learning to negotiate with Ransom Actors

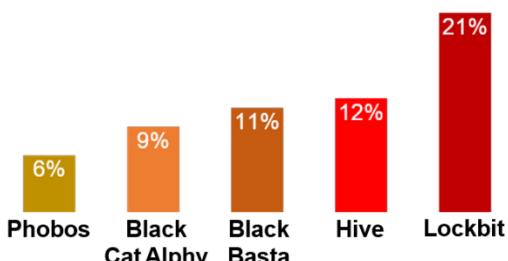


cybereason

Survey of 700 Cybersecurity Professionals  
Published November 2022

## Top Ransomware Gangs

Lockbit is responsible for most "successful" attacks

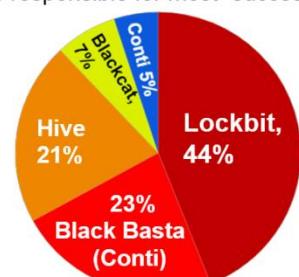


KROLL

Published November 2022

## Top 5 Ransomware Gangs

Lockbit is responsible for most "successful" attacks

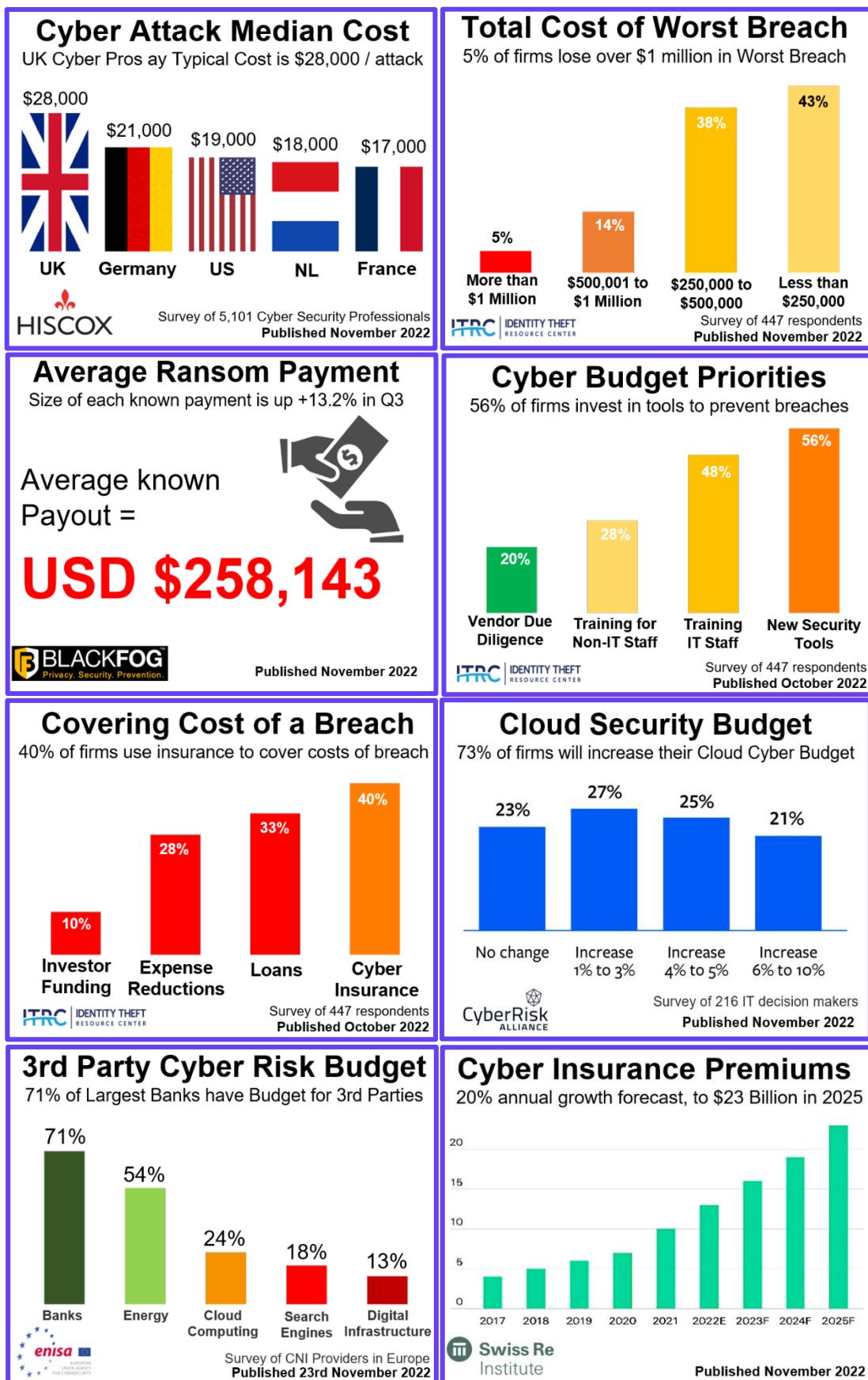


deepinstinct

Analysis of Deep Instinct Data  
Published November 2022

# Cyber Insights: Cyber Finances

Click each image to see each report in full. All were published in month to December 2022



# Cyber Insights: Cyber Insurance

Click each image to see each report in full. All were published in month to December 2022

### Cyber Insurance Prices

78% of Brokers say Price for Cyber Insurance rising

Category	Q2 2022 (%)	Q3 2022 (%)
Flood	19%	34%
Umbrella	32%	40%
Commercial Property	50%	37%
Cyber	85%	78%

**THE COUNCIL**  
The Council of Insurance Agents & Brokers  
Published November 2022

### Cyber Insurance Prices

Premium Price increased by 20.3% in last quarter

Quarter	Year	Percentage Change
Q2	17	-1.4%
Q1	18	0.4%
Q2	19	1.2%
Q1	20	4.4%
Q2	20	7.7%
Q3	20	25.5%
Q4	21	34.3%
Q3	22	20.3%

**THE COUNCIL**  
The Council of Insurance Agents & Brokers  
Published November 2022

### Cyber Insurance: Why Buy?

33% buy insurance as "it's a Board Requirement"

Reason	Percentage
Risk Reduction	40%
Board Requirement	33%
Ransom Incident	24%
Compliance	20%
No Reason	2%

**Delinea**  
Survey of 301 IT decision makers in USA  
Published November 2022

### Cyber Insurance: Why Buy?

79% of firms have claimed on their Cyber Insurance

Frequency	Percentage
No	20%
Once	37%
Multiple Times	41%
Yes(net)	79%

**Delinea**  
Survey of 301 IT decision makers in USA  
Published November 2022

### Cyber Insurance Adoption

74% in Finance sector are using Cyber Insurance

Industry	Percentage
Financial Services	74%
Tech, Media, & Telecoms	71%
Manufacturing	68%
Energy	66%
Transport & Distribution	64%

**HISCOX**  
Survey of 5,101 Cyber Security Professionals  
Published November 2022

### Cyber Insurance Adoption

69% in Ireland say they are using Cyber Insurance

Country	Percentage
Ireland	69%
Germany	67%
Spain	66%
US	65%
UK	62%

**HISCOX**  
Survey of 5,101 Cyber Security Professionals  
Published November 2022

### Cyber Insurance Claims

Professional Services & Health make most claims

Sector	Avg. Incident Cost	Number of Claims
Healthcare	~75	~1100
Professional services	~180	~1100
Other	~150	~800
Financial services	~50	~500
Manufacturing	~180	~400
Non profit	~50	~300
Public entity	~50	~200
Education	~50	~150
Retail	~100	~300
Technology	~300	~100

**Swiss Re Institute**  
Published November 2022

### Cyber Insurance: Why Buy?

51% of policies require firms to train staff on cyber

Reason	Percentage
CyberSec Trainings	51%
Malware Protection	48%
Backup Data	47%
MFA	47%
Antivirus	47%

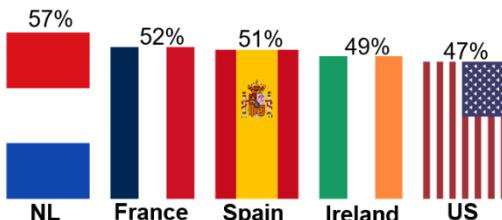
**Delinea**  
Survey of 301 IT decision makers in USA  
Published November 2022

# Cyber Insights: By Country & By Sector

Click each image to see each report in full. All were published in month to December 2022

## Cyber Attacks per Country

57% in NL say they have experienced Cyber Attack

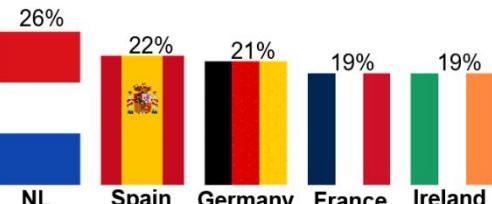


HISCOX

Survey of 5,101 Cyber Security Professionals  
Published November 2022

## Ransom Attacks by Country

26% in NL say they have experienced Ransomware

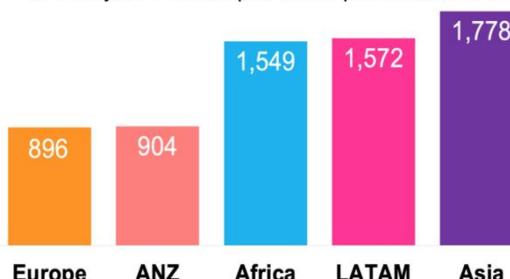


HISCOX

Survey of 5,101 Cyber Security Professionals  
Published November 2022

## Cyber Attacks per Region

1,778 Cyber Attacks per Week per Firm in Asia

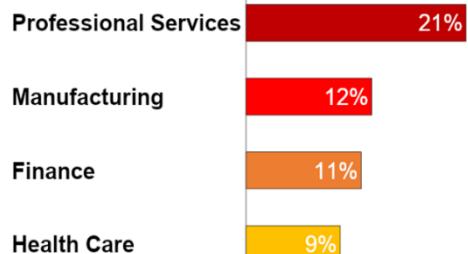


CHECK POINT

Published November 2022

## Most Targeted Sectors

21% of Cyberattacks targeted Professional Services

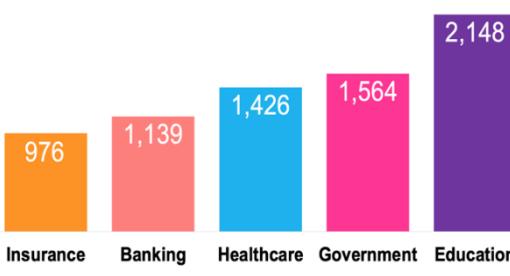


KROLL

Analysis of Kroll's Incident Response  
Published November 2022

## Most Targeted Sectors

Education tops at number 1 with 2,148 attacks

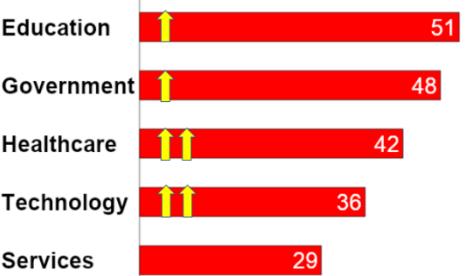


CHECK POINT

Analysis of CheckPoint's Customers  
Published November 2022

## Ransom Victims by Sector

Education & Government most attacked in October

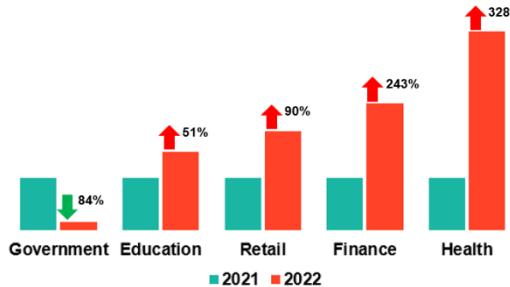


BLACKFOG

Published November 2022

## Ransomware by Industry

Finance & Healthcare saw triple-digit increases

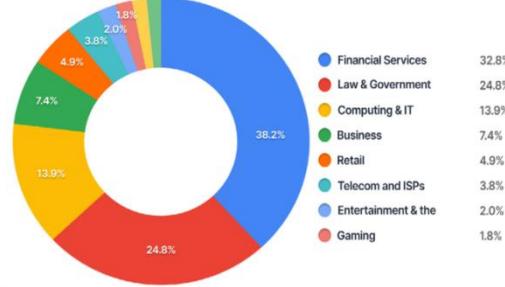


SONICWALL

Published November 2022

## DDoS Attacks by Sector

33% of Denial of Service attacks now target Finance



imperva

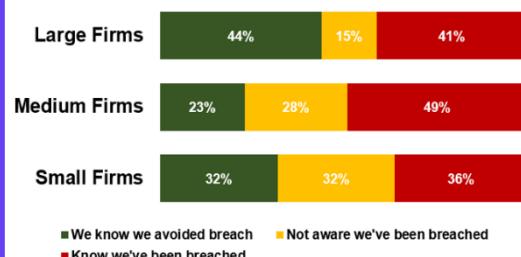
Published November 2022

# Cyber Insights: Cyber for Industrial Control

Click each image to see each report in full. All were published in month to December 2022

## Breaches at Manufacturers

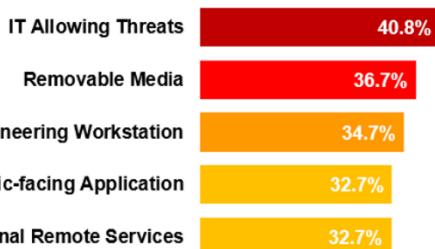
41% of Large Firms know they have been breached



Survey of 350 Industrial Firms  
Published November 2022

## Cyber for Industrial Control

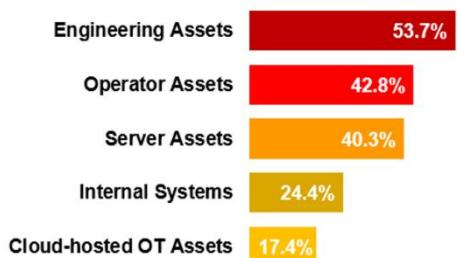
What are the top Initial Attack Vectors?



Survey of 332 professionals  
Published November 2022

## Cyber for Industrial Control

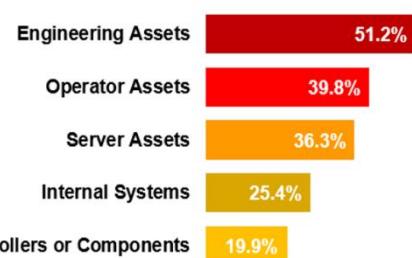
What System Components **likeliest** to be breached?



Survey of 332 professionals  
Published November 2022

## Cyber for Industrial Control

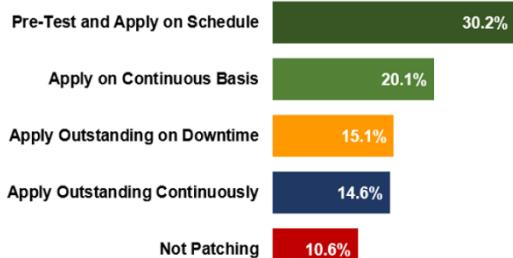
Which component has greatest **Impact** if breached?



Survey of 332 professionals  
Published November 2022

## Cyber for Industrial Control

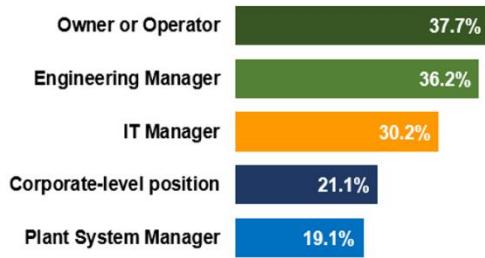
How do you implement **Patching** and updates?



Survey of 332 professionals  
Published November 2022

## Cyber for Industrial Control

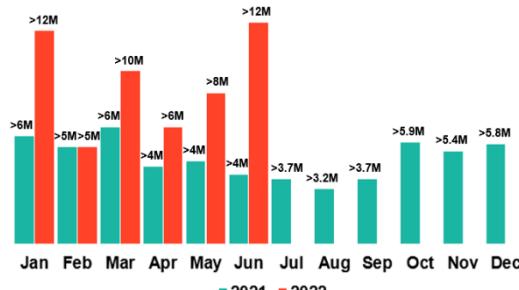
Who should **Maintain** Security Controls?



Survey of 332 professionals  
Published November 2022

## IoT Malware Volume Doubled

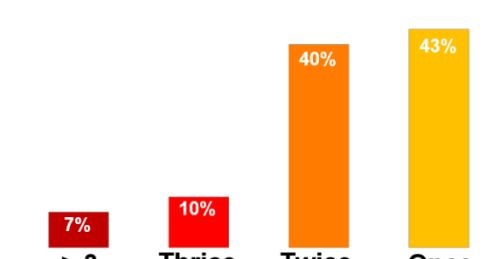
Internet of Things devices under accelerating attack



Published November 2022

## Frequency of Data Breach

43% of firms report being breached at least once



Survey of 447 respondents  
Published October 2022

# Cyber Insights: Cyber Risks & Vectors

Click each image to see each report in full. All were published in month to December 2022

## Top Global Emerging Risks

Cloud Concentration Risk is "Top Right" Priority

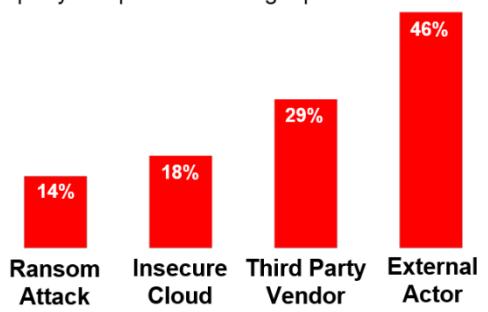


**Gartner**

333 Executives & Risk Managers  
Published 15th November 2022

## Sources of Data Breaches

3rd party compromise among top causes of breach



**ITRC** IDENTITY THEFT RESOURCE CENTER

Survey of 447 respondents  
Published October 2022

## Going Digital vs Cyber Risks

What are key challenges on new Digital initiatives?

Exposure To Security Risks 55%

Cost Of Disruption 41%

Finding The Right Partner 38%

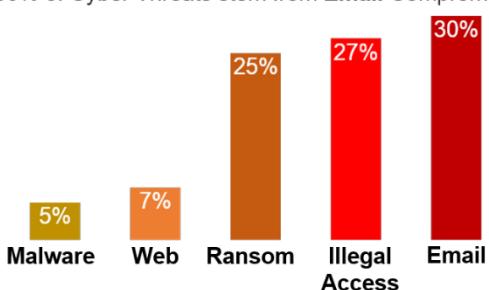
Lack Of Staff Experience 37%

**DLA PIPER**

Survey of Senior Execs from 350 Companies  
Published November 2022

## Most Worrying Cyber Threats

30% of Cyber Threats stem from Email Compromise

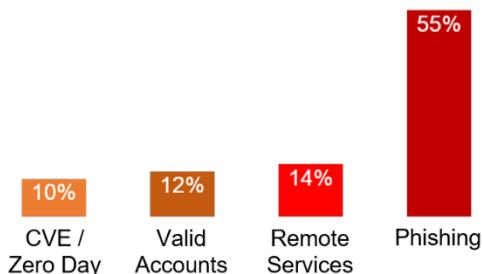


**KROLL**

Published November 2022

## Top Initial Access Methods

The Top Initial Access Method is Phishing at 55%



**KROLL**

Published November 2022

## False Sense of Security

62% use the same password across all accounts

62%  
...use the same password or a variation.

33%  
...create stronger passwords for their work accounts.

50%  
...ever change their password after a breach.

**LastPass** •••

Survey of 3,750 Professionals  
Published November 2022

## Cyber Threat Vectors

Phishing attacks are top concern for half of firms

We consider the primary IT security threat to our organization to be...



**SPANNING**  
A Kaseya COMPANY

Survey of more than 650 IT professionals  
Published November 2022

## Cyber Threat Response

Phishing Awareness is top priority for 36% of firms

Our organization's top priority this year is...



**SPANNING**  
A Kaseya COMPANY

Survey of more than 650 IT professionals  
Published November 2022

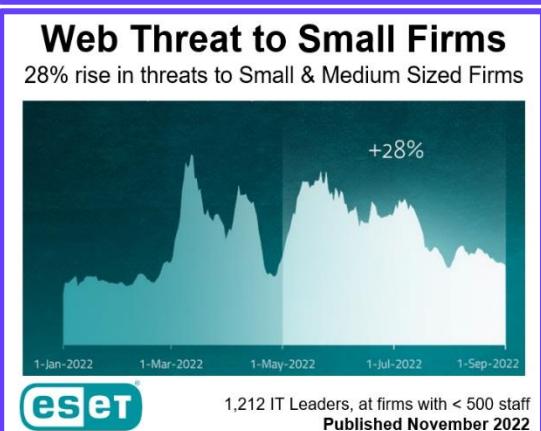
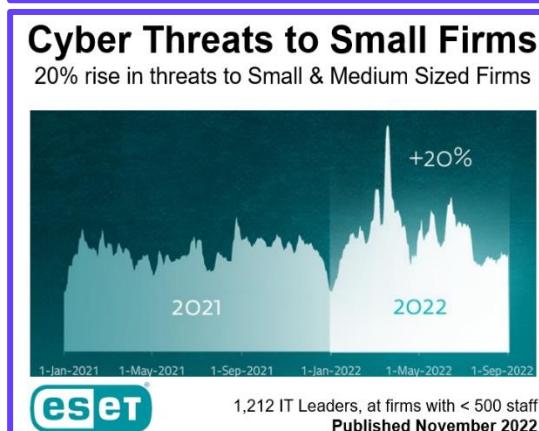
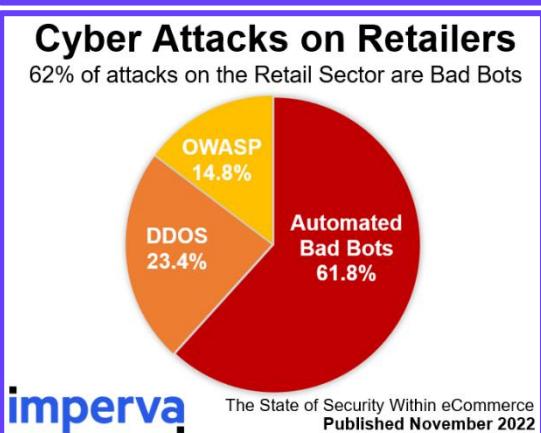
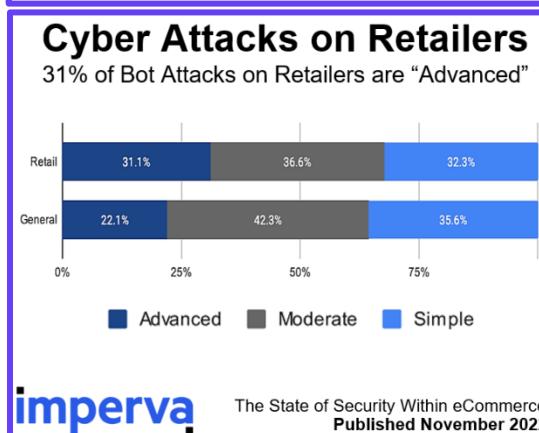
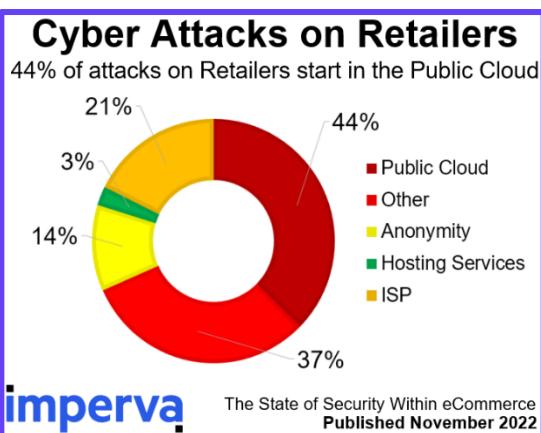
# Cyber Insights: *Detailed Reports*

Click each image to see each report in full. All were published in month to December 2022

<p><b>MANDIANT</b> Published November 2022</p> <p><b>Cyber Security Forecast</b> Adversaries for 2023</p>	<p><b>ACSC</b> Australian Cyber Security Centre Published Nov 2022</p> <p><b>Annual Cyber Threat Report</b> Cyber Threats Affecting Australia</p>
<p><b>CSCA</b> Published Nov '22</p> <p><b>Cyber Crisis Management</b> Exercises for Decision-Making</p>	<p><b>CSCA</b> Cyber Security &amp; Incident Response Center Published Nov '22</p> <p><b>Triage Cyber Vulnerabilities</b> How to Prioritize your Patching</p>
<p><b>NIST</b> Published Nov '22</p> <p><b>Cyber Performance Goals</b> Official Best Practice for USA Firms</p>	<p><b>BSI</b> Bundesamt für Sicherheit in der Informationstechnik Published Oct 2022</p> <p><b>German Cyber Security</b> Annual Review</p>
<p><b>enisa</b> European Network and Information Security Agency Published Nov 2022</p> <p><b>Cyber Threat Landscape</b> Annual Review</p>	<p><b>TEAM8</b> Published Nov 2022</p> <p><b>CISO Guide</b> Legal Risks &amp; Liabilities</p>

## Cyber Insights: *Retailers & Small Firms*

**Click each image** to see each report in full. All were published in month to December 2022

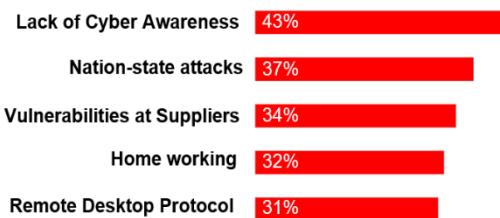


# Cyber Insights: Cyber Hygiene

Click each image to see each report in full. All were published in month to December 2022

## Cyber Risk “Root Causes”

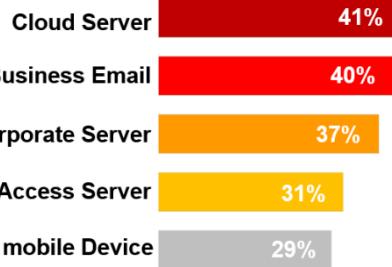
Small Firms say risk from Lack of Cyber awareness



1,212 IT Leaders at firms with < 500 staff  
Published November 2022

## Cyber Attack Vectors

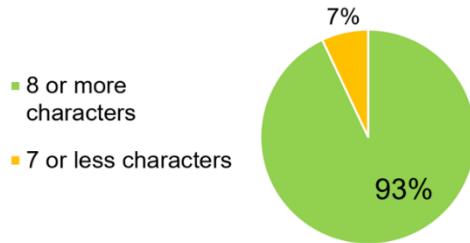
41% say cloud servers are now the #1 attack vector



Survey of 5,101 Cyber Security Professionals  
Published November 2022

## Password Brute Forcing

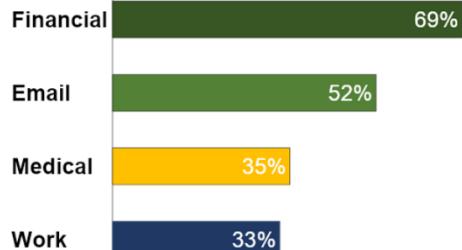
93% of attacks use passwords w/ 8 or more chars



Data Analysis of over 800M files  
Published November 2022

## Password Complexity

What online accounts have complex passwords?



Survey of 3,750 Professionals  
Published November 2022

## Top 10 Password Attacks

used in real brute force attacks with 12 characters

1	^_@\$\$wanniMaBl:: 1433 vl	6	P@ssw0rd5tgb
2	almalinux8svm	7	adminbigdata
3	dbname=template0	8	Pa\$\$w0rdpl#@#
4	shabixuege!@#	9	adm1nistrator1
5	@\$\$W0rd0123	10	administrator!@#\$



Data Analysis of over 800M files  
Published November 2022

## Common Passwords

The most common musicians found in passwords

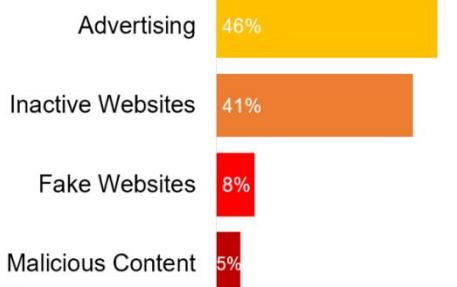
1	R.E.M	6	ABBA
2	Cher	7	Queen
3	Pink	8	Enya
4	Prince	9	Drake
5	Kiss	10	Jay-Z



Data Analysis of over 800M files  
Published November 2022

## Cyber Risk of “Look Alikes”

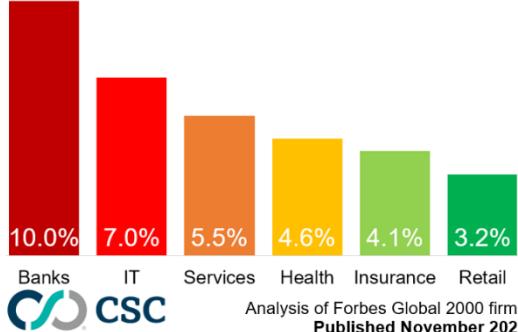
5% of homoglyph websites host malicious code



Analysis of Forbes Global 2000 firms  
Published November 2022

## Cyber Risk of “Look Alikes”

10% of “homoglyph” websites impersonate Banks



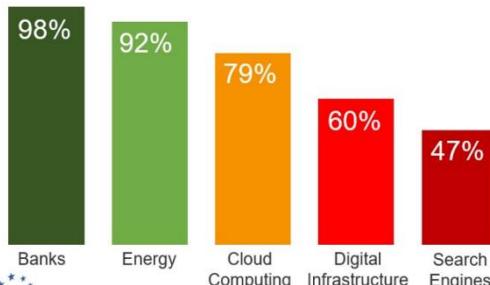
Analysis of Forbes Global 2000 firms  
Published November 2022

# Cyber Insights: *Clouds & Networks*

Click each image to see each report in full. All were published in month to December 2022

## 3rd Party Cyber Risk Policies

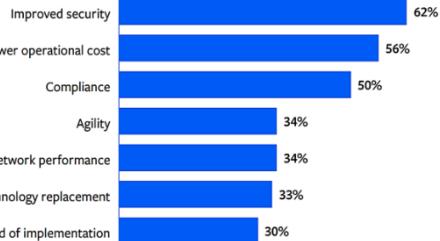
98% of Largest Banks have Policy about 3rd Parties



Survey of CNI Providers in Europe  
Published 23rd November 2022

## Cloud Security Goals

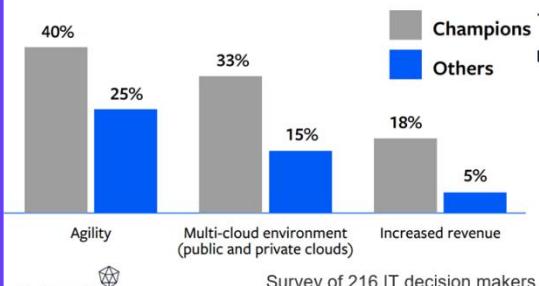
56% of top goals include Lower Operational Cost



Survey of 216 IT decision makers  
Published November 2022

## Cloud Security Goals

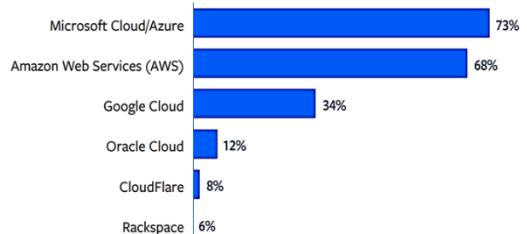
40% "Champion" firms' top goal is Cloud Agility



Survey of 216 IT decision makers  
Published November 2022

## Cloud Security Platforms

73% of firms currently use Microsoft Cloud/Azure



Survey of 216 IT decision makers  
Published November 2022

## Cyber Network Monitoring

Most Breaches were against firms with monitoring

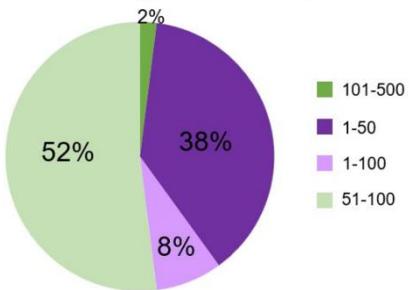
**Breaches in the last year relative to network monitoring capabilities**



Survey of more than 650 IT professionals  
Published November 2022

## Network Security

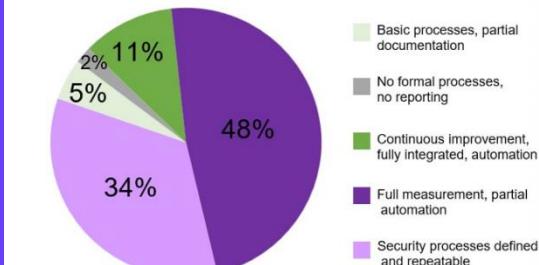
Number of misconfigurations in the past 12 months



Published November 2022

## Security of Firewalls

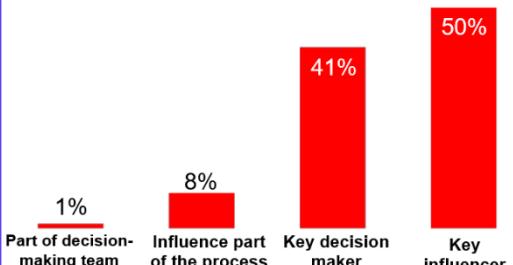
48% said that they had full measurement



Published November 2022

## Network Security Role

How organizations detect vulnerabilities



Survey of 160 senior cybersecurity in U.S.  
Published November 2022

# Cyber Insights: Cyber Security Prioritisation

Click each image to see each report in full. All were published in month to December 2022

## Cyber Security as Priority

Do you expect cyber security as your prime concern?

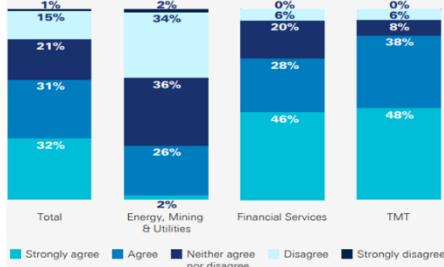


pillsbury

Survey of 150 corporate executives  
Published November 2022

## Cyber Security as Priority

Is Cybersecurity and cyber risk mitigation essential?

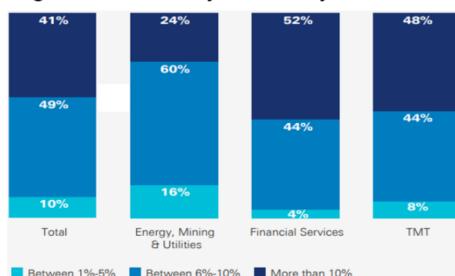


pillsbury

Survey of 150 corporate executives  
Published November 2022

## Cyber Security as Priority

Budget allocated to cybersecurity-related matter



pillsbury

Survey of 150 corporate executives  
Published November 2022

## Cyber Security as Priority

Biggest Cybersecurity-Related challenge

Rank 1-2, where 1=biggest challenge

Rate of increase of cyberattacks

**25%** **18%**

Pace of technological innovation

**19%** **19%**

Sourcing in-house cybersecurity expertise

**19%** **13%**

Training all our employees in proper cybersecurity practice

**15%** **9%**

■ 1 ■ 2

pillsbury

Survey of 150 corporate executives  
Published November 2022

## Cyber Security Attack types

What is the common attack in your organization?



pillsbury

Survey of 150 corporate executives  
Published November 2022

## Cyber Security Priorities

What do you think will be the most important trend?

Rank 1-2, where 1=most important

Better tools and processes for identifying threat detection and response

**25%** **13%**

The rise of ransomware attacks

**21%** **10%**

Companies increasingly turning to artificial intelligence

**10%** **13%**

The security challenges of a distributed/remote workforce

**9%** **5%**

■ 1 ■ 2

pillsbury

Survey of 150 corporate executives  
Published November 2022

## Cyber Insurance Purchased?

Do you have dedicated cybersecurity insurance?

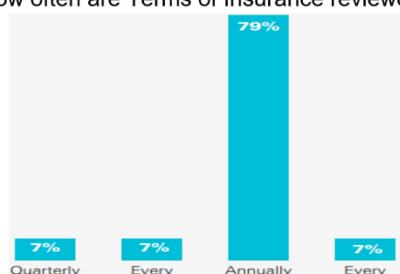


pillsbury

Survey of 150 corporate executives  
Published November 2022

## Cyber Insurance Reviewed?

How often are Terms of Insurance reviewed?



pillsbury

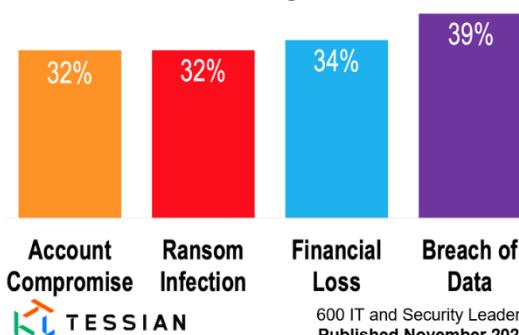
Survey of 150 corporate executives  
Published November 2022

# Cyber Insights: *Phishing & Malware*

Click each image to see each report in full. All were published in month to December 2022

## Phishing Attack Outcomes

39% of Successful Phishing Attacks cause Breach



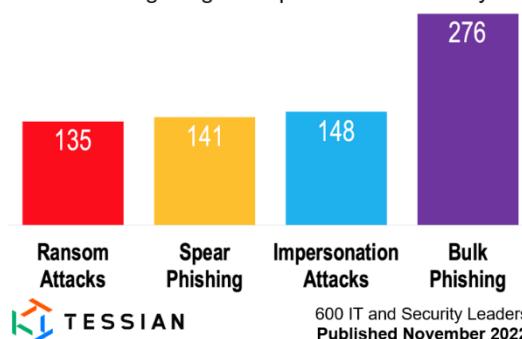
## Email Impersonation Attacks

Firms with 1,000+ Staff hit by 205 Spear Phish p.a.



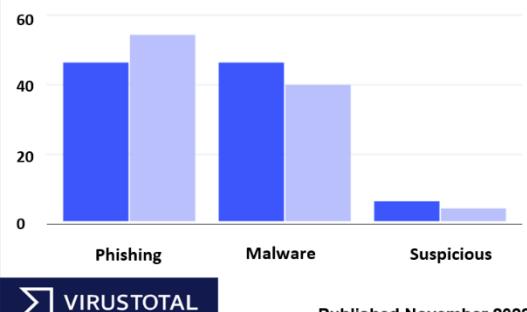
## Email Attack Volume

Global Firms getting 141 Spear Phish emails / year



## Phishing vs Malware

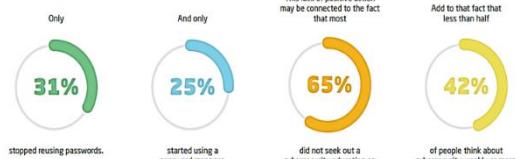
Most Attacks are still dominated by Phishing



## Cyber Education Benefits

31% of Staff stop reusing passwords after Training

**Of those who received a cybersecurity education,**



LastPass...!

Survey of 3,750 Professionals  
Published November 2022

## Cyber Security for Domains

61% use DMARC authentication & conformance



## K-12 School Cyber Concerns

Top concern is insufficient budget for Cyber Security

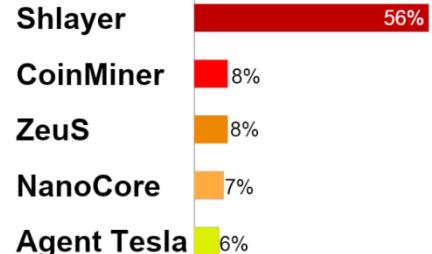
- #1 Lack of Sufficient Funding
- #2 Increasing Sophisticated Threats
- #3 Poor Documented Processes
- #4 Lack of Cyber Strategy
- #5 Availability of Cyber Experts

CIS Center for Internet Security

Survey of 14,000 Org. Members  
Published November 2022

## Malware for K-12 Schools

56% of Malware attacks now by Shlayer



CIS Center for Internet Security

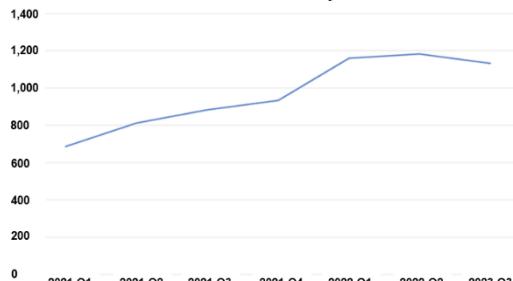
Survey of 14,000 Org. Members  
Published November 2022

# Cyber Insights: Cyber Attacks

Click each image to see each report in full. All were published in month to December 2022

## Increase in Cyber Attacks

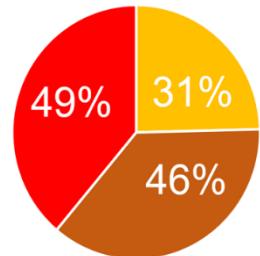
Global attacks increased by 28% in 2022



Published November 2022

## Common Cyber Attacks

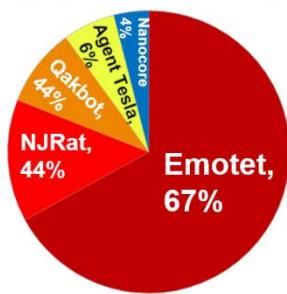
49% of firms have experienced Ransomware



Survey of 700 Cybersecurity Professionals  
Published November 2022

## Top Bank Trojans & Spyware

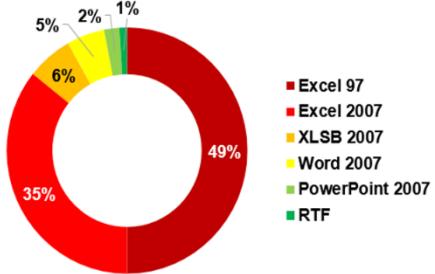
67% of Bank Trojans & Spyware now Emotet



Analysis of Deep Instinct Data  
Published November 2022

## Malicious Microsoft Files

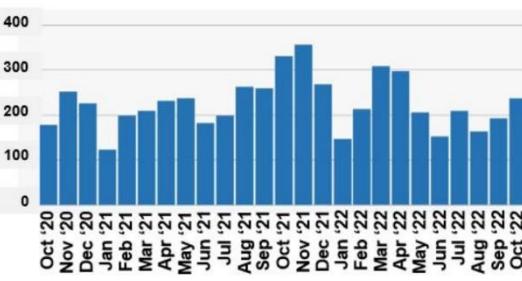
Excel Files most likely to have malwares in Microsoft



Published November 2022

## Released Data by Ransom

Most victim data released in Oct. in the last 5 mos.



Published November 2022

## Cyber Attack Effects

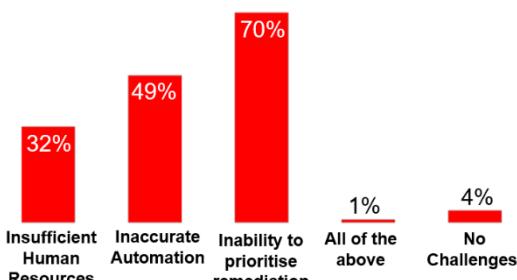
21% say Worst Attack threatened firm's Solvency



Survey of 5,101 Cyber Security Professionals  
Published November 2022

## Main Security Challenges

Inability to Prioritise Remediation is highest at 70%



Published November 2022

## Attacks on Social Media

87% of firms report revenue loss after account hack



Survey of 447 respondents  
Published October 2022

# Cyber Insights: Cyber Finances

Click each image to see each report in full. All were published in month to December 2022

### Ransomware Gangs

22% of Ransoms paid go to Lockbit Ransom Gang

Gang	Percentage
BlackCat	22%
Phobos	10%
HelloXD	10%
Lockbit	11%

**Trellix** Published November 2022

### Ransomware Tools

33% Global Ransom Tools are Cobalt Strike

Tool	Percentage
WinPEAS	6%
RCLONE	10%
Mimikatz	33%
Cobalt Strike	22%

**Trellix** Published November 2022

### NIS Investments

Published Nov 2022

**Trellix** Published November 2022

### Top Cyber Spending Focuses

Spending priorities of Large Firms with 1,000+ staff

- #1 = Existing threats & vulnerabilities
- #2 = Achieving Regulatory Compliance
- #3 = Updated Policies & Procedures
- #4 = Improved security of app & svcs
- #5 = Security management framework

**HISCOX**

Survey of 5,101 Cyber Security Professionals  
Published November 2022

### Cyber Insurance: Why Buy?

49% of Insurance Policies pay for Data Recovery

Reason	Percentage
Data Recovery	49%
Monitoring Services	38%
Improvement Costs	37%
Incident Response	36%
Device Replacement	35%

**Delinea**

Survey of 301 IT decision makers in USA  
Published November 2022

### Email Attacks

68% of Email Attacks are Phishing

Type	Percentage
Scam	9%
Malware	22%
Phishing	68%

**Trellix** Published November 2022

### Microsoft 365 Security Benchmark

Published Nov 2022

**Trellix** Published November 2022

### Top Domains Attacked

Web Hosting is the most attacked in 2022

Category	Percentage
Government	Low
Health	Low
Education	Low
Economy	Medium
Web Hosting	High

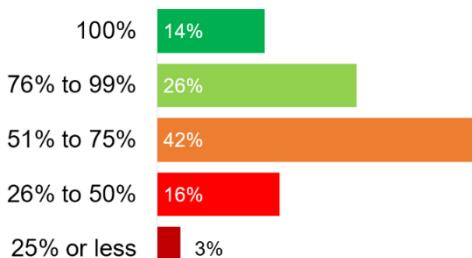
**VIRUSTOTAL** Published November 2022

# Cyber Insights: *Ransomware*

Click each image to see each report in full. All were published in month to December 2022

## Data Recovery after Ransom

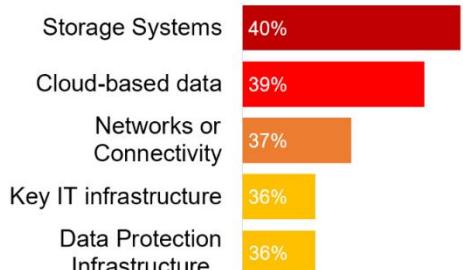
% of Data Recovered after Paying Ransom



Survey of 620 IT & CyberSecurity Pros  
Published November 2022

## Systems hit by Ransomware

39% of Ransomware targets Cloud-based Data



Survey of 620 IT & CyberSecurity Pros  
Published November 2022

## Ransomware Resilience

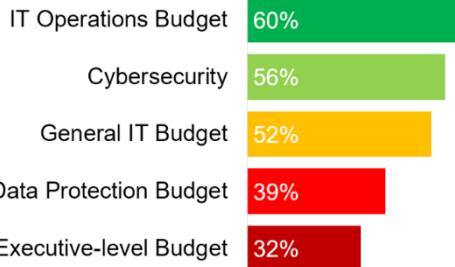
58% of firms Test their Ability to Recover their Data



Survey of 620 IT & CyberSecurity Pros  
Published November 2022

## Ransom Resilience Budget

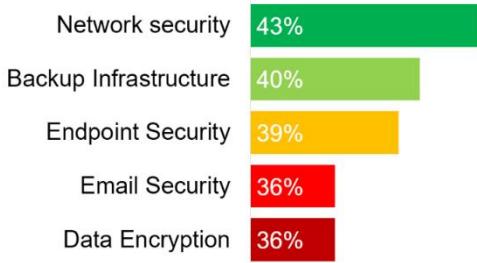
60% of firms fund resilience from IT Ops Budget



Survey of 620 IT & CyberSecurity Pros  
Published November 2022

## Ransom Prevention

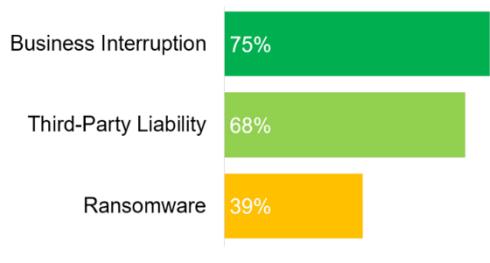
43% say Network Security is most important



Survey of 620 IT & CyberSecurity Pros  
Published November 2022

## Cyber Insurance Purchased

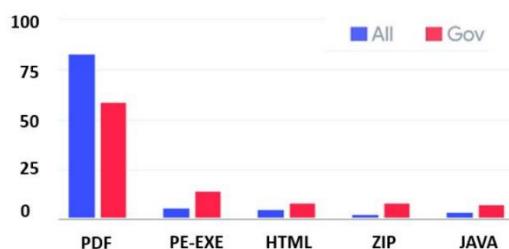
39% of firms buy insurance for Ransomware



Survey of 620 IT & CyberSecurity Pros  
Published November 2022

## Top Suspicious Files

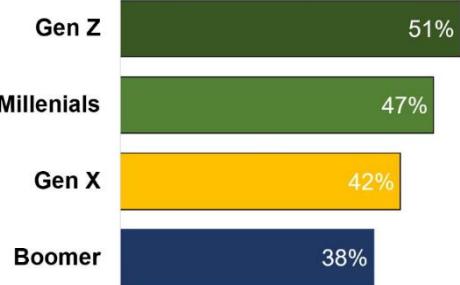
PDF is the most suspicious file type



Published November 2022

## Memorizing Passwords

51% of Gen Z believe memorizing is “very safe”



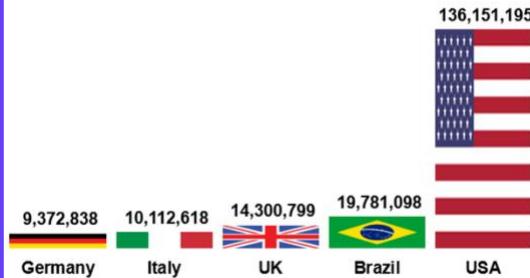
Survey of 3,750 Professionals  
Published November 2022

# The Best Cyber Insights of 2022

Click each image to see each report in full. All were published in month to Nov 2022

## Ransomware Attack Volume

136 million Ransom attempts on US Firms this year

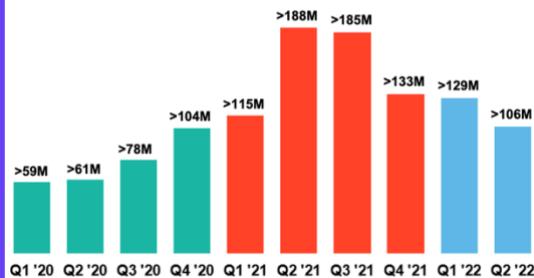


**SONICWALL**

Published November 2022

## Ransomware Attack Volume

Good News as ransom attack volumes are declining



**SONICWALL**

Published November 2022

## Cyber for Industrial Control

Who should maintain Security Controls?

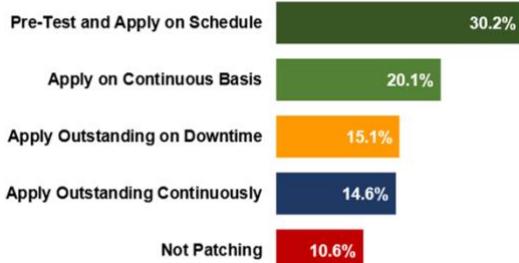


**SANS DRAGOS**

Survey of 332 professionals  
Published November 2022

## Cyber for Industrial Control

How do you implement Patching and updates?

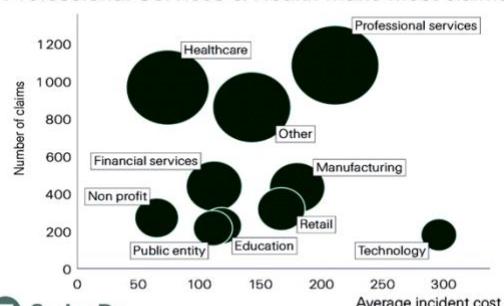


**SANS DRAGOS**

Survey of 332 professionals  
Published November 2022

## Cyber Insurance Claims

Professional Services & Health make most claims

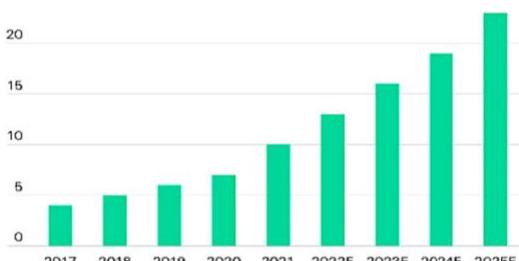


**Swiss Re Institute**

Published November 2022

## Cyber Insurance Premiums

20% annual growth forecast, to \$23 Billion in 2025

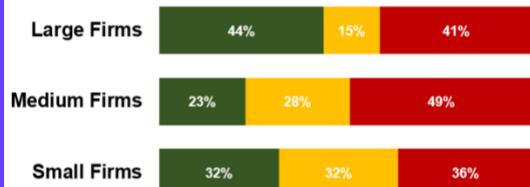


**Swiss Re Institute**

Published November 2022

## Breaches at Manufacturers

41% of Large Firms know they have been breached



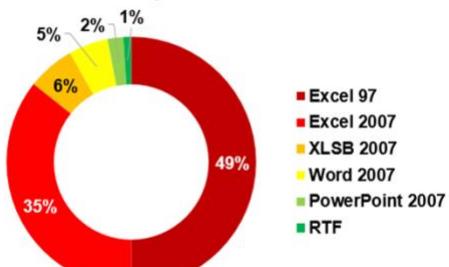
■ We Know we avoided breach  
■ Not aware we've been breached  
■ Know we've been breached

**FT FINANCIAL TIMES**

Survey of 350 Industrial Firms  
Published November 2022

## Malicious Microsoft Files

Excel Files most likely to have malwares in Microsoft



**SONICWALL**

Published November 2022

# The Best Cyber Insights of 2022

Click each image to see each report in full. All were published in month to Nov 2022

### Cyber Budget Priorities

56% of firms invest in tools to prevent breaches

Priority	Percentage
Vendor Due Diligence	20%
Training for Non-IT Staff	28%
Training IT Staff	48%
New Security Tools	56%

Survey of 447 respondents  
Published October 2022

**ITRC | IDENTITY THEFT RESOURCE CENTER**

### Financial Loss After Breach

38% of firms lose \$250k to \$500k after breach

Loss Range	Percentage
More than \$1 Million	5%
\$500,001 to \$1 Million	14%
\$250,000 to \$500,000	38%
Less than \$250,000	43%

Survey of 447 respondents  
Published October 2022

**ITRC | IDENTITY THEFT RESOURCE CENTER**

### Frequency of Data Breach

43% of firms report being breached at least once

Breach Frequency	Percentage
> 3	7%
Thrice	10%
Twice	40%
Once	43%

Survey of 447 respondents  
Published October 2022

**ITRC | IDENTITY THEFT RESOURCE CENTER**

### Cause of Data Breach

3<sup>rd</sup> party compromise among top causes of breach

Cause	Percentage
Ransom Attack	14%
Insecure Cloud	18%
Third Party Vendor	29%
External Actor	46%

Survey of 447 respondents  
Published October 2022

**ITRC | IDENTITY THEFT RESOURCE CENTER**

### Cyber Security Maturity

Australian Execs rate themselves as most mature

Country	Maturity Score
Australia	2.85
UK	2.71
US	2.61

Survey of 750 Senior Execs.  
Published November 2022

**THREATQUOTIENT**

### Cyber Security Automation

More than two-thirds says it is important

Importance Level	Percentage
Increasing budgets	98%
Experienced problems	97%
Says it's important	68%
Issues stop automation	21%

Survey of 750 Senior Execs.  
Published November 2022

**THREATQUOTIENT**

### Cyber Leaders Struggling

CISOs "struggle to keep up with cyber innovations"

Country	Percentage
USA	49%
UK	36%

405 CISOs in firms with > 500 staff  
Published November 2022

**BLACKFOG**

### INTERPOL's Global Top 5

Ransomware is "crime most likely to increase"

- #1 = Ransomware
- #2 = Phishing and Online Scams
- #3 = Online Child Sexual Exploitation
- #4 = Business Email Compromise
- #5 = Computer Intrusion

**INTERPOL**

Global Survey of Police Forces  
Published November 2022

# The Best Cyber Insights of 2022

Click each image to see each report in full. All were published in month to November 2022

### Ransom is most Feared

91% say Ransom is Top 3 cyber concern for them

Cyber Threat	Percentage
Ransomware	91%
Phishing	76%
Encrypted Malware	66%
File-less attacks	39%
Memory-based Malware	24%
Cryptojacking	23%
IoT malware	22%
Side-channel attacks	18%

Survey of SonicWall Customers (80% in USA)  
Published October 2022

**SONICWALL®**

### Firms breached by Ransom

Good news: decline in known Victims since March

Month	Number of Firms Breached
Jan-22	~150
Feb-22	~210
Mar-22	~280
Apr-22	~270
May-22	~210
Jun-22	~150

Secureworks®  
Published October 2022

### Ransom Victims by Sector

Education remained most often breached in Sept

Sector	Number of Victims
Education	44
Government	43
Health	35
Tech	28
Retail	19

↑ indicates increase from previous month

**BLACKFOG**  
Privacy. Security. Prevention.  
Published October 2022

### Ransom Victims by Size

Active Hackers continue to focus on smaller firms

Year	Small	Mid-sized	Large
2020	~10	~10	~10
2021	~15	~15	~10
2022	~20	~20	~10

Skewed by PrismHR  
Shift to mid-sized firms

**BLACKFOG**  
Privacy. Security. Prevention.  
Published October 2022

### Ransom Payments increase

Size of each known payment +8% from Q1/22

Average known Payout =

**USD \$228,125**

**BLACKFOG**  
Privacy. Security. Prevention.  
Published October 2022

### Total Cost / Ransom Incident

The typical Ransom paid (\$262k) is 30% of Total

Category	Amount
Ransom Amount (N=815)	262K
Crisis Services (N=712)	146K
Incident (N=815)	455K

6,339 Cyber Incident Claims Analysis  
Published October 2022

**NetDiligence®**

### Ransoms & Data Exfiltration

Top Ransomware Exfiltration Country: China (25%)

Country	Percentage
China	25%
Russia	15%
Ukraine	10%
Iran	5%
Rest of the World	45%

**BLACKFOG**  
Privacy. Security. Prevention.  
Published October 2022

### Cyber Ransom Laundering

Transfers of Crypto by Ransom Gangs via Ren App

Quarter	Conti	Ryuk	Other	Darkside	Total
Q4 2020	\$0.5m	\$0.7m	\$0.0m	\$0.0m	\$1.2m
Q1 2021	\$0.0m	\$0.0m	\$0.0m	\$0.0m	\$0.0m
Q2 2021	\$16.2m	\$1.2m	\$0.0m	\$0.0m	\$17.4m
Q3 2021	\$31.5m	\$0.0m	\$0.0m	\$0.0m	\$31.5m
Q4 2021	\$49.0m	\$0.0m	\$0.0m	\$0.0m	\$49.0m
Q1 2022	\$9.8m	\$0.0m	\$0.0m	\$0.0m	\$9.8m
Q2 2022	\$45.2m	\$0.0m	\$0.0m	\$0.0m	\$45.2m

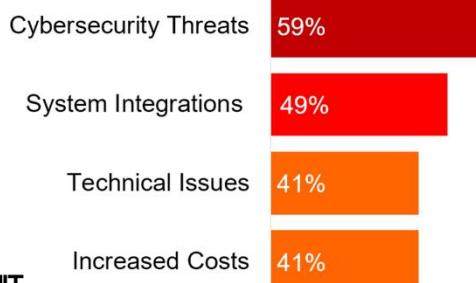
**ELLIPTIC**  
Analysis of Decentralized Exchanges  
Published October 2022

# Cyber Insights: Cyber in Banks

Click each image to see each report in full. All were published in month to November 2022

## Digital Payments Challenges

59% say Cybersecurity is a top challenge



MIT  
Technology  
Review

Published October 2022

## Cyber Challenges for Banks

Reducing Costs now #2 challenge for IT Leaders

#1 Need to Support New Technology

#2 Reducing Security Costs

#3 Employee Retention

#4 Adhering to Regulations

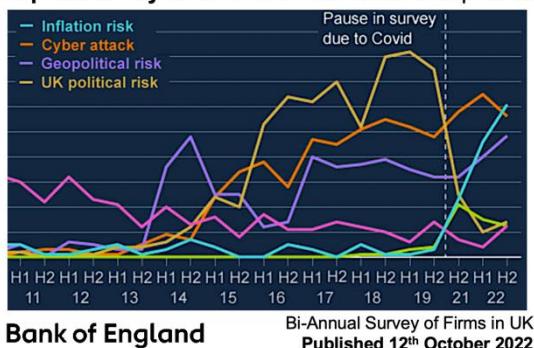
#5 Threat Landscape & Cyber Warfare

Bridewell  
CONSULTING

Survey of 500+ IT Decision Makers  
Published October 2022

## Risks to UK Financial Firms

Top risks = Cyber & Inflation ahead of Geopolitics

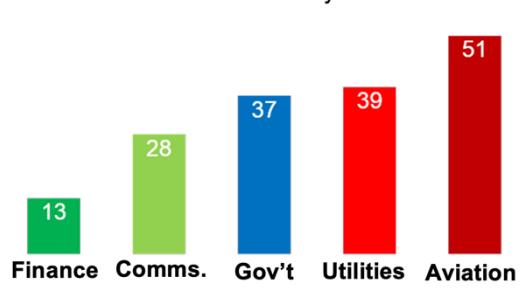


Bank of England

Bi-Annual Survey of Firms in UK  
Published 12<sup>th</sup> October 2022

## Banks lead Cyber Resilience

Finance Firms take fewest days to detect attacks

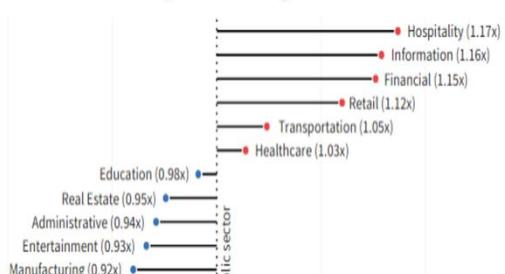


Bridewell  
CONSULTING

Survey of 500+ IT Decision Makers  
Published October 2022

## Banks more likely to Claim

Finance firms report more cyber losses to Insurers

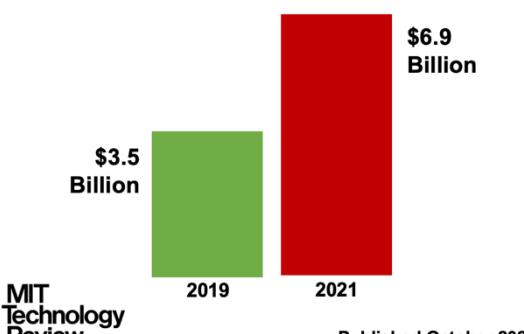


Cyentia  
INSTITUTE

Review of Cyber Insurance Claims  
Published October 2022

## Cybercrime Annual Loss

Annual Losses "doubled" between 2019 and 2021

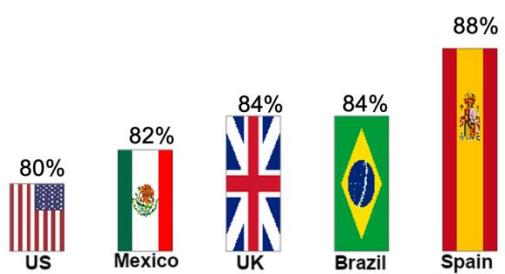


MIT  
Technology  
Review

Published October 2022

## Cyber Security Prioritization

88% in Spain say their board prioritizes cyber security

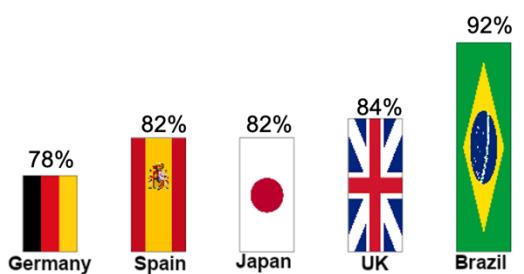


proofpoint.

Survey of 600 Board Directors  
Published October 2022

## Cyber Security Investment

84% in UK say their cyber budget is now Adequate

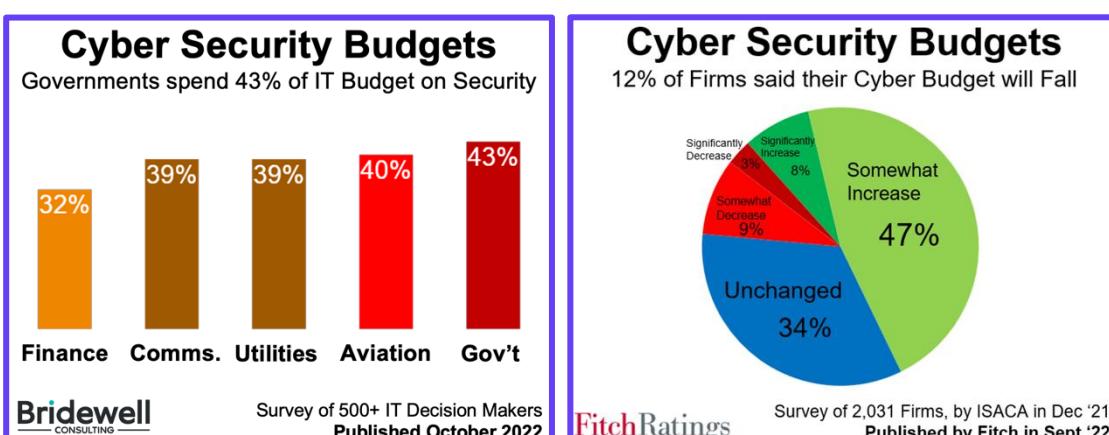
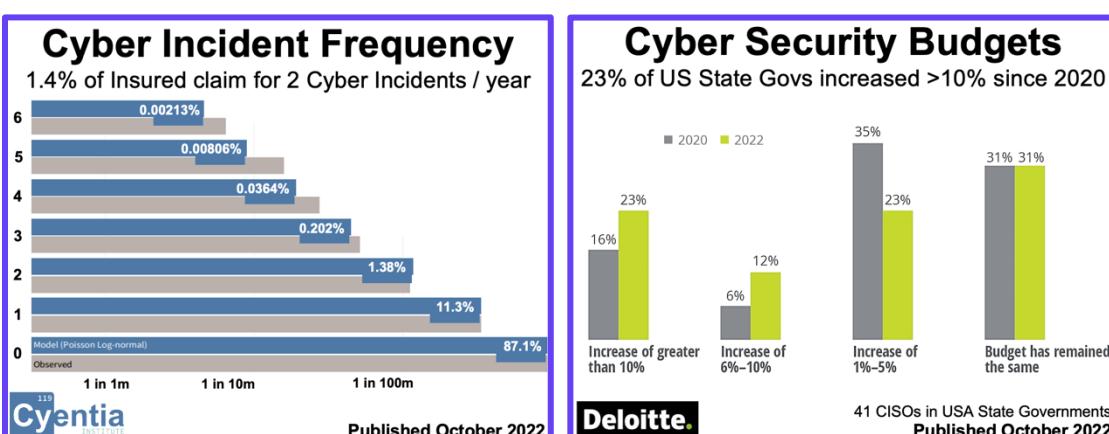
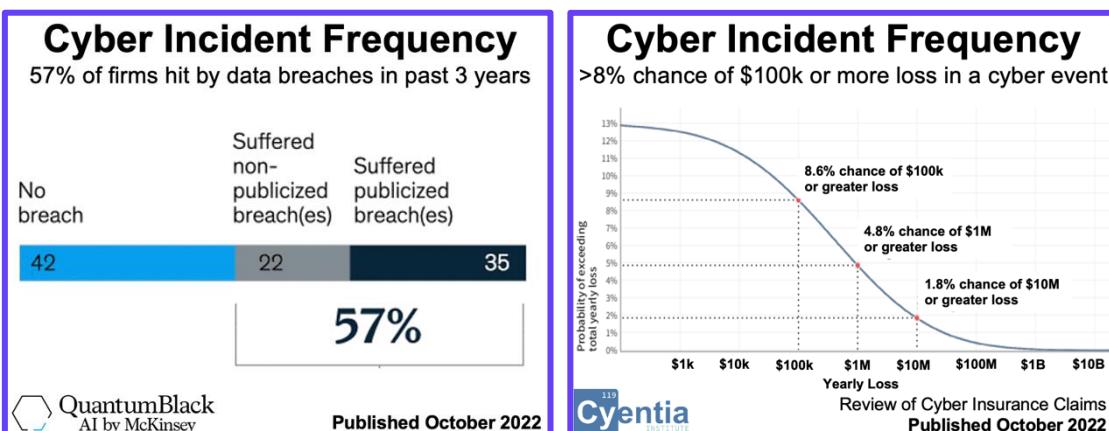
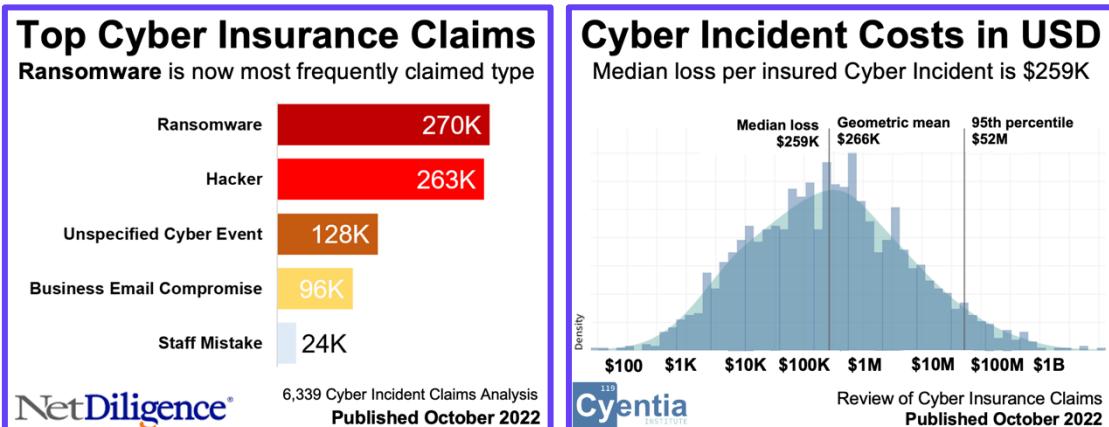


proofpoint.

Survey of 600 Board Directors  
Published October 2022

# Cyber Insights: Cyber Risk Quantification

Click each image to see each report in full. All were published in month to November 2022

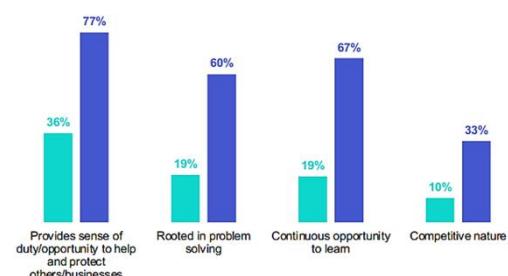


# Cyber Insights: Cyber Incident Response

Click each image to see each report in full. All were published in month to November 2022

## Cyber Incident Responders

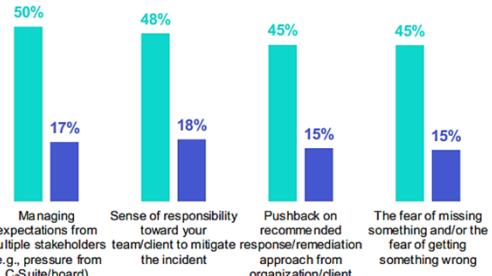
36% say sense of duty attracts them to this job



Survey of 1,107 Cyber Incident Responders  
Published October 2022

## Cyber Incident Stressors

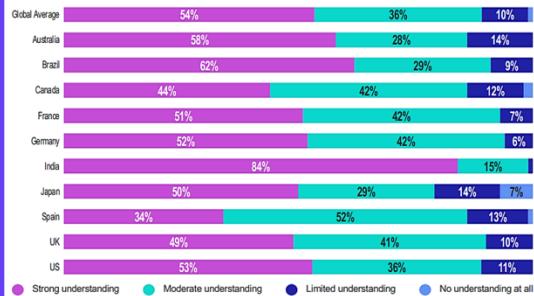
17% say they are most stressed with stakeholders



Survey of 1,107 Cyber Incident Responders  
Published October 2022

## Cyber Incident Response

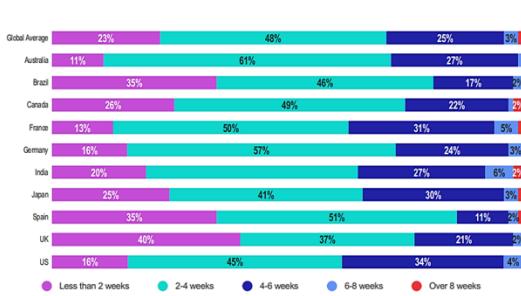
49% in UK say their Leaders understand it very well



Survey of 1,107 Cyber Incident Responders  
Published October 2022

## Cyber Response Length

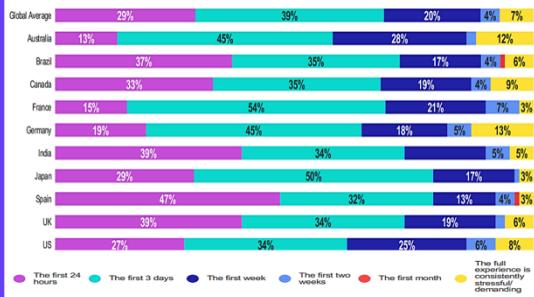
40% in UK responded incident in less than 2 weeks



Survey of 1,107 Cyber Incident Responders  
Published October 2022

## Cyber Incident Response

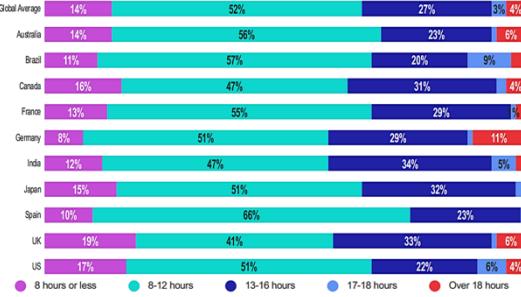
47% in Spain say the first 24 hours is most stressful



Survey of 1,107 Cyber Incident Responders  
Published October 2022

## Cyber Incident Response

11% in Germany say they work over 18 hours



Survey of 1,107 Cyber Incident Responders  
Published October 2022

## Cyber Response Stressors

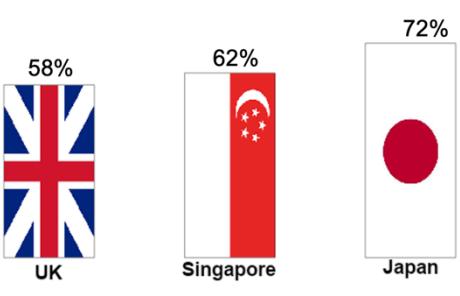
19% say that most stressful is missing something



Survey of 1,107 Cyber Incident Responders  
Published October 2022

## Cyber Attack Preparedness

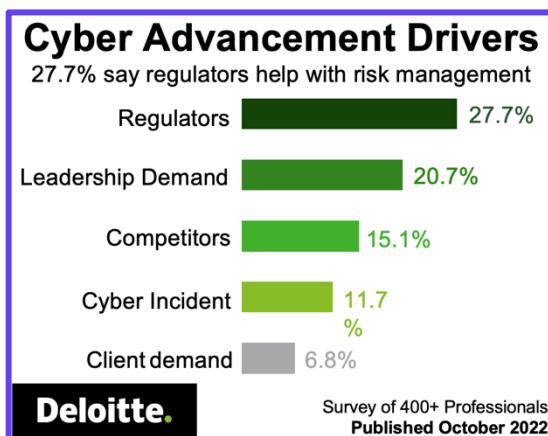
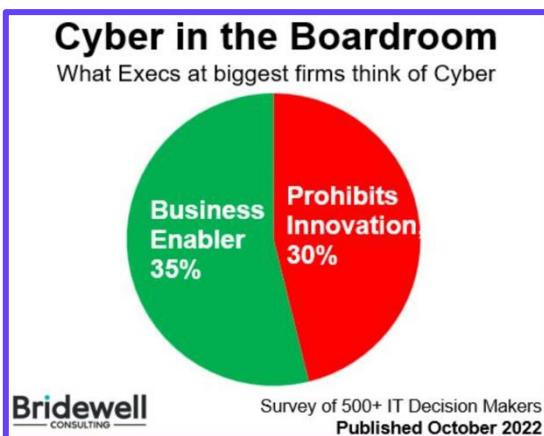
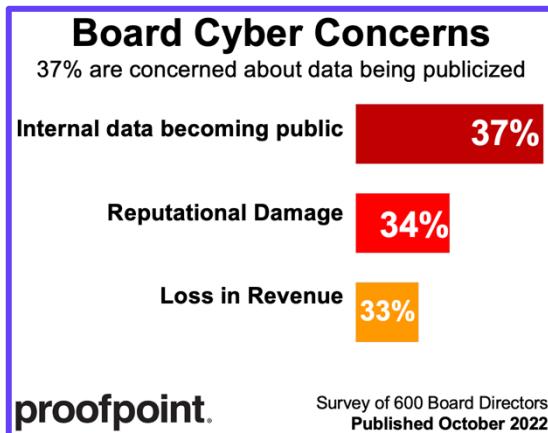
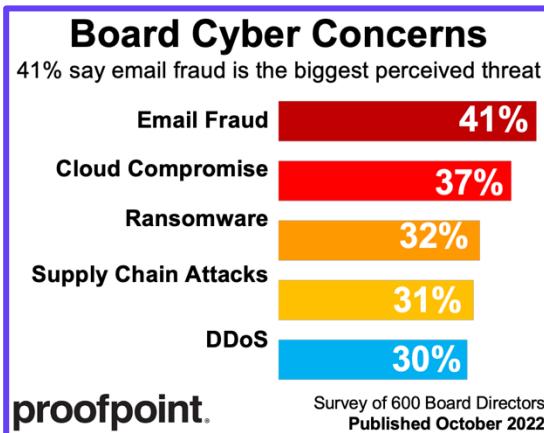
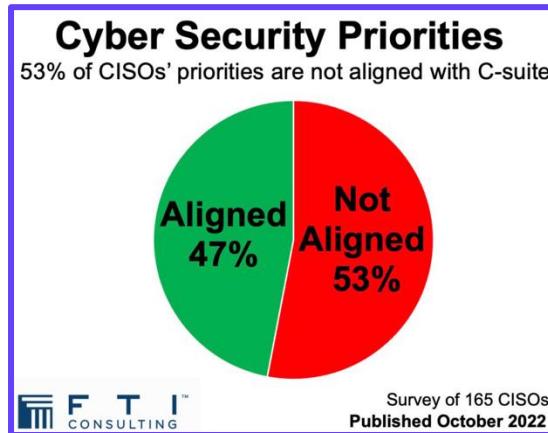
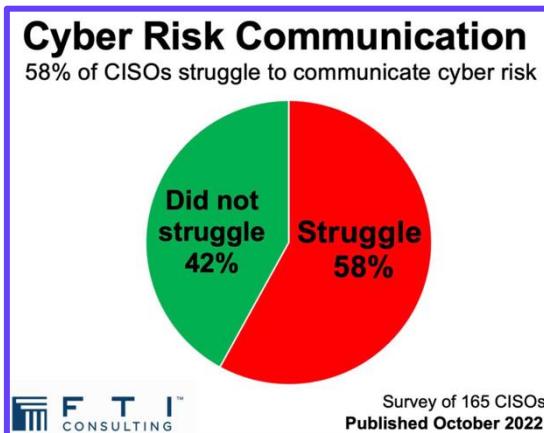
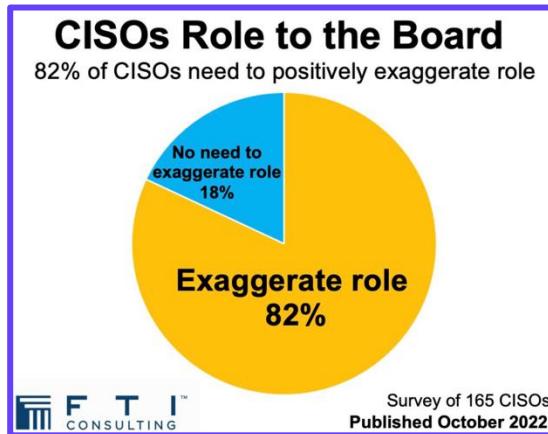
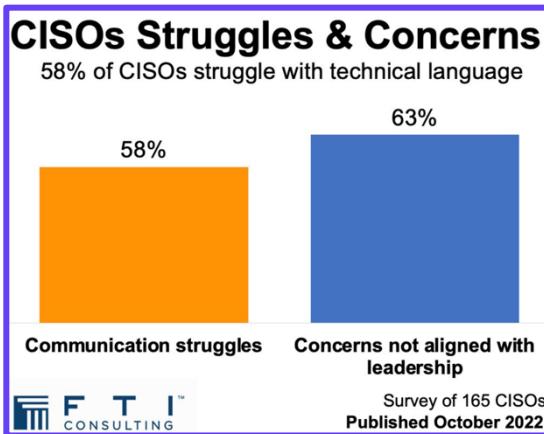
72% in Japan feel unprepared for a cyber breach



Survey of 600 Board Directors  
Published October 2022

# Cyber Insights: CISOs in the Boardroom

Click each image to see each report in full. All were published in month to November 2022

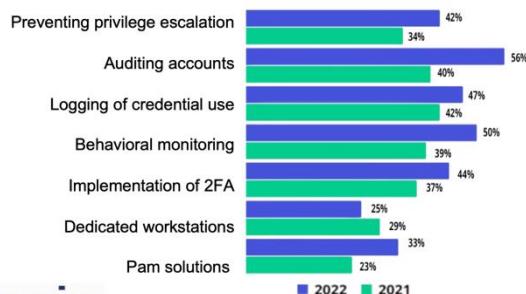


# Cyber Insights: Cyber Development

Click each image to see each report in full. All were published in month to November 2022

## Ransomware Preparedness

9% improvement of privilege escalation indicated

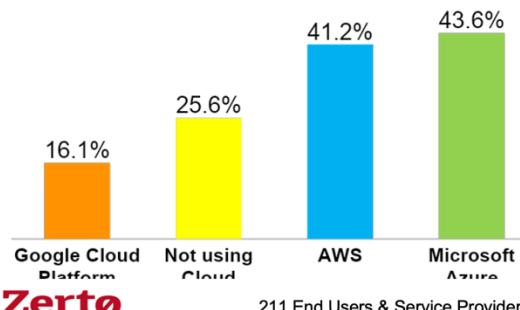


**axio**

Published October 2022

## Cloud as Disaster Strategy

43.6% are using Microsoft Azure as protection

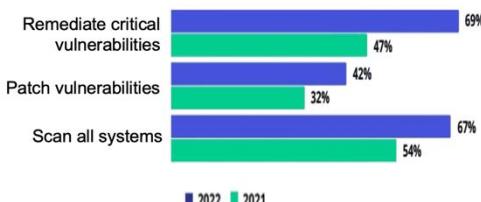


**Zerto**  
a Hewlett Packard Enterprise company

211 End Users & Service Providers  
Published October 2022

## Vulnerability Management

67% report that they scan all systems in 2022

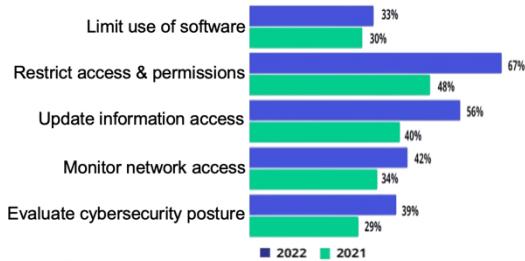


**axio**

Published October 2022

## Third Party Management

10% Increase for Evaluation of Cyber Posture

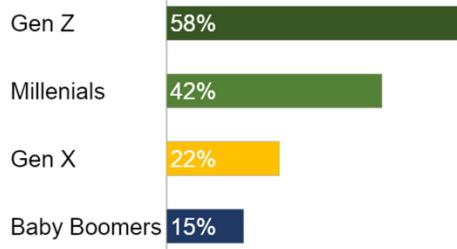


**axio**

Published October 2022

## Knowledge on Cybersecurity

Younger Gens disregard mandatory IT updates

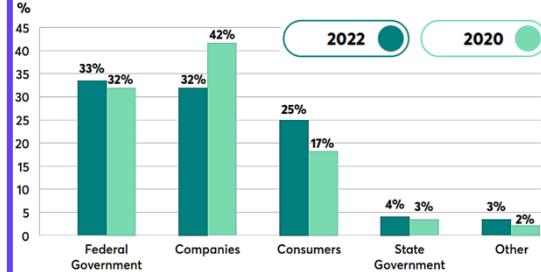


**EY**

Survey of 1,000 full- and part-time US employees aged 18+  
Published October 2022

## Consumer Cyber Readiness

Companies' Privacy Accountability preferred at 42%



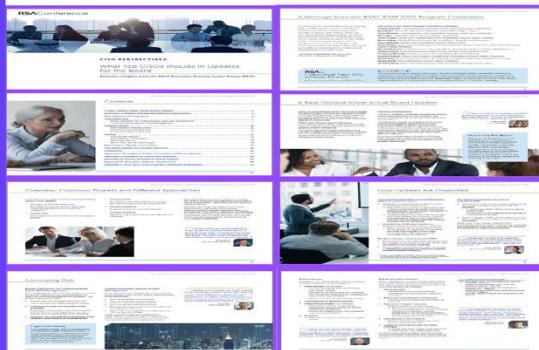
**ASPN DIGITAL**  
THE ASPIRE INSTITUTE

Published October 2022

## RSA Conference CISO PERSPECTIVES

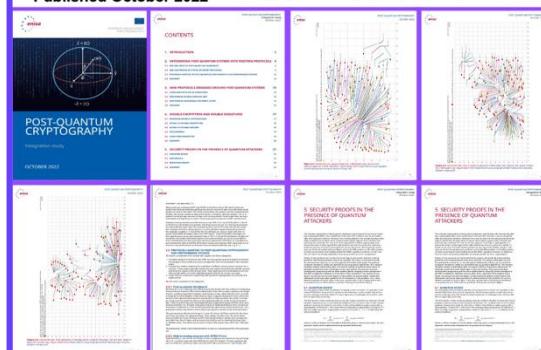
Published October 2022

Insights from ESAF 2022



## POST-QUANTUM CRYPTOGRAPHY

Published October 2022



# Cyber Insights: Security & Challenges

Click each image to see each report in full. All were published in month to November 2022

### Cyber Challenges

Real-time data visibility is #1 challenge in Aviation

Transport & Aviation	Finance	Utilities
Real-time data visibility	Trust in cyber security tools	Protecting our critical assets
Supporting remote and hybrid working	Managing cloud security	Trust in cyber security tools
Lack of cyber security talent	Real-time data visibility	Lack of cyber security talent
Improving cyber resilience	Complying with regulations	Data protection and privacy
Managing supply chain risks	Supporting remote and hybrid working	Managing supply chain risks/complying with regulations

**Bridewell CONSULTING**

Survey of 500+ IT Decision Makers  
Published October 2022

### Cyber Security Staffing

62% of firms say Cyber Security is Understaffed

Category	Percentage
Significantly Understaffed	15%
Somewhat Understaffed	47%
Appropriately Staffed	34%
Somewhat Overstaffed	2%
Significantly Overstaffed	1%

**Fitch Ratings**

Survey of 2,031 Firms, by ISACA in Dec '21  
Published by Fitch in Sept '22

### US Cyber Security Demand

769,736 Cyber Security job openings available

**Cyber Seek**

Published October 2022

### Cyber Communications

66% of CISOs struggle to understand roles

Struggle Level	Percentage
Struggle	66%
Did not struggle	34%

**FTI CONSULTING**

Survey of 165 CISOs  
Published October 2022

### Consumer Cyber Readiness

MFA feature highest usage increase at 27%

Category	2020 (%)	2022 (%)
Strong Password	74%	14%
Phone unlock Auth	69%	16%
GPS Access during App use	65%	16%
Non-Invasive Apps Preference	71%	9%
Mindful Permission Settings	60%	18%
MFA	50%	27%

**ASOPEN DIGITAL**

Published October 2022

### Manage Service Account

50% of organizations review service account

Review Type	2022 (%)	2021 (%)
Review privileges service account	50%	38%
Audit of service account use	47%	36%

**axio**

Published October 2022

### Cyber and Technology Slip

Most important Risk Categories in 2021-2022

Risk Category	UK 2021 (%)	UK 2022 (%)	US 2021 (%)	US 2022 (%)
Cyber and Technology	35%	22%	40%	20%
Business	34%	32%	31%	26%
Environmental	10%	21%	14%	26%
Retail, Wholesale, Food & Beverage	-	-	-	-

**beazley**

Published October 2022

### Biggest Resilience Drops

Technology, Media, & Telecoms dropped 14 points

Sector	Drop (-)
Tech, Media & Telecoms	-14
Retail, Wholesale, Food & Beverage	-9
Real Estate and Construction	-5
Energy and Utilities (including mining)	-5

**beazley**

Published October 2022

# Cyber Insights: Cyber Concerns & Strategies

Click each image to see each report in full. All were published in month to November 2022

### Cyber Attacks Concerns

66% of firms now more concerned than they were

Concern Level	Percentage
More Concerned	66%
Less Concerned	5%
About the same	29%

**SONICWALL®**  
Survey of SonicWall Customers (80% in USA)  
Published October 2022

### Reevaluating Strategies

66.8% are reevaluating ransomware strategies

Response	Percentage
Yes	66.8%
No	20.3%
Other	12.9%

**Zerto**  
a Hewlett Packard Enterprise company  
217 End Users & Service Providers  
Published October 2022

### Zero Trust Security Strategy

72% of C-Level identifies zero trust as important

Importance Level	Percentage
Important	72%
Business Critical	26%
Neither Important nor Unimportant	3%

**okta**  
700 Security Decision Makers  
Published October 2022

### Cyber Zero Trust Security

42% of companies have implemented in 2022

Year	Already Implemented	Next 12-18 Months
2021	24%	65%
2022	55%	42%

**okta**  
700 Security Decision Makers  
Published October 2022

### Incident Response Trends

"Duty to protect" is top reason to work in profession

Trend	Percentage
Sense of Duty	80%
Fighting Multiple Attacks	68%
Stress in Daily Life	67%

**IBM**  
Survey of 1,100 Cyber Incident Responders  
Published October 2022

### Cyber and Technology Risk

Change in risk & resilience perceptions in UK & US

The scatter plot shows the change in risk and resilience perceptions for various cyber and technology risks in the UK & US, comparing 2021 (blue dots) and 2022 (pink dots). The x-axis represents Resilience (Low to High) and the y-axis represents Risk (Low to High).

Risk Type	2021 (Risk)	2022 (Risk)	2021 (Resilience)	2022 (Resilience)
Cyber	High	High	Medium	Medium
Disruption	Low	Medium	Very Low	Medium
Tech obsolescence	Medium	Medium	Medium	High
Intellectual property	Low	Low	Very Low	Very Low

**beazley**  
Published October 2022

**Ministry of Defence**  
**Cyber Primer**  
Cyber within Defence Concept  
Published October 2022

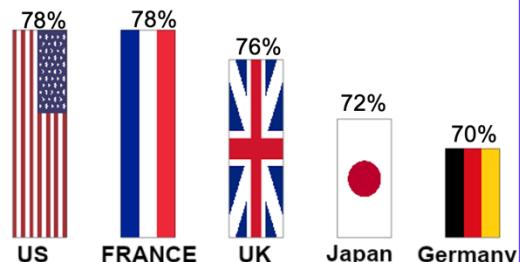
**okta** **Zero Trust Security**  
2022 Global Organizations

# Cyber Insights: Attack Trends

Click each image to see each report in full. All were published in month to November 2022

## Risk of Material Cyber Attack

78% in US say "we're at risk of material (big) attack"

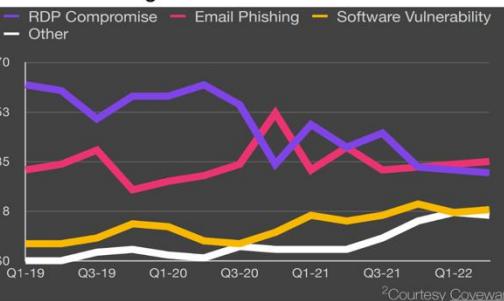


**proofpoint.**

Survey of 600 Board Directors  
Published October 2022

## Cyber Attack Vectors

Email Phishing now most successful for hackers

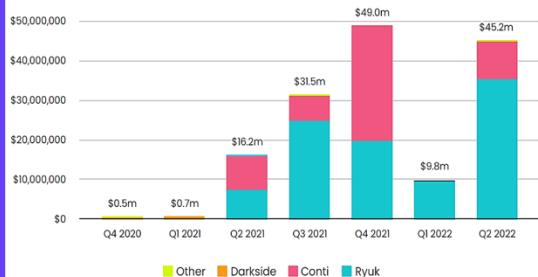


**BLACKFOG**

Published October 2022

## Ransom Laundering

Ryuk and Conti laundered over \$150m through Ren

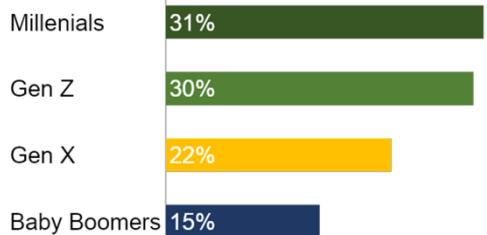


**ELLIPTIC**

Published October 2022

## Work & Personal Passwords

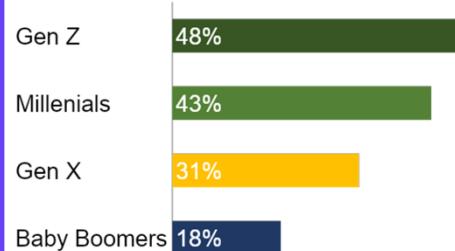
Younger Gens use the same password on accounts



**EY** Survey of 1,000 full- and part-time US employees aged 18+  
Published October 2022

## Web Browser Cookies

Younger Gens accept cookies on their work devices



**EY**

Survey of 1,000 full- and part-time US employees aged 18+  
Published October 2022

## ivanti Growth of Ransomware

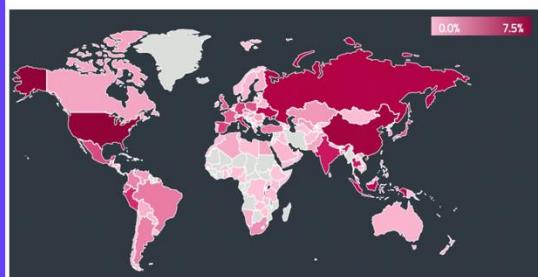
Complexity and Impact in 2022

Published October 2022



## Cyber Ransomware Volume

USA, Russia & China detect the most Ransomware

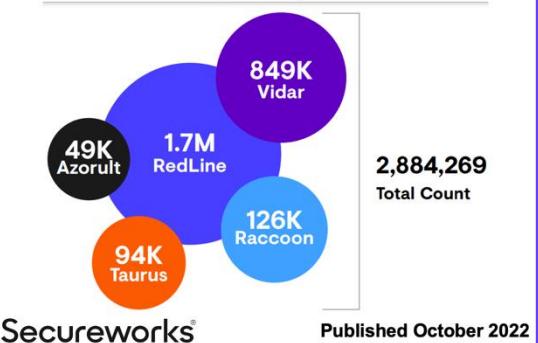


**we live security™**

Published October 2022

## Cyber Info stealers

RedLine with highest logs offered at 1.7M



# Cyber Insights: Cyber Threats

Click each image to see each report in full. All were published in month to November 2022

### Cyber Risk Assessment

26.6% say they are fully assessed for cyber risks

We are fully assessed	26.6%
Plans to do it within next 1 year	18.4%
Plans to do it within next 2-4 yrs	16.2%
Not in our plan	6.9%
Probably do it in the next 6-10 yrs	6.1%

**Deloitte.** Survey of 400+ Professionals Published October 2022

### Top 5 Nastiest Malware

Ranking of the year's biggest cyber threat

- #1 = Emotet
- #2 = LockBit
- #3 = Conti
- #4 = Qbot
- #5 = Valyria

**opentext** Published October 2022

### Initial Access Vectors

Exploitation of remote services highest at 52%

Vector	Percentage
Exploitation of remote services	52%
Credentials	39%
Phishing	2%
Network misconfiguration	2%
Drive by download	2%
Commodity malware infection	3%

**Secureworks** Published October 2022

### Cyber Privacy Responsibility

Companies hold the most responsibility for data

Sector	2022 (%)	2020 (%)
Federal Government	33%	32%
Companies	32%	42%
Consumers	25%	17%
State Government	4%	3%
Other	3%	2%
No one, I don't think it's a problem	3%	3%

**CR Consumer Reports** Published October 2022

### Cyber Incident Frequency

22% of impacted firms experience >=2 Cyber Event

Frequency	Percentage
1	78%
2	12%
3	4%
4	2%
5+	4%

**Cyentia INSTITUTE** Published October 2022

### Cyber Interruption Costs

Cyber Security Incidents highest cost at \$643K

Category	Cost (\$K)
Business Interruption (N=259)	340K
Crisis Services (N=241)	133K
Legal/Regulatory (N=7)	113K
Incident (N=259)	643K

**NetDiligence** 6,339 Cyber Incident Claims Analysis Published October 2022

### Cyber Security Budgets

"Significant Underfunding" of Cyber at 19% of Firms

Budget Status	Percentage
Significantly Overfunded	2%
Somewhat Overfunded	3%
Appropriately Funded	34%
Somewhat Underfunded	41%
Significantly Underfunded	19%

**Fitch Ratings** Survey of 2,031 Firms, by ISACA in Dec '21 Published by Fitch in Sept '22

### Ransom Strategies

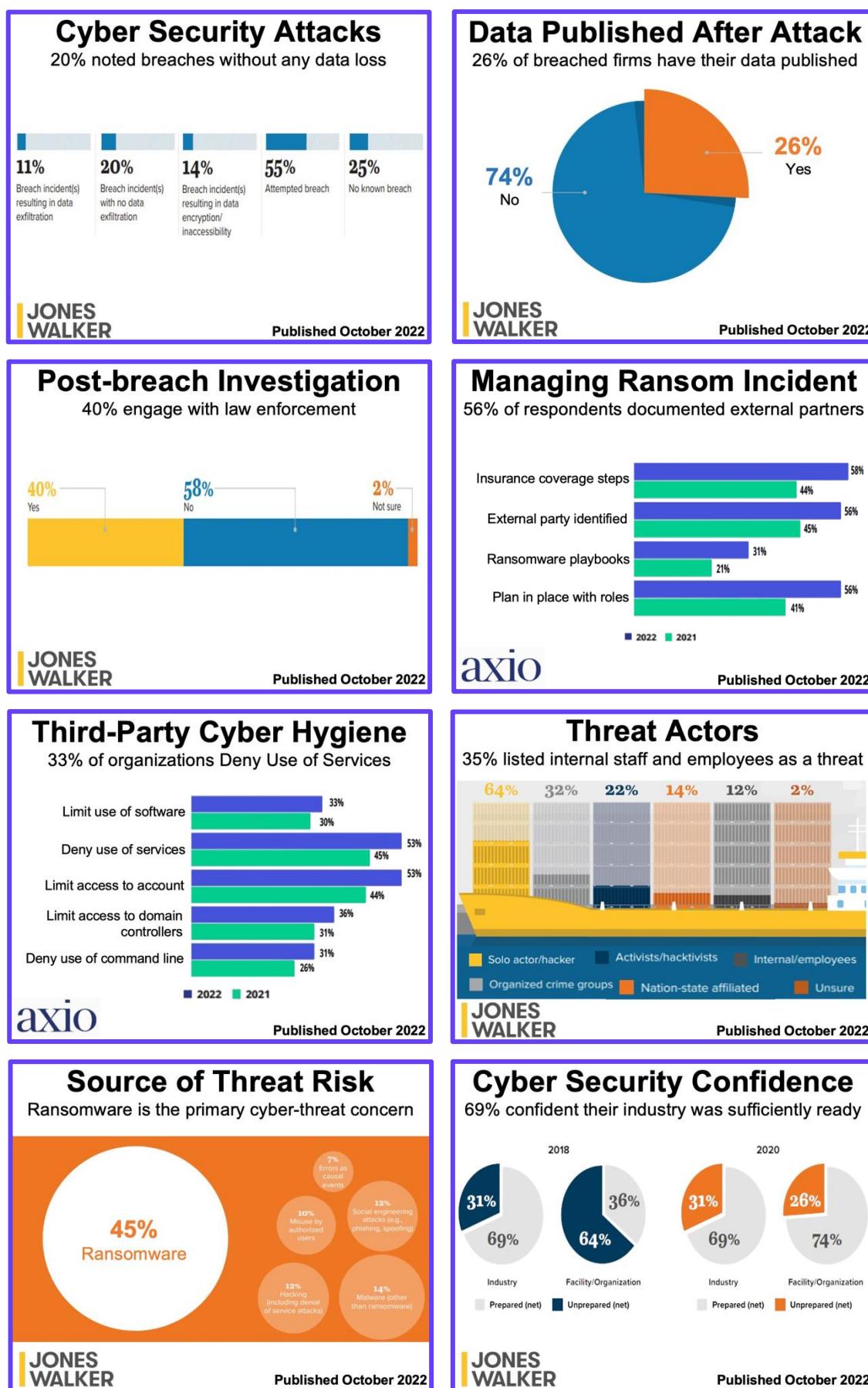
51% of strategies are focused on prevention

Strategy Focus	Percentage
Yes, strategy is focused on prevention	28.3%
Yes, strategy is focused on recovery	10%
Yes, strategy is focused on prevention and recovery	51.6%
No formalized strategy is in place yet	8.7%
Not sure	0%
Possible, might be another team	0%

**Zerto** a Hewlett Packard Enterprise company 219 End Users & Service Providers Published October 2022

# Cyber Insights: Cyber Attacks

Click each image to see each report in full. All were published in month to November 2022



# Cyber Insights: Insurance & Incidents

Click each image to see each report in full. All were published in month to November 2022

### Cyber Insurance Claims

Firms average \$170K per Insured Incident

Crisis Services (N=4,270)	110K
Legal/Regulatory (N=336)	82K
Incident (N=6,339)	170K

**NetDiligence®**

6,339 Cyber Incident Claims Analysis  
Published October 2022

### Personal Cyber Insurance

Wealthy Consumers more likely to have insurance

Middle class	11%
Upper middle class	24%
Mass Affluent	63%
High net worth NW	83%

**CHUBB®**

Survey of 1,605 respondents  
Published October 2022

### Personal Cyber Insurance

64% values insurance to replace stolen money

The ability to replace money that was stolen from your bank account	64%
Covering the cost for legal, public relations, and digital forensic services to help you recover from a cybercrime	58%
Reimbursement for fraudulent credit card charges	56%
Reimbursement of money paid after being tricked or deceived into voluntarily sending money	49%
Access to an expert who can help evaluate your cyber vulnerabilities	48%
Counsel on how to respond to a ransomware attack	43%
Coverage/protection against cyberbullying	33%

**CHUBB®**

Survey of 1,605 respondents  
Published October 2022

### Cyber Security Framework

46% implemented NIST cybersecurity framework

NIST Cybersecurity Framework	46%
ISO 27001/27002	37%
NERS CIP	21%
IASME Governance	15%
Cobit	7%

**JONES WALKER**

Published October 2022

### Type of Cyber Attack

20% listed ransomware as the primary attack

**JONES WALKER**

Published October 2022

### Firms breached by Ransom

Good news: decline in known Victims since March

**we live security™**

Published October 2022

### Cyber Insurance Trends

Insurance Capacity & Pricing

**GLOBAL INSURANCE LAW**

Published October 2022

### NetDiligence® Cyber Insurance Claims Study

Published Oct 2022

**NetDiligence®**

Published Oct 2022

# The Best Cyber Insights of 2022

Click each image to see each report in full. All were published in month to October 2022

## Cyber Insurance Essentials

To buy Insurance, firms must often demonstrate 10:

- |                            |                 |
|----------------------------|-----------------|
| 1. IT Security Leadership  | 6. MFA          |
| 2. Staff Training on cyber | 7. IRP          |
| 3. Strong Passwords        | 8. EDR          |
| 4. System Backups          | 9. TPRM         |
| 5. Regulatory Compliance   | 10. Pen Testing |

FitchRatings

Published September 2022

## Cyber Insurance Pricing

Price for \$10m Cover now \$175k for big firms in Oz



2021 FINANCIAL REVIEW

2022 FINANCIAL REVIEW

Published September 2022

## Cyber Insurance Coverage

89% of Energy firms "have Insurance for Ransom"

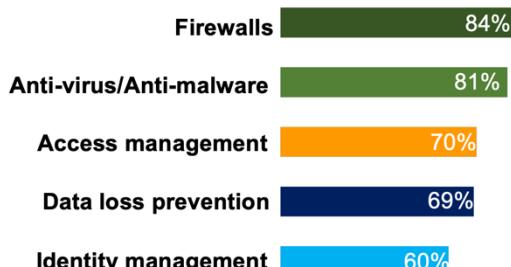


SOPHOS

Survey of 5,600 IT professionals  
Published September 2022

## Cyber Attack Protection

84% of orgs fully deploy firewalls to stop attacks

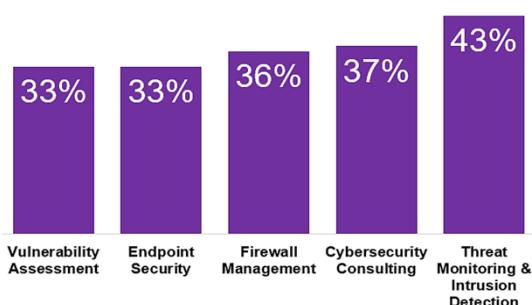


proofpoint.

Published September 2022

## Cyber Security Services

Threat Monitoring & Intrusion Detection top at 43%



vade

Published September 2022

## Cyber Insurance Market USA

\$4.9bn paid by firms to Insurers who paid out 65%

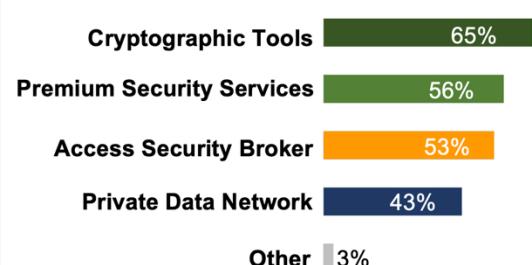


FitchRatings

Published September 2022

## Cloud Protection Tools

65% say they use cryptographic tools for cloud data

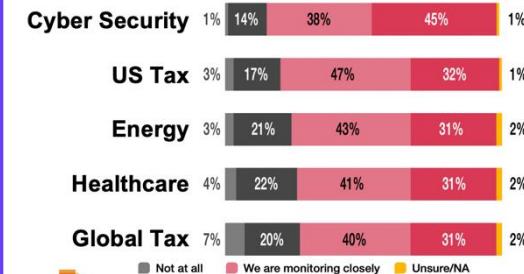


proofpoint.

Published September 2022

## Cyber is #1 on Firms' Radars

45% of "taking action" on Cyber, vs 31% on Energy

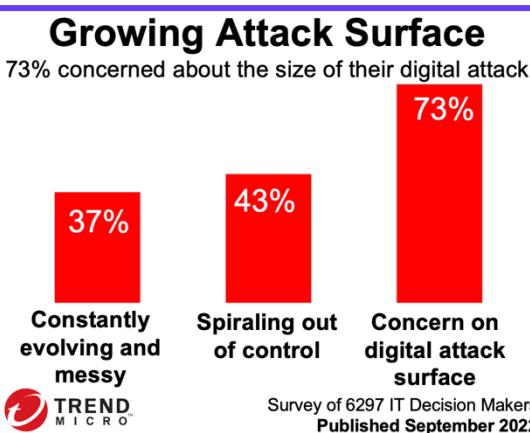
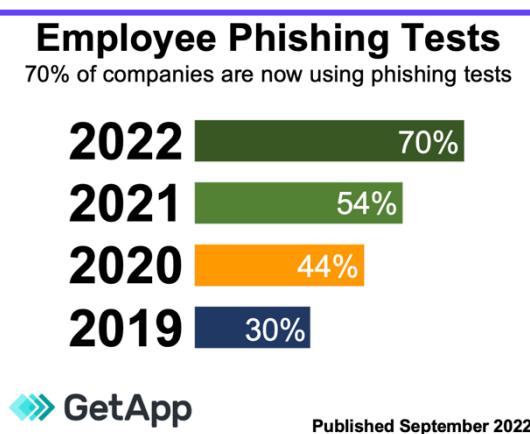
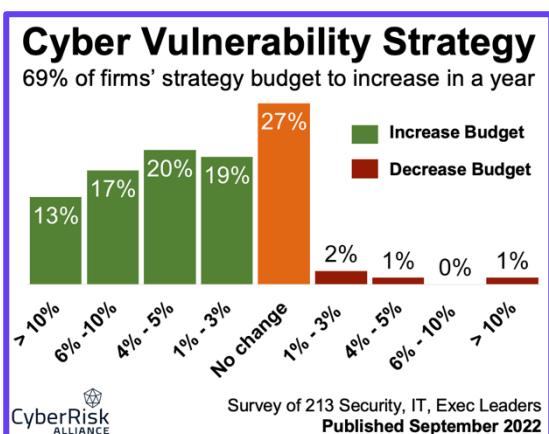
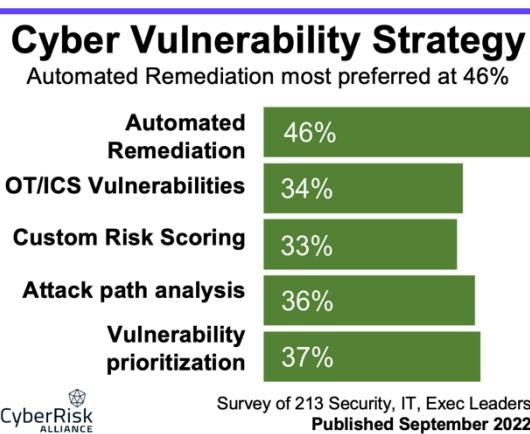
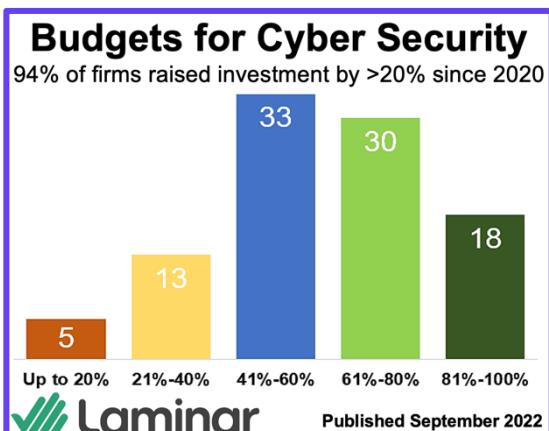


pwc

Interviews with 722 US execs  
Published August 2022

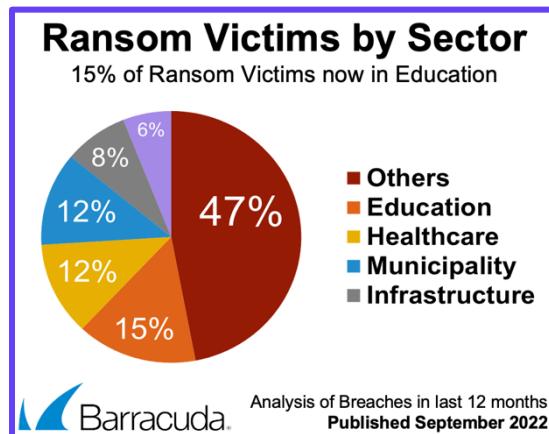
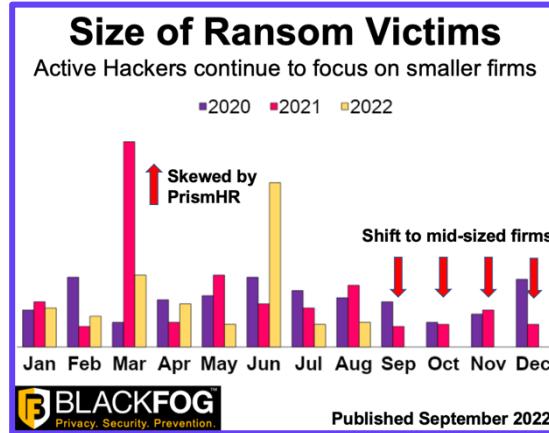
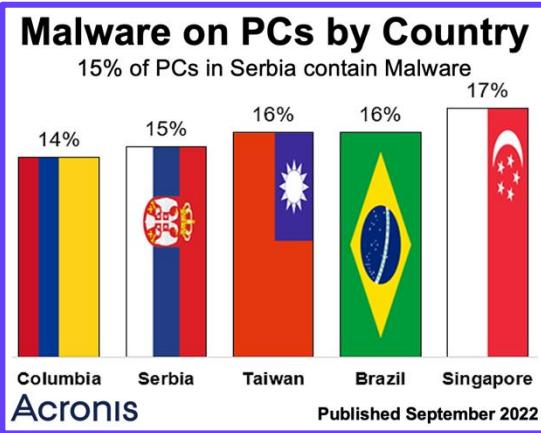
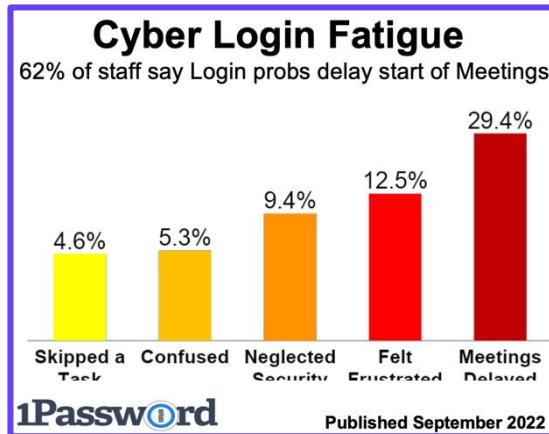
# Cyber Insights: Cyber Security Investments

Click each image to see each report in full. All were published in month to October 2022



# Cyber Insights: People & Cyber Challenges

Click each image to see each report in full. All were published in month to October 2022



# Cyber Insights: Cyber Threats & Lures

Click each image to see each report in full. All were published in month to October 2022

### Cyber Attack Vectors

Email Phishing now most successful for hackers

Quarter	RDP Compromise	Email Phishing	Software Vulnerability	Other
Q1-19	~60%	~25%	~5%	~10%
Q3-19	~55%	~30%	~5%	~10%
Q1-20	~60%	~20%	~5%	~10%
Q3-20	~65%	~40%	~5%	~10%
Q1-21	~35%	~35%	~10%	~10%
Q3-21	~40%	~30%	~15%	~10%
Q1-22	~35%	~35%	~15%	~10%

2 Courtesy Coveware

**BLACKFOG**  
Privacy. Security. Prevention.

Published September 2022

### Gaming-related Cyberthreats

'Downloader' highest Cyberthreat lure at 88.56%

Cyber Threat Type	Percentage
Downloader	88.56%
AdWare	4.19%
Trojan	3%

**SECURELIST**

Analysis from KSN  
Published September 2022

### Exfiltrated Sensitive Data

45% of Cloud Exfiltrated Data come from Dropbox

Cloud Provider	Percentage
Other	11%
iCloud	15%
Google Drive	25%
Dropbox	45%

**CYBERHAVEN**

Published September 2022

### Malicious Email Attachments

49% of malicious email files received are now Excel

Year	Percentage
2019	11%
2020	23%
2021	30%
2022-H1	49%

**CHECK POINT**

Published September 2022

### Emails for Cyber Attacks

29.4% of malicious emails are now Phishing Attacks

Malicious Email Type	Percentage
Executable in archive	4.6%
Extortion	5.3%
Advance-fee scam	9.4%
URL	12.5%
Phishing	29.4%

**HORNSECURITY**

Published September 2022

### Emails for Cyber Attack

58% of malicious emails are now Phishing Attacks

Malicious Email Type	Percentage
Phishing	58
Malware	28
Advanced Attacks	7
Others	5
BEC	2

**ACRONIS**

Published September 2022

### Risks in Media Value Chain

50% of Content Mgmt. Firms have big cyber issue

Risk Category	Percentage
Content Management	50%
Distribution	23%
Production	28%
Monetization	13%

**BlueVoyant**

Analysis from 485 Media Vendors  
Published September 2022

### Cyber Attack Tools

Cobalt Strike seen most on compromised systems

Cyber Attack Tool	Percentage
Cobalt Strike	36%
Mimikatz	28%
XMRig	15%
PsExec	14%
Metasploit	7%

**CHECK POINT**

Published September 2022

# Cyber Insights: Cloud Vulnerabilities

Click each image to see each report in full. All were published in month to October 2022

## Cloud Security Challenges

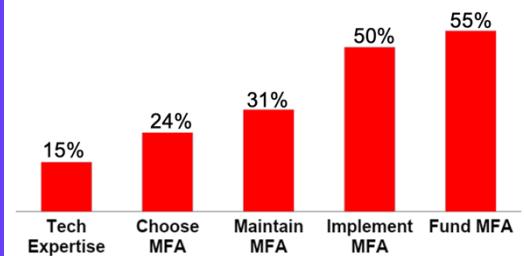
45% agree that inefficient cloud security processes use up significant Engineering Effort



Survey of 400 Cloud & Security Pros  
Published September 2022

## Small Firms' MFA challenges

Getting Funding for Multi-factor Authentication is top

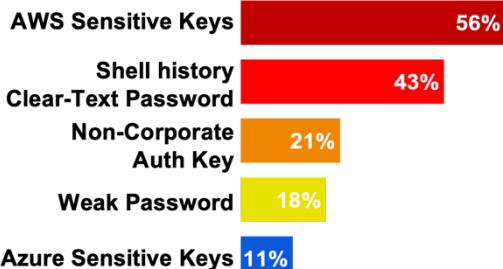


CYBER READINESS INSTITUTE

Survey of 1,403 small firms  
Published July 2022

## Cloud Security at Risk

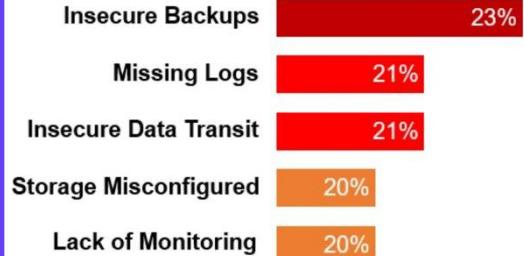
18% of firms have cloud workload with weak p/word



Published September 2022

## Cloud Security Mistakes

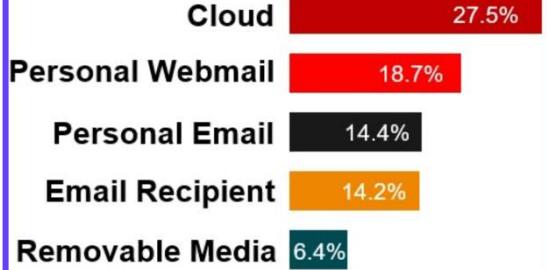
23% of Pros report Insecure Use of Data Backups



Survey of 400 Cloud & Security Pros  
Published September 2022

## 5 Ways Staff Steal Secrets

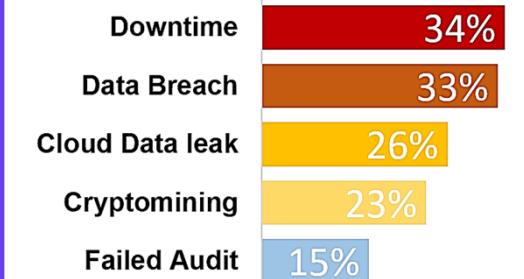
27.5% of Staff who Steal move Data onto Cloud



Data from 1.4m Employees  
Published September 2022

## Serious Cloud Incidents

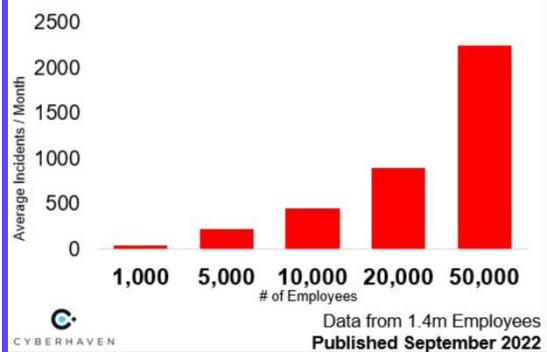
34% hit by Downtime due to misconfiguration



Survey of 400 Cloud & Security Pros  
Published September 2022

## Data Theft by Staff at Firms

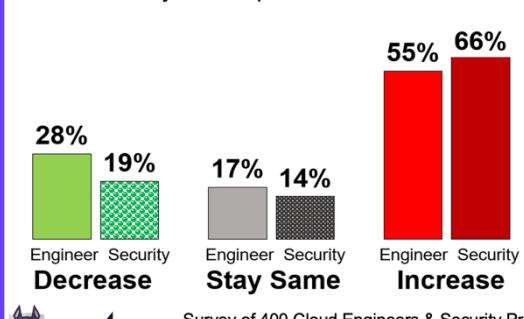
Firms with > 50K staff have > 2K incidents / month



Data from 1.4m Employees  
Published September 2022

## Cloud Risk Expected in 2023

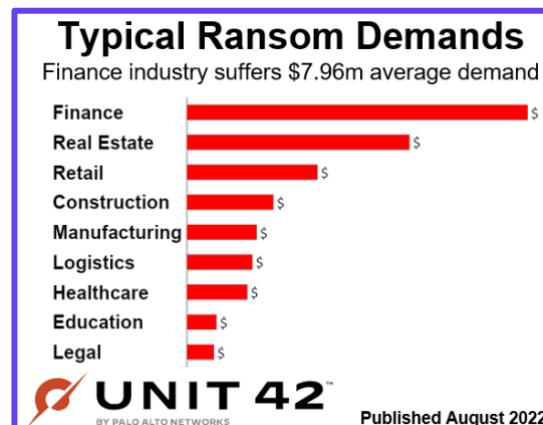
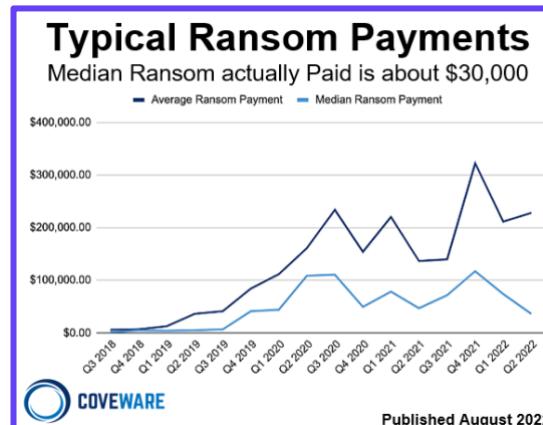
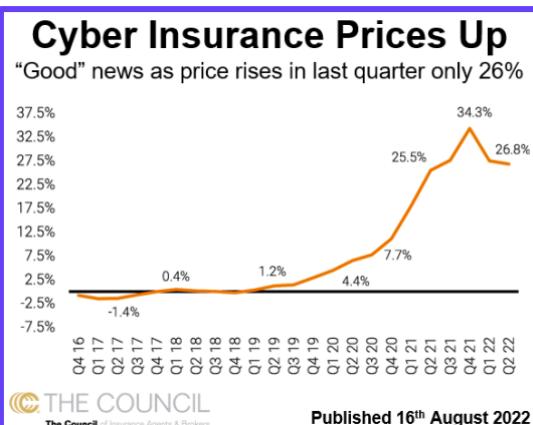
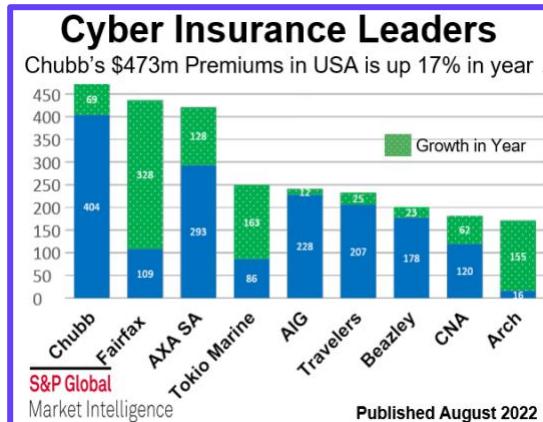
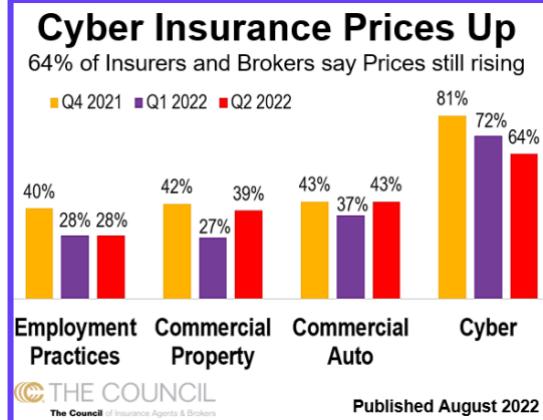
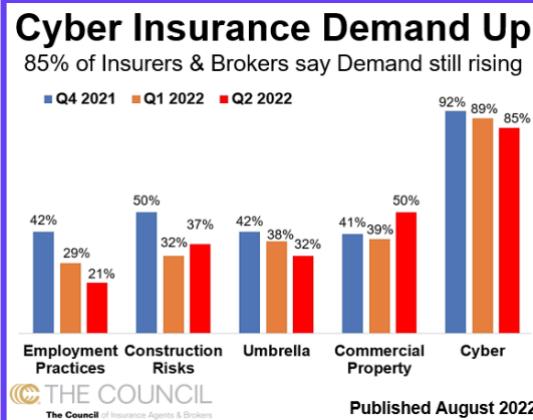
66% of Security Pros expect Cloud Risk to Increase



Survey of 400 Cloud Engineers & Security Pros  
Published September 2022

# Cyber Insights: Cyber Insurance & Costs

Click each image to see each report in full. All were published in month to September 2022



# Cyber Insights: Ransom Attacks

Click each image to see each report in full. All were published in month to September 2022

### Ransom Attacks by Region

4.76% of African firms attacked by Ransom / week

Region	Percentage
Australasia	0.88%
North America	0.93%
European Union	1.51%
South America	4.35%
Africa Union	4.76%

Published August 2022

### Ransom Reports by Country

US & Germany report the most Ransom breaches

Country	Ransomware Incidents
Netherlands	~20
Switzerland	~20
UK	~30
Spain	~40
Italy	~50
France	~60
Germany	~100
US	~120

Based on 600+ Ransom Incidents  
Published August 2022

### Ransom Attacks by Sector

Finance is the most targeted industry for hackers

Sector	Approx. Ransom Attacks
Finance	~80
Professional & Legal Services	~70
Manufacturing	~65
Healthcare	~60
High Technology	~45
Wholesale & Retail	~45
Education	~35
Hospitality	~35

Published August 2022

### Ransom Reports by Sector

Industrial Sector most hit by ransomware incidences

Sector	Approx. Ransom Reports
Industrial	~80
Information Services	~70
Government	~65
Health	~60
Finance	~55
Transportation	~50
Education	~40
Energy	~25

Based on 600+ Ransom Incidents  
Published August 2022

### Ransom Attacks by Sector

Professional Services firms hit most frequently

Sector	Percentage
Professional Services	21.9%
Public Sector	14.4%
Real Estate	2.5%
Technology Hardware	6.3%
Software Services	9.4%
Utilities	2.5%
Food & Staples Retail	3.8%
Financial Services	6.9%
Consumer Services	5.5%
Health Care	10.07%
Materials	8.1%
Media	1.3%
Insurance	1.9%

Published August 2022

### Ransom Demanded vs Payment

Tech Sector pays 40% of initial ransom demand

Sector	Initial Demand (%)	Paid (%)
Tech	~60%	~40%
Manufact	~74%	~40%
Logistics	~70%	~40%
Retail	~62%	~40%
Health	~85%	~40%
Legal	~53%	~40%
Finance	~51%	~40%

Published August 2022

### Ransom Attack Response

Implement recovery plan is top mentioned response

- #1 Implement Recovery Plan (45%)
- #2 Analyse damage of attack (39%)
- #3 Quarantine the Endpoints (37%)
- #4 Inform all of the Employees (37%)
- #5 Inform affected Customers (33%)

Survey of 505 InfoSec Leaders  
Published August 2022

### Size of Firms hit by Ransom

Typical Firm hit by Ransom now has about 110 staff

Quarter	Median Company Size
Q3 2018	~20
Q4 2018	~30
Q1 2019	~40
Q2 2019	~50
Q3 2019	~60
Q4 2019	~40
Q1 2020	~50
Q2 2020	~100
Q3 2020	~150
Q4 2020	~220
Q1 2021	~200
Q2 2021	~180
Q3 2021	~140
Q4 2021	~150
Q1 2022	~160
Q2 2022	~140

Published July 2022

# Cyber Insights: Costs and Finances

Click each image to see each report in full. All were published in month to September 2022

### Costs of Data Breaches

Over 200 breaches cost between \$10M - \$100M

Breach Cost Range	Count
\$1K-\$10K	463
\$10K-\$100K	646
\$100K-\$1M	588
\$1M-\$10M	365
\$10M-\$100M	221

Review of 2,400 data breaches  
Published August 2022

BLACK KITE

### Cost of Data Breach: Factors

An implemented DevSecOps reduces costs most

Factor	Impact
DevSecOps Implemented	Green bar
Tested IR Plan	Green bar
Pen Tests Done	Green bar
Third Party Involved	Red bar
Compliance Failures	Red bar

IBM Security  
Published August 2022

### Cause of Costly Breaches

Breaches involving Unsecured databases cost most

Cause	Cost (M)
Unsecured Database	\$113 M
Human's Error	\$26 M
Ransomware	\$22 M
Unsecured Network	\$19 M
Phishing	\$11 M

Review of 2,400 data breaches  
Published August 2022

BLACK KITE

### Average cost of data breaches

Finance industry increased by \$0.25 million or 4.4%

Industry	2021	2022
Gov	\$2.1	\$1.9
Industry	\$4.2	\$4.5
Services	\$4.7	\$4.7
Pharma	\$5.0	\$5.0
Financial	\$5.7	\$6.0

IBM Security  
Published August 2022

### Cost of Cyber Crime

Increase from \$3 trillion to \$10.5 trillion in 2025

Year	Cost (\$T)
2015	\$3T
2021	\$6T
2022	\$7T
2025	\$10.5T

Secureworks®  
Published August 2022

### Ransom Recovery Cost

19% agree cost to recover from Ransom is > \$1M

Cost Range	Percentage
<\$1K	~1%
\$1K-10K	~5%
\$10K - 50K	~10%
\$50K - \$100K	~16%
\$100K - \$500K	~17%
\$500K - \$1M	~15%
>\$1M	~18%

MENLO SECURITY  
Survey of 505 InfoSec Leaders  
Published August 2022

### # of "Successful" Ransom

July had lowest number of attacks so far this year

Month	2020	2021	2022
Jan	~15	~18	~12
Feb	~12	~15	~18
Mar	~18	~20	~15
Apr	~15	~22	~18
May	~18	~20	~22
Jun	~20	~22	~18
Jul	~15	~20	~18
Aug	~18	~20	~15
Sep	~22	~20	~18
Oct	~25	~22	~15
Nov	~18	~20	~18
Dec	~22	~20	~18

BLACKFOG Privacy. Security. Prevention.  
Published August 2022

### Size of Ransom Victims

Hackers return to targeting smaller firms in July

Month	2020	2021	2022
Jan	~10	~12	~10
Feb	~8	~10	~8
Mar	~12	~25	~10
Apr	~10	~12	~10
May	~15	~18	~10
Jun	~18	~20	~15
Jul	~10	~12	~8
Aug	~12	~15	~10
Sep	~8	~10	~8
Oct	~10	~12	~8
Nov	~12	~15	~10
Dec	~15	~18	~10

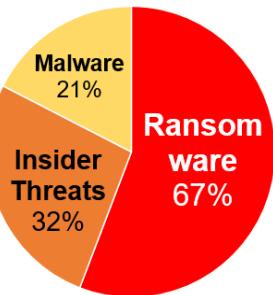
BLACKFOG Privacy. Security. Prevention.  
Published August 2022

# Cyber Insights: Cyber & People

Click each image to see each report in full. All were published in month to September 2022

## Cyber Risk CISOs fear most

67% of CISOs say Ransomware is most significant

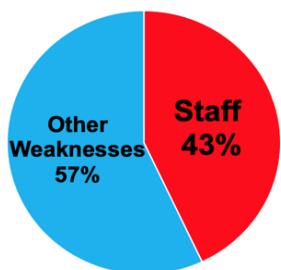


HEIDRICK & STRUGGLES

Survey of 327 CISOs  
Published August 2022

## The Weakest Link in Cyber

43% of InfoSec Leaders say Staff are weakest link

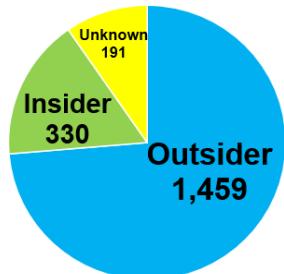


MENLO SECURITY

Survey of 505 InfoSec Leaders  
Published August 2022

## Who Causes Data Breaches

Almost 75% of breached files caused by Outsiders

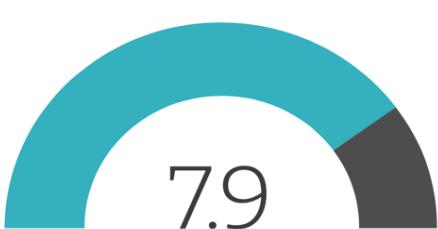


FLASHPOINT

Published August 2022

## Staff spot most Email Fraud

Most Employees are Highly Capable

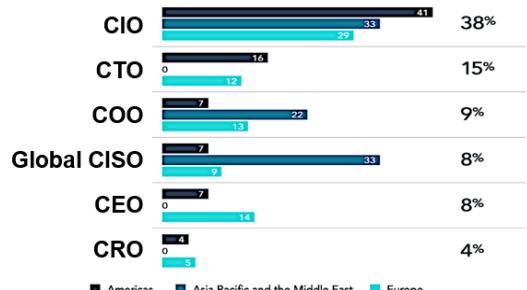


SC MEDIA

Survey of 221 Professionals  
Published August 2022

## CISO Reporting Lines

38% of CISOs still report directly to the CIO

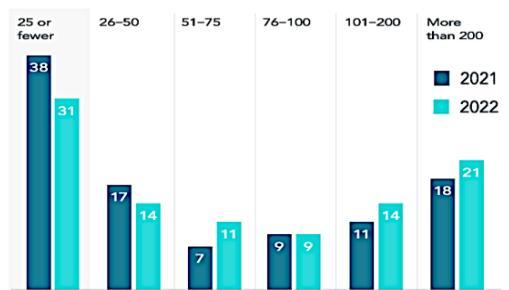


HEIDRICK & STRUGGLES

Survey of 327 CISOs  
Published August 2022

## Cyber Teams run by CISOs

21% of CISOs in the survey have over 200 staff

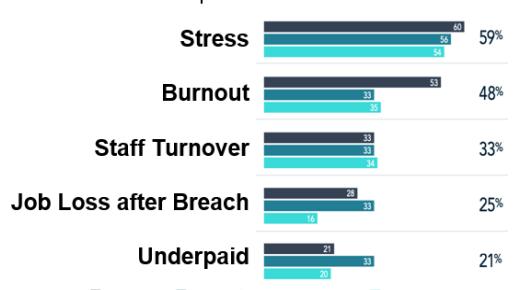


HEIDRICK & STRUGGLES

Survey of 327 CISOs  
Published August 2022

## CISO personal challenges

59% of CISOs report stress related to their role

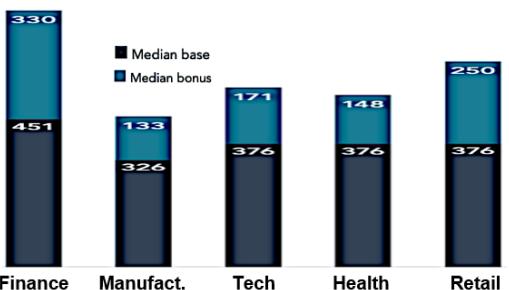


HEIDRICK & STRUGGLES

Survey of 327 CISOs  
Published August 2022

## CISO Compensation

Finance CISOs paid 70% more than Manufacturing



HEIDRICK & STRUGGLES

Survey of 327 CISOs  
Published August 2022

# Cyber Insights: Ransom Vectors & Techniques

Click each image to see each report in full. All were published in month to September 2022

### How Firms hit by Ransom

Phishing highest risk for ransom attack at 70%

Risk Type	Percentage
Phishing	70%
Unpatched Vulnerabilities	56%
Supply Chain	44%
Malware	44%
Wide Privileged Access	42%
Segmentation	22%
Insider Threat	16%

The CISO Circuit by YL VENTURES Published August 2022

### How Firms hit by Ransom

Email Phishing is now the top attack vector

COVEWARE Published August 2022

### How Firms hit by Ransom

17% of victims still don't know how hackers got in

MENLO SECURITY Survey of 505 InfoSec Leaders Published August 2022

### Most Pervasive Ransomware

Lockbit 2.0 now used in 30% of ransom attacks

INTEL471 Published August 2022

### Data Stolen by Ransomware

Continuous increase in total Terabytes stolen

enisa Based on 600+ Ransom Incidents Published August 2022

### Data Stolen by Ransomware

Top Ransomware Exfiltration Country: China (24%)

BLACKFOG Privacy. Security. Prevention. Published August 2022

### Ransom Gangs vs Finance

Finance & Insurance hit most by LockBit & Conti

UNIT 42 BY PALO ALTO NETWORKS Published August 2022

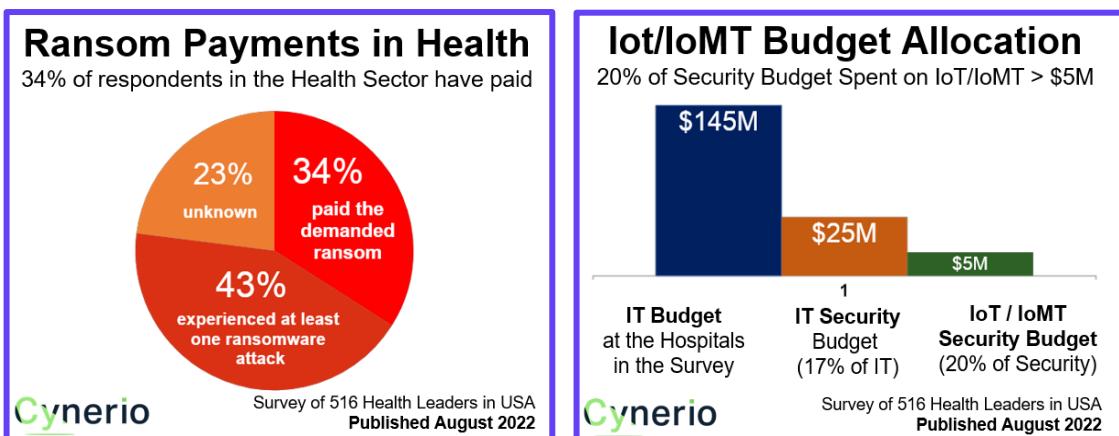
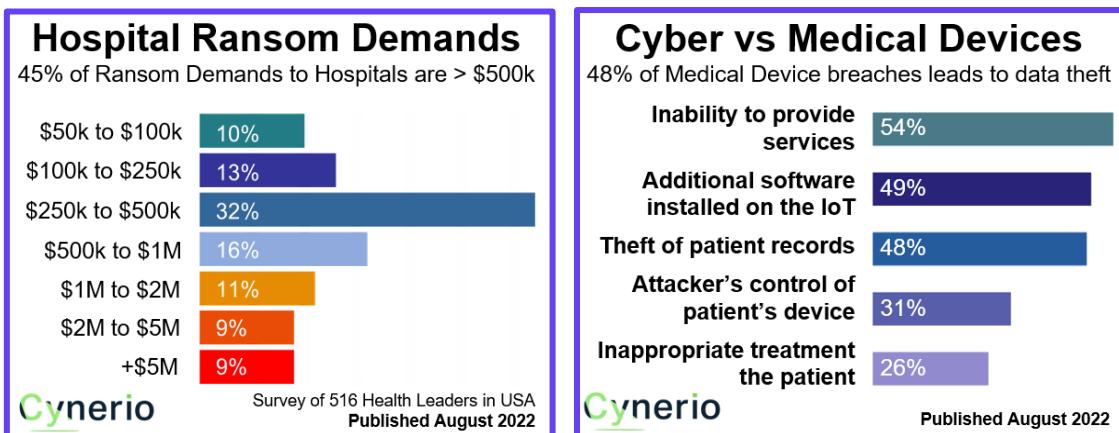
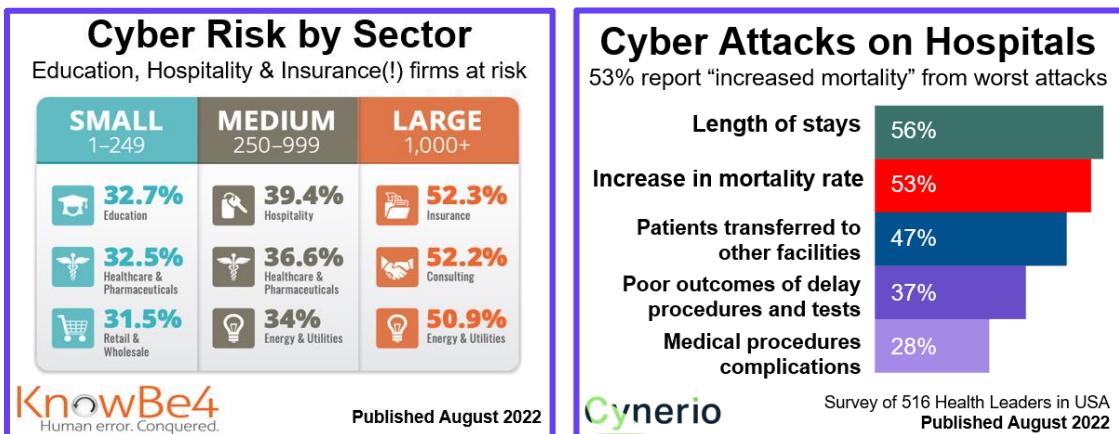
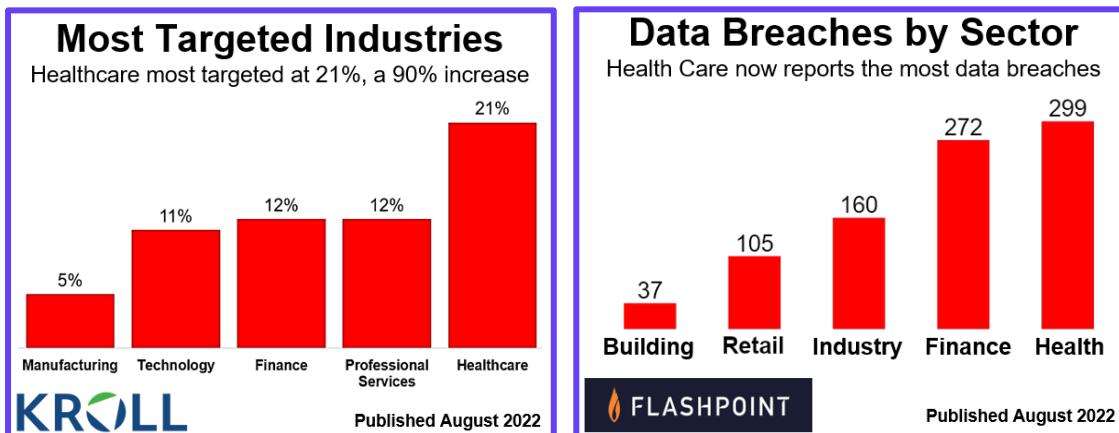
### Ransomware Recovery

64% of firms implements a Ransom Recovery plan

The CISO Circuit by YL VENTURES Published August 2022

# Cyber Insights: Healthcare Attacks

Click each image to see each report in full. All were published in month to September 2022



# Cyber Insights: Cloud Security

Click each image to see each report in full. All were published in month to September 2022

### Ransomware in the Cloud

75% believe that ransomware exists in the cloud

Timeframe	Percentage
At Present	75%
Next Year	14%
Next Few Years	11%

**The CISO Circuit by YL VENTURES**

Published August 2022

### Defence vs Cloud Ransoms

57% believe slight solution changes are needed

Solution Change	Percentage
None	6%
No change	14%
New Solutions	23%
Slight Changes	57%

**The CISO Circuit by YL VENTURES**

Published August 2022

### Cyber Attacks on Clouds

47% of successful attacks involve Data Exfiltration

Attack Type	Percentage
Account Takeover	34%
Adversarial Access	35%
System Sabotage	37%
Access Loss	37%
Data Exfiltration	47%

Survey of 960 IT Professionals

**proofpoint.**

Published August 2022

### Cyber Attacks on Clouds

58% of successful attacks involve 3rd Parties

Target	Percentage
Remote Staff	35%
Office Staff	36%
Execs	42%
Clients	43%
3rd Parties	58%

Survey of 960 IT Professionals

**proofpoint.**

Published August 2022

### Visibility of Cloud Security

81% of firms lack visibility of internet-facing assets

Category	Percentage
Restrict Network Access for Mission-Critical & Sensitive Resources	36% (Blue)
Full Visibility of All Resources Accessible from the Internet	19% (Blue)
Restrict Network Access for Mission-Critical & Sensitive Resources	64% (Red)
Full Visibility of All Resources Accessible from the Internet	81% (Red)

Survey of 326 firms in N. America

**ermetic**

Published August 2022

### Controls for Cloud Security

Basic Controls for Managing Access Permissions

- #1 = Policy checking with business functions
- #2 = Permissions granted just-in-time basis
- #3 = Automated detection of accessibility
- #4 = Least Privilege Method access grant
- #5 = Accessibility & Resources Visibility

**ermetic**

Survey of 326 firms in N. America

Published August 2022

### Who owns Cloud Security

21% of firms have Dedicated Cloud Security Team

Team	Percentage
IT/Operations	7%
Development	6%
SRE	5%
DevOps	4%
Dedicated Team	3%

Survey of 326 firms in N. America

**ermetic**

Published August 2022

### Spend on Cloud Security

56% of large firms spend over \$10M on CloudSec

Spending Range	Percentage
1M - 5M	22%
6M - 10M	21%
11M - 20M	21%
21M - 50M	22%
> 50M	13%

Survey of 326 firms in N. America

**ermetic**

Published August 2022

# Cyber Insights: *Ransomware*

Click each image to see each report in full. All were published in month to September 2022

### Ransom Victims by Sector

Education & Government still most frequent in July

Sector	Count
Education	34
Government	30
Technology	24
Manufacturing	22
Healthcare	21

Published August 2022

### Top Ransomware Methods

63% of Blackmail uses Double Extortion Technique

Method	Percentage
Name and shame	37%
Data Auction	60%
Blackmail	63%

Survey of 125 Cyber Professionals  
Published August 2022

### Top Ransomware Variants

BlackCat is now the most common ransom variant

Rank	Ransomware Type	Market Share %
1	BlackCat	16.9%
2	Lockbit 2.0	13.1%
3	Hive	6.3%
4	Quantum	5.6%
4	Conti V2	5.6%
5	Phobos	5%
5	Black Basta	5%
5	AvosLocker	5%

Published August 2022

### Ransomware Victims

Previously Breached firms most likely future victims

- #1 = Suffered a past data breach
- #2 = Out of date systems
- #3 = Susceptibility to phishing
- #4 = Publicly visible critical ports
- #5 = Botnet infection

Review of 2,400 data breaches  
Published August 2022

### Initial Access for Ransom

67% of Threat actors use External Remote Services

Method	Percentage
Phishing	13%
CVE / Zero-Day Exploit	20%
External Remote Services	67%

Published August 2022

### Initial Access for Ransomware

48% of initial access by Ransomware is via S/W

Method	Percentage
Other	1%
Compromised Credentials	2%
Phishing	3%
Brute-force Attacks	5%
Software Vulnerability	48%

BY PALO ALTO NETWORKS  
Published August 2022

### Ransomware Solutions 2022

20% believe Point Ransom Solutions impractical

Belief	Percentage
Point Ransom Solutions impractical	20%
Ransomware solutions must focus on response and recovery	17%
Ransomware solutions must focus on prevention	14%

Published August 2022

### Protection against Ransom

Firewalls are most trusted tool against cyber threat

- #1 Firewalls (74%)
- #2 Network perimeter strength (66%)
- #3 Phishing protection (62%)
- #4 Mobile device protection (61%)
- #5 Endpoint protection (59%)

Survey of 505 InfoSec Leaders  
Published August 2022

# Cyber Insights: Attacks & Vulnerabilities

Click each image to see each report in full. All were published in month to September 2022

### Cyber Attack Vectors

Email Phishing still most successful for hackers

Category	Q1-19	Q3-19	Q1-20	Q3-20	Q1-21	Q3-21	Q1-22
RDP Compromise	\$65	\$53	\$60	\$35	\$55	\$40	\$35
Email Phishing	\$35	\$38	\$25	\$38	\$30	\$30	\$32
Software Vulnerability	\$5	\$10	\$5	\$10	\$15	\$18	\$18
Other	\$5	\$5	\$5	\$5	\$5	\$5	\$5

Courtesy Coveware

### Vulnerabilities Hackers Love

"Most Mentioned" in Bad Actor chats = Log4Shell

Vulnerability	Percentage
Log4Shell	71%
ProxyShell	18%
ProxyLogon	9%
VMware	3%

### Top Malware File Types now

34% now spreadsheet (eg XLS) & Archive (eg ZIP)

File Type	Percentage
Spreadsheets	34%
Archives	32%
Scripts and executables	12%
Documents	10%
PDF	5%
Other	3%

Analyzed by HP Wolf Security Experts

### Top Threat Incident Types

Ransomware poses the biggest threat at 33%

Threat Type	Percentage
Web Compromise	5%
Illegal Access	26%
Email Compromise	30%
Ransomware	33%

### Top Witnessed Exploits

30% of exploits come from DoublePulsar

Exploit Type	Percentage
DoublePulsar	31%
Log4j	29%
SMB	27%
SSH	13%

### Malware Detection

Malware detected by Nuspire falling in latest data

Date	Malware Activity	Moving Average
1 Apr '22	~400,000	~380,000
15 Apr '22	~380,000	~390,000
6 May '22	~350,000	~380,000
20 May '22	~420,000	~400,000
3 Jun '22	~300,000	~380,000
24 Jun '22	~280,000	~350,000

### What Data is most Breached

22% of Breached Files hold victim's Date of Birth

Data Type	Percentage
Name	67%
SSN	42%
Financial	26%
Address	28%
Date of Birth	22%

### Mega Breaches: Great News

Only 5 new breaches of >1M records in H1 2022

H1 Year	Breaches
2018 H1	13
2019 H1	34
2020 H1	34
2021 H1	17
2022 H1	5

# Cyber Insights: Phish & Email Attacks

Click each image to see each report in full. All were published in month to September 2022

### Email Security Concerns

Ransomware is the top concern for Organizations

Concern	Percentage
Resources shortage	11
Losing money	25
Receive Files	47
Phish	60
Ransom	65

**SC MEDIA** Survey of 221 Professionals Published August 2022

### Email Security Strategies

Top Drivers Organizations consider in Security

Strategy	Percentage
Client Demands	19
Remote Work	40
Monetary Loss	42
Regulatory Requirement	46
Loss of Data Breach	67

**SC MEDIA** Survey of 221 Professionals Published August 2022

### Cyber Attacks via Email

Phishing is the most common attack via email

Attack Type	Percentage
Phish	68.47%
Scam	8.35%
Malware	7.01%
BEC	6.08%
Ransom Extortion	5.64%
Other	4.44%

**\Abnormal** Published August 2022

### Phishing Attacks via SaaS

Increase in phishing activity in the latter half of 2021

Date	Personal Branding	Design/Prototyping	Notetaking/Collaboration	Website Builders	Form Builders	File Sharing
2020-01	0.1	0.1	0.1	0.1	0.1	0.1
2020-07	0.2	0.2	0.2	0.2	0.2	0.2
2021-01	0.5	0.5	0.5	0.5	0.5	0.5
2021-07	1.5	1.5	1.5	1.5	1.5	1.5
2022-01	2.5	2.5	2.5	2.5	2.5	2.5
2022-04	4.5	4.5	4.5	4.5	4.5	4.5

**UNIT 42 BY PALO ALTO NETWORKS** Published August 2022

### Phishing Attack Volume

1% of all email to firms with 500 mailboxes is Phish

Mailbox Size	Percentage
0-500	1.0%
1,000-1,500	1.8%
3K - 5K	1.5%
10K - 20K	0.7%
50K - 300K	0.4%

**\Abnormal** Published August 2022

### Cyber in Identity Crimes

2021: 677 Cases of Identity Crimes in Non-finance

Year	Cases
2019	331 cases
2020	202 cases
2021	677 cases

**ITRC IDENTITY THEFT RESOURCE CENTER** Published August 2022

### Threats in Removable Media

52% of Threats is designed to Exploit USB

Threat Type	Percentage
Remote Access	51%
Industrial Specific	32%
Disruptive Against OT	81%
Designed for USB	52%

**Honeywell** Published August 2022

### Cyber Supply Chain Resilience

New Version Launched

The report includes sections such as Executive Summary, Introduction, Objectives, Scope, Methodology, Key Findings, and Recommendations.

# Cyber Insights: Practices & Activities

Click each image to see each report in full. All were published in month to September 2022

### Highest Botnet Activities

38% of Botnets now observed are Torpig

Botnet	Percentage
Mirai	4%
Andromeda	16%
STRRAT	18%
Sora	24%
Torpig	38%

### Risk Awareness Practices

Best practices for staff cyber security awareness

- #1 = Use real-world Attack Methods
- #2 = Don't do this alone
- #3 = Don't try to train on everything
- #4 = Make it relevant
- #5 = Treat programme like marketing

Published August 2022

Published August 2022

### STRRAT Botnet Activity

Highest Level of Activity in the month of May

Date	Activity Level
1 Apr '22	~25,000
15 Apr '22	~18,000
6 May '22	~40,000
20 May '22	~12,000
3 Jun '22	~25,000
24 Jun '22	~10,000

### Threat Intelligence TIBER EU

Purple Teaming Best Practices

Published Aug 2022

### Cyber Supply Chain Resilience

New Version Launched

Published Aug '22

### Latest Ransomware Trend

Sophos X-Ops Active Adversary

Published Aug 2022

### Metaverse or Metaworse?

Cyber Threats in Metaverse

Published Aug 2022

### Ransom Defense Blueprint

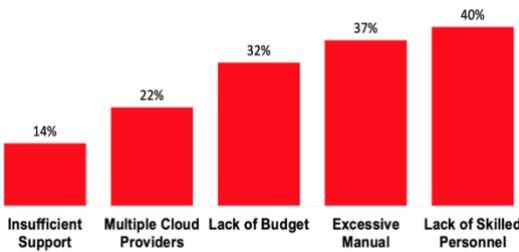
Action Plan for SMEs

# Cyber Insights: Cyber Budgets & ROI

Click each image to see each report in full. All were published in month to August 2022

## Budgets & Barriers to Cyber

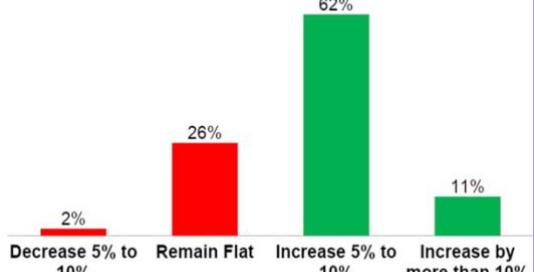
32% of CISOs say "Lack of Budget" is a key barrier



Survey of 200 CISOs  
Published July 2022

## Cyber Security Budgets

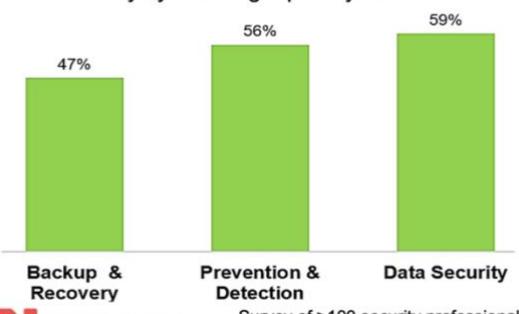
73% of CISOs expect their budget to grow this year



Survey of 200 CISOs  
Published July 2022

## Cyber Budgeting Priority

Data security cyber budget priority in 59% of firms



Survey of >100 security professionals  
Published July 2022

## Cyber Tools with poor ROI

Security Tools that CISOs say are "Too Expensive"

- #1 Security Info & Event Mngt (SIEM)
- #2 Network Traffic Analysis (NTA)
- #3 Cloud Access Sec Broker (CASB)
- #4 User & Entity Behavior Analytics
- #5 Deception



Survey of 200 CISOs  
Published July 2022

## Cloud Cyber Security Threat

Misconfiguration of the Cloud Platform is top threat

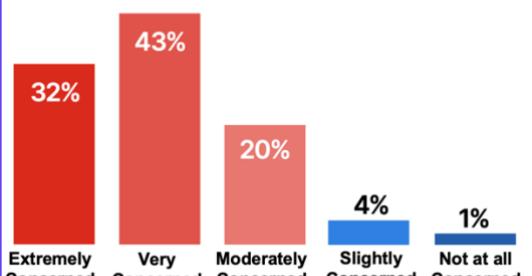
- #1 Misconfiguration of Cloud Platform
- #2 Insecure interfaces/APIs
- #3 Exfiltration of sensitive data
- #4 Unauthorized Access
- #5 Hijacked accounts, services, traffic



Survey of 800+ Cyber Pros  
Published July 2022

## Cloud Cyber Security Fears

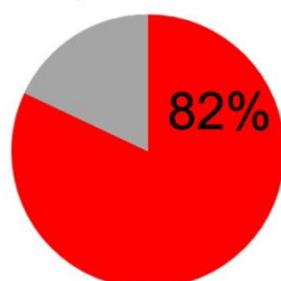
32% are extremely concerned about Cloud Security



Survey of 800+ Cyber Pros  
Published July 2022

## Cyber Insurance Inflation

82% of Insurers expect increase over the next 2 yrs



Survey of 400 Global Insurers  
Published July 2022

## Cyber Insurance Price Rises

Lack of understanding is #3 reason for price rises

- #1 Sophistication of threat actors
- #2 Cost of ransomware attacks
- #3 Lack of accurate understanding of cyber posture at insured firms



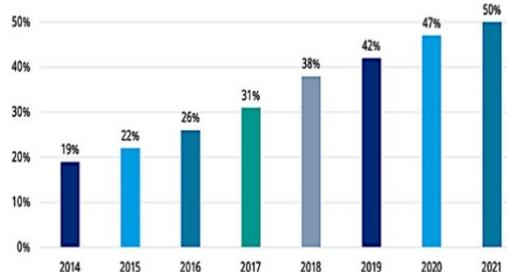
Survey of 400 Global Insurers  
Published July 2022

# Cyber Insights: Cyber Insurance

Click each image to see each report in full. All were published in month to August 2022

## Cyber Insurance Popularity

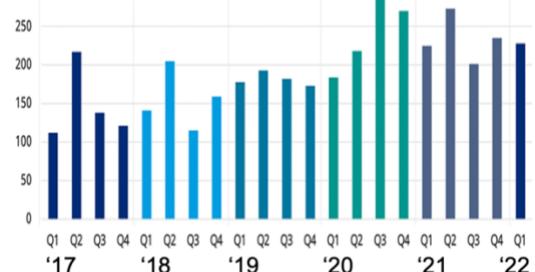
50% of insured firms in USA now buy Cyber cover



Published July 2022

## Cyber Insurance # of Claims

# of Claims on Cyber Insurance in USA falling



Published July 2022

## Cyber Insurance Inflation

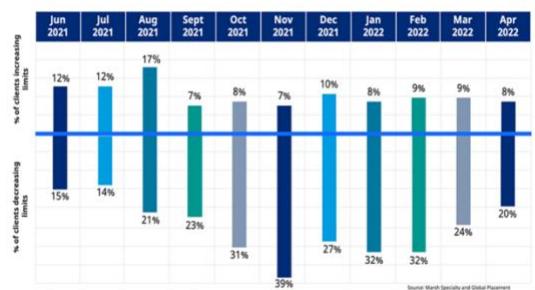
Annual inflation in USA has fallen to 90% price rise



Published July 2022

## Cyber Insurance Cover

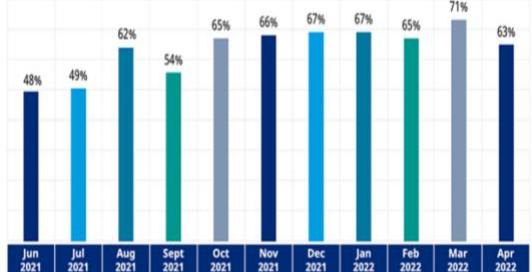
Only 20% reduced their firms' limits in latest survey



Published July 2022

## Cyber Insurance Retentions

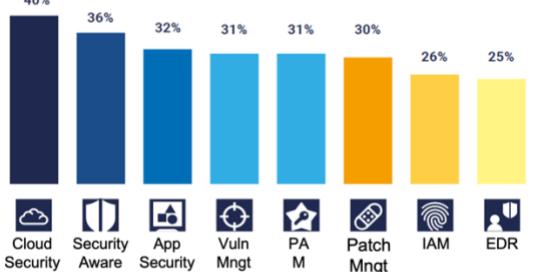
63% of insured are retaining more risk themselves



Published July 2022

## Cyber Underwriting

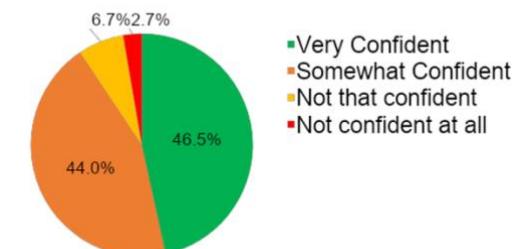
40% of Insurers agree Cloud Security is important



Survey of 400 Global Insurers  
Published July 2022

## Cyber Underwriting

46.5% very confident in their underwriting process



Survey of 400 Global Insurers  
Published July 2022

## Cyber Insurance Changes

#1 change by Insurers = "require more evidence"

**#1 = Require detailed evidence**  
of security posture at customers

**#2 = Reduce # of insured firms**  
to limit risk exposure

**#3 = Require more transparency**  
from firms about security metrics



Survey of 400 Global Insurers  
Published July 2022

# Cyber Insights: Ransomware

Click each image to see each report in full. All were published in month to August 2022

### # of Ransom Incidents Flat

Number has been roughly flat for six months

Month	2020	2021	2022
Jan	~45%	~55%	~60%
Feb	~40%	~50%	~55%
Mar	~45%	~55%	~60%
Apr	~40%	~50%	~55%
May	~50%	~60%	~65%
Jun	~55%	~65%	~70%
Jul	~50%	~60%	~65%
Aug	~55%	~60%	~65%
Sep	~60%	~65%	~70%
Oct	~65%	~70%	~75%
Nov	~60%	~65%	~70%
Dec	~65%	~70%	~75%

■ 2020 ■ 2021 ■ 2022

**TITANIAM** Published July 2022

### # of Ransom Incidents down

Drop in incidents in Q1 '22 compared to last year

Quarter	2020	2021	2022
Q1 '20	~20%	-	-
Q2 '20	-	~30%	-
Q3 '20	-	~65%	-
Q4 '20	-	~65%	-
Q1 '21	-	~65%	-
Q2 '21	-	~75%	-
Q3 '21	-	~70%	-
Q4 '21	-	~75%	-
Q1 '22	-	~65%	-

**beazley** Published July 2022

### Ransom paid after data theft

60% of exfiltration attacks led to extortion of victims

Category	Percentage
Exfiltration led to ransom payment	59%
Exfiltration did not lead to ransom payment	41%

Survey of >100 security professionals

**TITANIAM** Published July 2022

### Size of Ransom Victims Up

Active Hackers targeted larger firms in June

Month	2020	2021	2022
Jan	~10%	~10%	~10%
Feb	~10%	~10%	~10%
Mar	~10%	~10%	~10%
Apr	~10%	~10%	~10%
May	~10%	~10%	~10%
Jun	~10%	~10%	~10%
Jul	~10%	~10%	~10%
Aug	~10%	~10%	~10%
Sep	~10%	~10%	~10%
Oct	~10%	~10%	~10%
Nov	~10%	~10%	~10%
Dec	~10%	~10%	~10%

■ 2020 ■ 2021 ■ 2022

**BLACKFOG** Published July 2022

### Sectors targeted by Ransom

Industrial Sector targeted most at 18.4% of attacks

Sector	Percentage
Government	5.5%
Healthcare	6.4%
Construction	7.9%
Technology	8.7%
Industrial	18.4%

**digital shadows** Published July 2022

### Ransom Victims by Sector

Education & Government now breached most often

Sector	Count
Education	28
Government	25
Manufacturing	21
Technology	21
Healthcare	18

**BLACKFOG** Published July 2022

### Ransom Gang Locations

Top Ransomware Exfiltration Country: China (24%)

Location	Percentage
China	24%
Rest of the World	55%
Russia	19%
Ukraine	1%
Iran	1%

**BLACKFOG** Published July 2022

### Action after Data Exfiltrated

64% of Security Pros "very interested" in new tools

Interest Level	Percentage
Very interested	64%
Somewhat interested	36%

**TITANIAM** Survey of >100 security professionals Published July 2022

# Cyber Insights: Phishing

Click each image to see each report in full. All were published in month to August 2022

### Email now top Cyber Vector

Email Phishing now most successful for hackers

Category	Q1-19	Q3-19	Q1-20	Q3-20	Q1-21	Q3-21	Q1-22
RDP Compromise	\$55	\$53	\$58	\$60	\$55	\$45	\$38
Email Phishing	\$35	\$38	\$28	\$38	\$32	\$35	\$35
Software Vulnerability	\$10	\$12	\$15	\$18	\$15	\$18	\$18
Other	\$10	\$12	\$15	\$18	\$15	\$18	\$18

Courtesy Coveware

**BLACKFOG**  
Privacy. Security. Prevention.

Published July 2022

### Phish are part of most Hacks

Phishing used in most publicised Breaches in USA

Hack Type	Count
Malware	22
Ransomware	55
Phishing	107

**ITRC** | IDENTITY THEFT RESOURCE CENTER

Published July 2022

### Phish is now top Cyber Fear

Phishing is the Entry Point that the Pros fear most

- #1 = Phishing
- #2 = Ransomware
- #3 = Misconfigurations
- #4 = Poor Passwords
- #5 = Lack of Patching

**coresecurity**  
by HelpSystems

Global Survey of cybersecurity professionals  
Published July 2022

### Most Phish-prone™ Firms

Large Insurers at high risk, before staff are trained

Size	Industry	Percentage
SMALL 1-249	Education	32.7%
MEDIUM 250-999	Hospitality	39.4%
LARGE 1,000+	Insurance	52.3%
SMALL 1-249	Healthcare & Pharmaceuticals	32.5%
MEDIUM 250-999	Healthcare & Pharmaceuticals	36.6%
LARGE 1,000+	Consulting	52.2%
SMALL 1-249	Retail & Wholesale	31.5%
MEDIUM 250-999	Energy & Utilities	34%
LARGE 1,000+	Energy & Utilities	50.9%

**KnowBe4**  
Human error. Conquered.

Published July 2022

### Benefit of Phishing Training

Insurers, Hospitality & Education see huge benefit

Sector	Before Training (%)	After Training (%)
Education	50	20
Hospitality	50	20
Insurance	50	20

**KnowBe4**  
Human error. Conquered.

Survey of 30,000+ firms  
Published July 2022

### Top Faked Sites For Phishing

LinkedIn Still Rank Number One Brand to be Faked

Brand	Percentage
LinkedIn	45%
Microsoft	13%
DHL	12%
Amazon	9%
Apple	3%

**CHECK POINT**  
YOU DESERVE THE BEST SECURITY

Published July 2022

### Cyber Awareness for Staff

What's needed by Awareness Initiatives in Firms

- #1 = Program Management
- #2 = Employee Training Time
- #3 = Staff Awareness Program
- #4 = Better Staff Engagement
- #5 = Bigger Budget

**SANS** SECURITY AWARENESS

Published July 2022

### Business Email Compromise

Most vulnerable are Professional Services & Assoc.

Industry	2020 (%)	2021 (%)	Q1 2022 (%)
Professional Services	21	22	30
Education	7	8	12
Finance	17	14	12
Healthcare	16	12	11
Manufacture	8	10	8

**beazley**

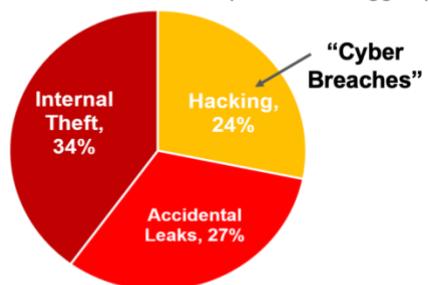
Published July 2022

# Cyber Insights: Data Breaches

Click each image to see each report in full. All were published in month to August 2022

## Top Causes of Data Breach

Internal causes most breaches (but not the biggest)



**TOMIC**  
THE FAKE DATA COMPANY

Survey of 1,000 U.S. Professionals  
Published July 2022

## Effect of Data Breach

28% experienced an Insurance Premium Increase



**TOMIC**  
THE FAKE DATA COMPANY

Survey of 1,000 U.S. Professionals  
Published July 2022

## Cyber Breach Causes in UK

20% of cyber breaches at small firms via a 3<sup>rd</sup> party

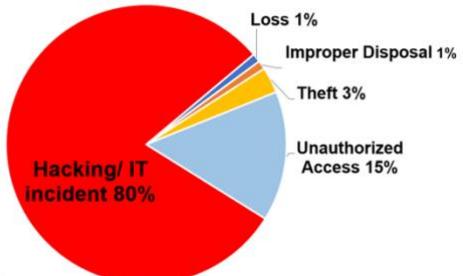
- #1 = Third Party Attack
- #2 = External Plugin Malware
- #3 = Email/Website Malware
- #4 = Accidentally divulging information
- #5 = No Cyber Security Protection

**DirectLine Group**

Survey of 2,000 UK Adults  
Published July 2022

## Cybersecurity in Healthcare

80% of breaches caused by Hacking/IT incidents

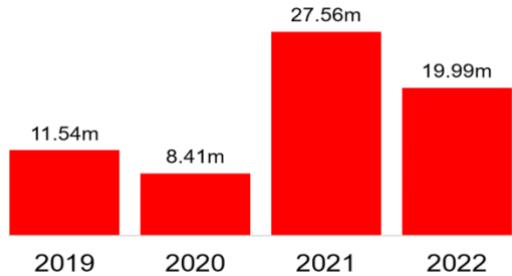


**Fortified**  
HEALTH SECURITY

Data from USA HHS  
Published July 2022

## Cyber Breaches in Health fall

19.99m American Health Records Breached in H1

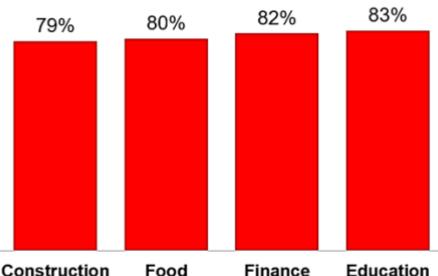


**Fortified**  
HEALTH SECURITY

Data from USA HHS  
Published July 2022

## Sensitive Data in Firms

Education uses the most sensitive data at 83%

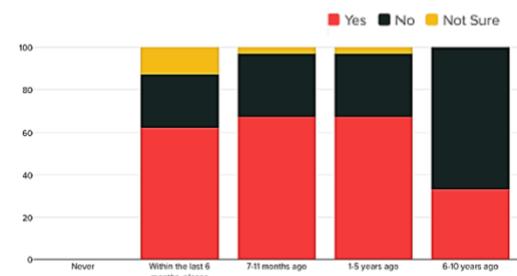


**TOMIC**  
THE FAKE DATA COMPANY

Survey of 1,000 U.S. Professionals  
Published July 2022

## Attacks involving data theft

Data exfiltration occurrence rising to 68% of attacks

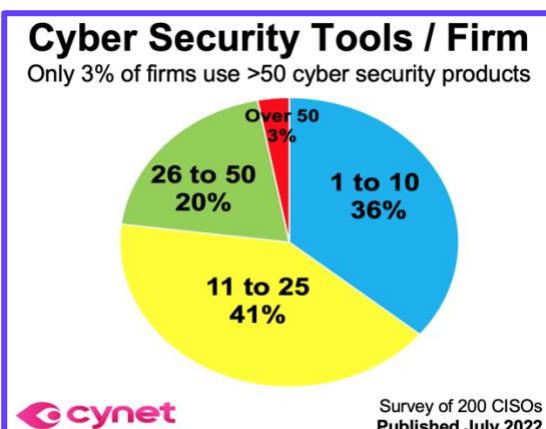
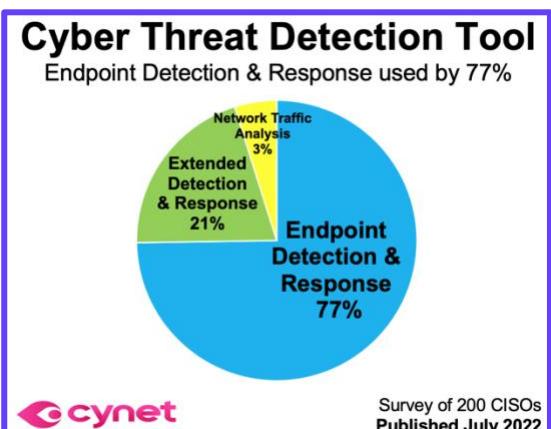
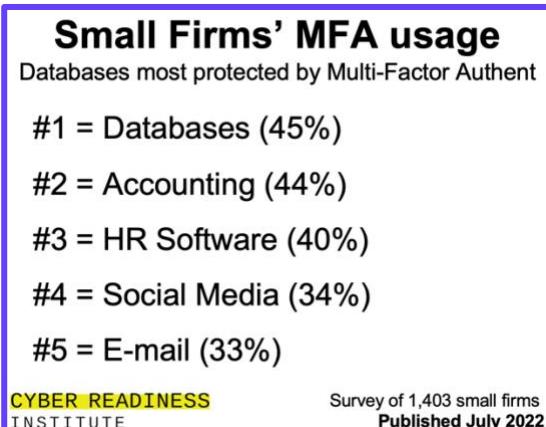
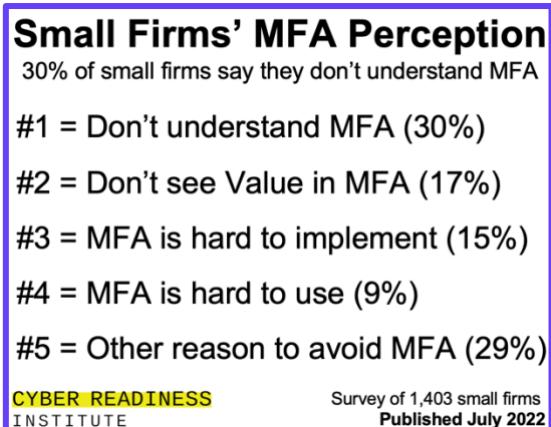
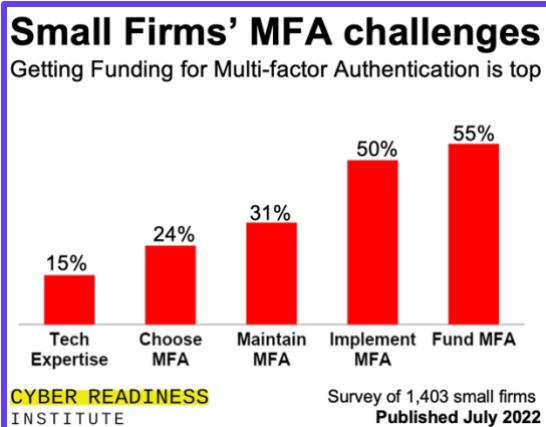
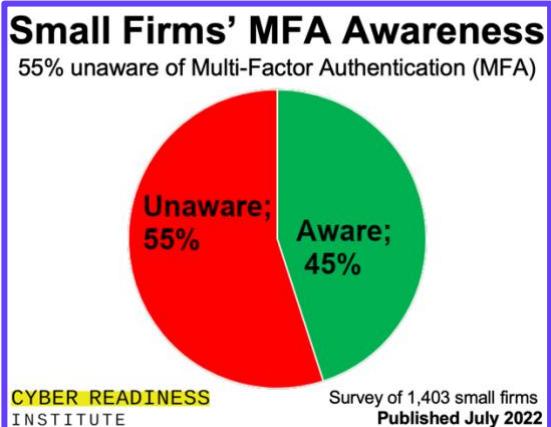


**TITANIAM**

Survey of >100 security professionals  
Published July 2022

# Cyber Insights: MFA & Pen Testing

Click each image to see each report in full. All were published in month to August 2022



# Cyber Insights: Industrial & OT Security

Click each image to see each report in full. All were published in month to August 2022

### Industrial Cyber Security

Challenges faced in implementing Security Projects

Challenge	Percentage
Project Cost	27%
Legacy Infrastructure	32%
Technical Knowledge	34%
Lack of Device Control	36%
Scalability	39%

Survey of 800 participants  
Published July 2022

Barracuda

### Industrial Cyber Security

93% of firms had IIoT/OT projects fail

Reason	Percentage
Security Projects failed	93%
Tech Implementation took too long	55%
Tech too expensive	41%
No clear project owner	39%
Lack of Tech sourced	38%
No failure in Security Projects	7%

Survey of 800 participants  
Published July 2022

Barracuda

### Industrial Cyber Security

All Oil & Gas firms have suffered security incidents

Sector	Percentage
Biotech	82%
Energy	85%
Manufacturing	98%
Agriculture	98%
Oil & Gas	100%

Survey of 800 participants  
Published July 2022

Barracuda

### Firms' OT Security Risk

21% of Operational Tech is at "Severe" Cyber Risk

Risk Level	Percentage
Unknown	4%
Moderate	20%
High	98%
Severe	21%

SCADAfence

Survey of 3,500 Cyber Security Pros  
Published July 2022

### What reduces OT Security?

69% say it's a lack of Operational Technology Staff

Factor	Percentage
Lack of OT staff	69%
New Cyber Threats	18%
Compliance Requirements	8%
Other	5%

SCADAfence

Survey of 3,500 Cyber Security Professionals  
Published July 2022

### IoT Cyber Security: Reasons

Preventing another incident is top reason to Invest

Reason	Percentage
Comply with Industry Regulations	21%
Protect a private 5G System	25%
Business partner's request	29%
Prevent Recurrence of Incidents	30%

TREND MICRO

Survey of 900 respondents  
Published July 2022

### IoT Cyber Breach: Response

52% of firms improve security after incidents on IoT

Response	Percentage
Always/Usually	52%
Sometimes/Rarely	48%

TREND MICRO

Survey of 900 respondents  
Published July 2022

### IoT Cyber Attacks: the Cost

Worst attacks on IoT (Internet of Things) by sector

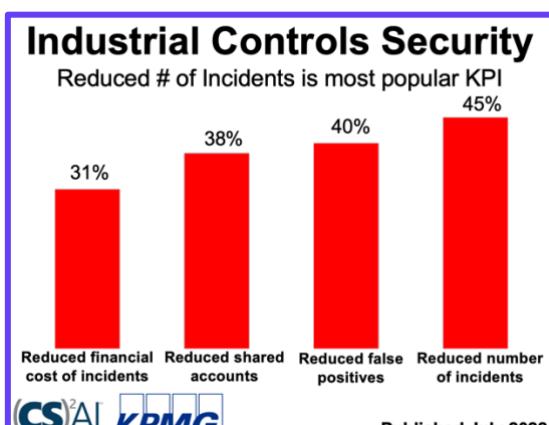
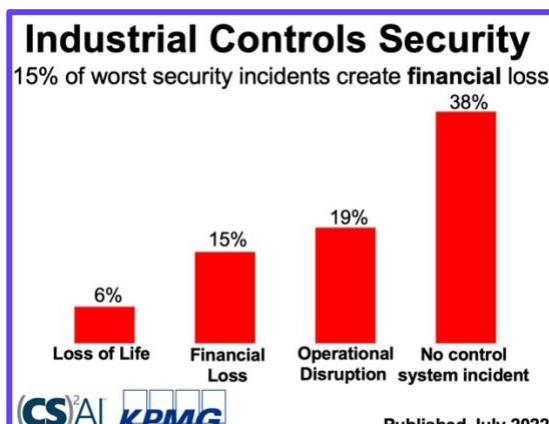
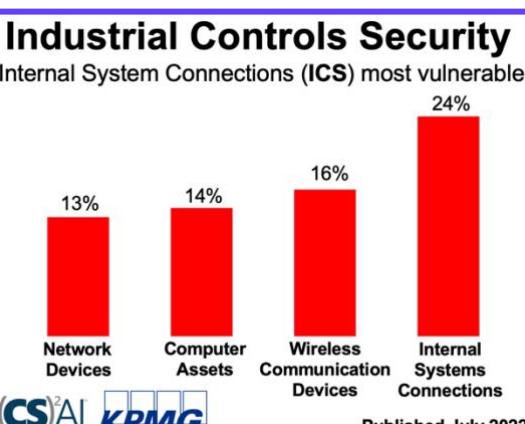
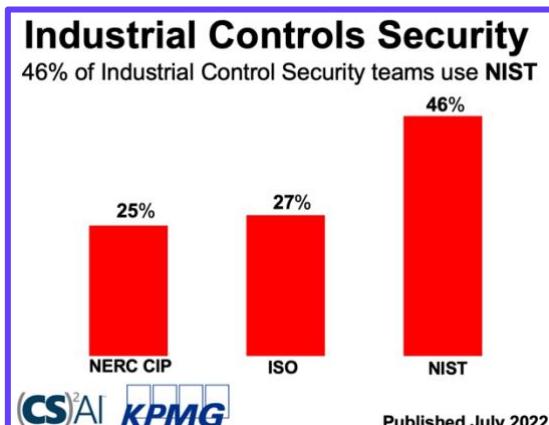
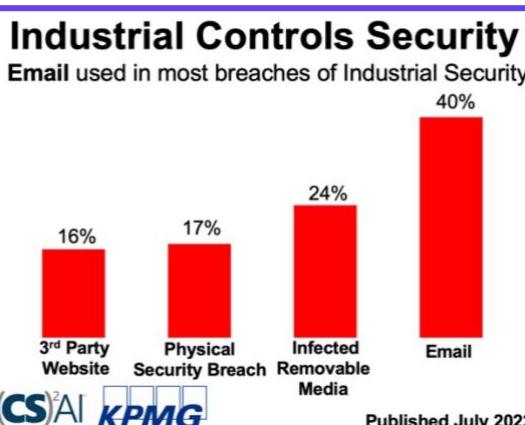
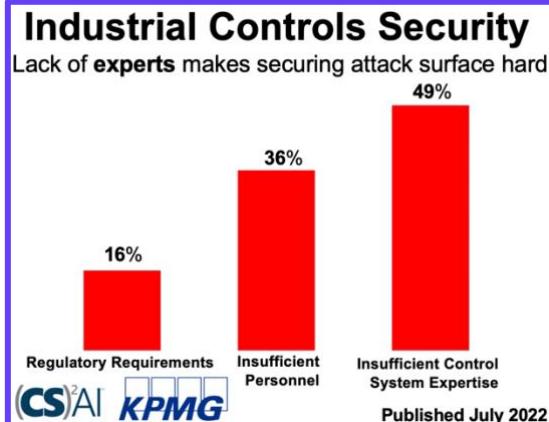
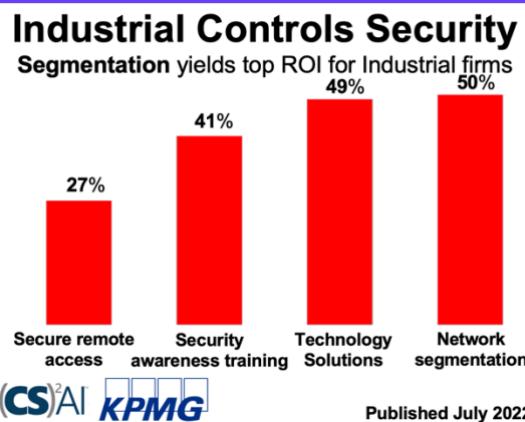
Sector	Cost
Manufacturing	\$1,832,203
Electricity	\$3,379,540
Oil and gas	\$3,385,887

TREND MICRO

Published July 2022

# Cyber Insights: *Industrial Controls Security*

Click each image to see each report in full. All were published in month to August 2022



# Cyber Insights: *Ransom Payments*

Click each image to see each report in full. All were published in month to July 2022

## Ransom Payments are down

Size of each known payment -34% from Q4 in 2021

Average known  
Payout =



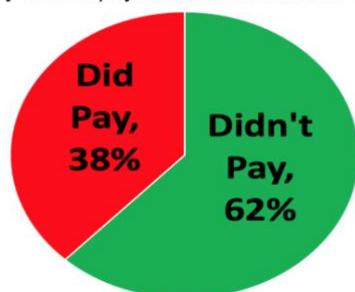
**USD \$211k**



Published June 2022

## Paying Ransomware Attacks

62% say did not pay most recent ransom demand



1,000 Cyber Experts in USA + Europe  
Published June 2022

## Prep for Ransom Recovery

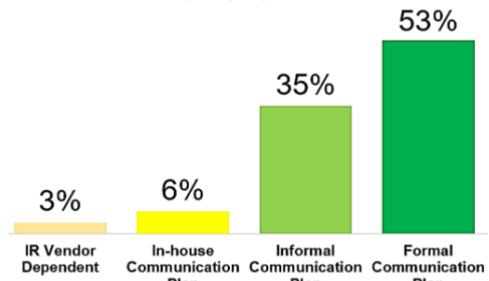
58% have ongoing Data Recovery Testing Plans



Online Survey of 620 IT & Cyber Professionals  
Across N. America & W. Europe  
Published June 2022

## Ransom Response Plans

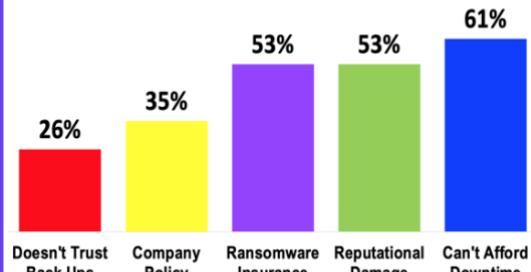
53% of firms have pre-prepared Formal Comms



Online Survey of 620 IT & Cyber Professionals  
Across N. America & W. Europe  
Published June 2022

## Reasons for Paying Ransom

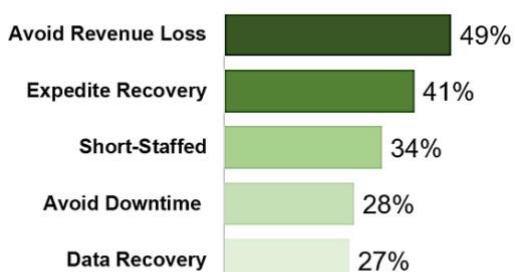
61% of firms who paid "can't afford any downtime"



1,000 Cyber Experts in USA + Europe  
Published June 2022

## Reasons for Paid Ransom

49% of Firms Paid Ransom to Avoid Revenue Loss



Survey of 1,456 cybersecurity professionals  
Published June 2022

## Resources for Recovering

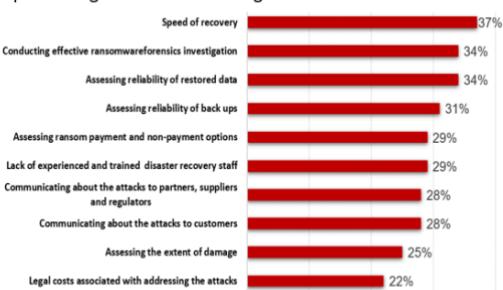
39% of firms handled their worst attack in-house



Survey of 858 senior decision-makers  
Published June 2022

## Challenges for Recovering

Top challenges when recovering from a ransomware incident



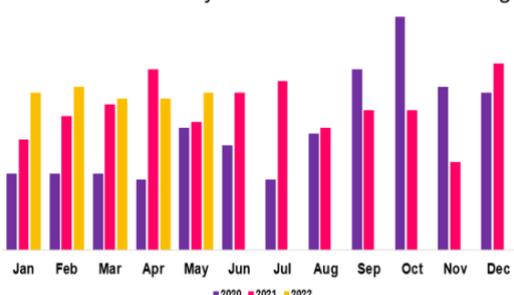
Survey of 463 IT leaders' decision makers  
Published June 2022

# Cyber Insights: *Ransom Frequency*

Click each image to see each report in full. All were published in month to July 2022

## # of “Successful” Ransoms

Good news: monthly success rate NOT increasing

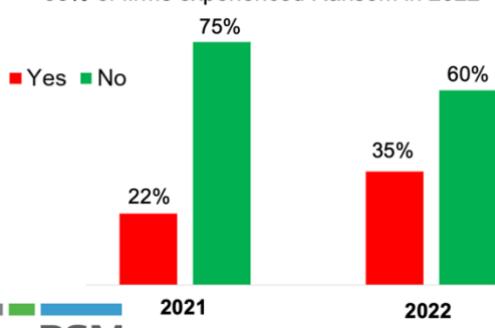


**BLACKFOG**  
Privacy. Security. Prevention.

Published June 2022

## Ransom “Victim” Rate

35% of firms experienced Ransom in 2022

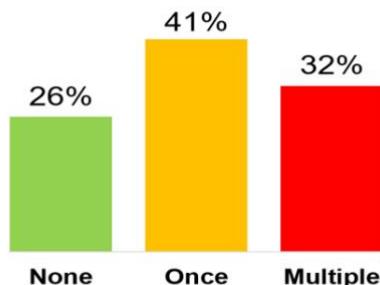


**RSM**

Published June 2022

## Ransom Repeat Victims

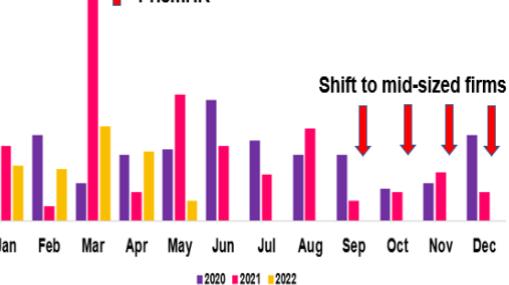
Multiple successful attacks on 32% of firms



**HITACHI**  
Inspire the Next

Online Survey of 620 IT & Cyber Professionals  
Across N. America & W. Europe  
Published June 2022

Skewed by PrismHR

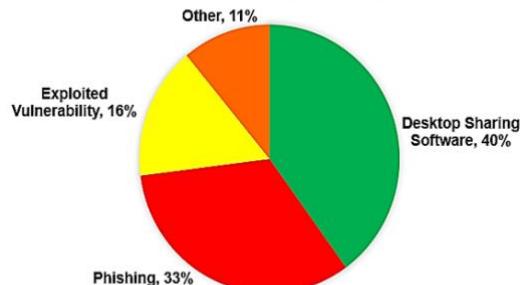


**BLACKFOG**  
Privacy. Security. Prevention.

Published June 2022

## Routes for Ransom Attacks

40% of breaches used Desktop Sharing Software

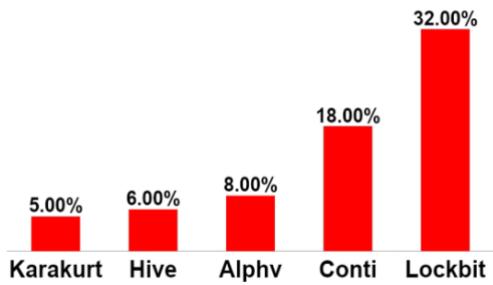


**II howden**

Published June 2022

## Active Ransomware Gangs

Lockbit most active gang for Q1 2022

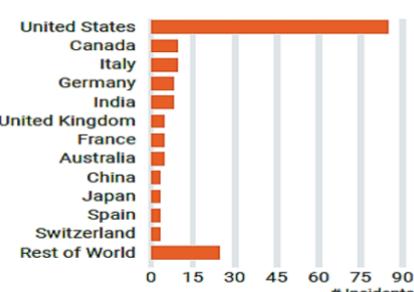


**KELA**

Published June 2022

## Ransom Incidents by Country

Ransom frequency highest in the United States



**RAPID7**

Review of ransomware data disclosures  
Published June 2022

## Ransom Incidents by Industry

Ransom frequency highest in healthcare industry



**RAPID7**

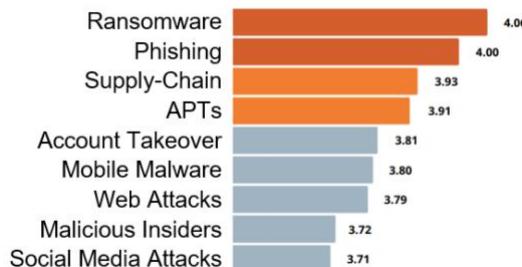
Review of ransomware data disclosures  
Published June 2022

# Cyber Insights: Ransomware Trends

Click each image to see each report in full. All were published in month to July 2022

## Ransom's Top Cyber Fears

Ransomware is top security concern for CISOs

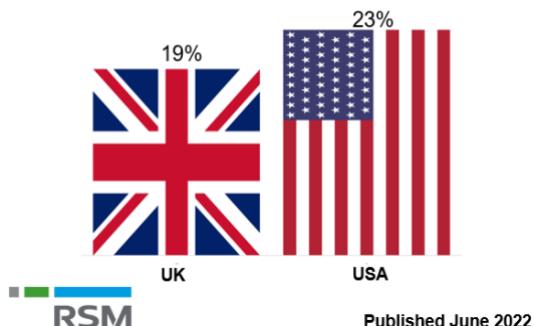


CISOs CONNECT

Survey of 411 CISOs  
Published June 2022

## Ransomware Frequency

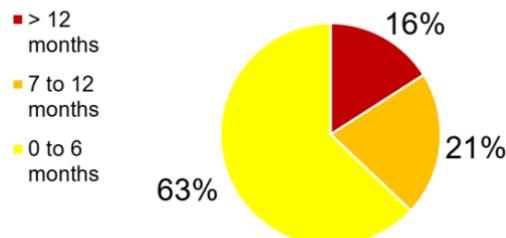
19% of UK execs report attack, narrowing gap with US



Published June 2022

## Before the Ransom Demand

16% of attackers were inside, a year before Ransom

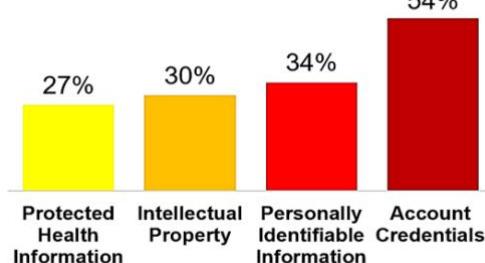


cybereason®

Survey of 1,456 cybersecurity professionals  
Published June 2022

## Ransom Double Extortions

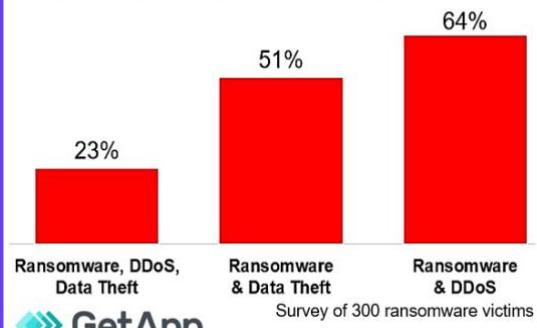
54% of attackers leverage Account Credentials



cybereason® Survey of 1,456 cybersecurity professionals  
Published June 2022

## Multifaceted Ransom Attacks

60% of ransom victims faced multifaceted attacks

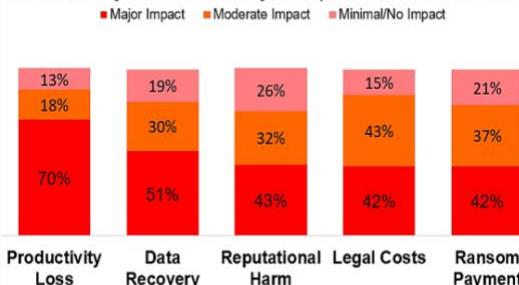


GetApp

Survey of 300 ransomware victims  
Published June 2022

## Impacts of Ransom Attacks

Productivity Loss has Major Impact on 70% of firms

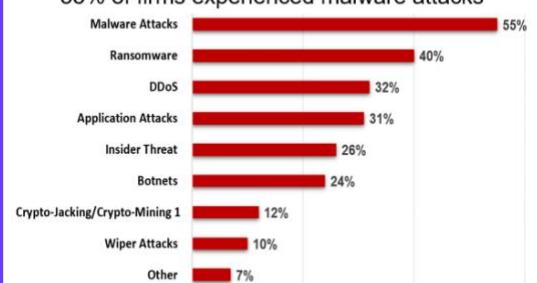


GetApp

Survey of 300 ransomware victims  
Published June 2022

## Cyber Attacks Experienced

55% of firms experienced malware attacks

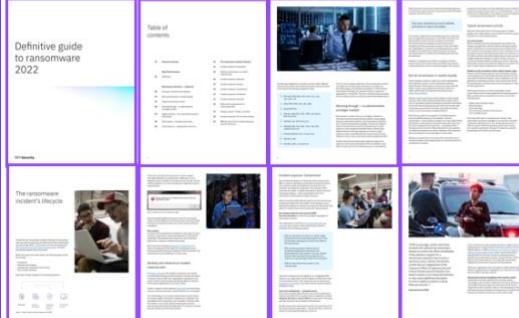


Cymulate

Survey of 858 senior decision-makers  
Published June 2022

## Definitive Guide to Ransomware 2022

IBM Security  
Published June 2022



# Cyber Insights: Cyber Risk Governance

Click each image to see each report in full. All were published in month to July 2022

### Cyber Risk Governance

Firms that are Not Breached discuss Cyber the most

Breaches	Percentage
No Breaches	15.2
All Responses	13.2
2-5 Breaches	10.8
1 Breach	9.4
6+ Breaches	8.8

Cymulate Survey of 858 senior decision-makers Published June 2022

### Cyber Risk Quantification

Factors used by Firms to assess \$ size of Risks

Factor	Percentage
Business Interruption	90%
Data Breaches	71%
Ransomware demands	65%
Post-incident costs	52%
Regulatory fines	49%

Marsh Microsoft Published June 2022

### Harms from Cyber Attack

5% of firms suffered "Very High Damage" in last year

Damage Level	Percentage
Very High Damage	5%
High Damage	22%
Moderate Damage	31%
Low Damage	41%

Cymulate Survey of 858 senior decision-makers Published June 2022

### Recovery from Cyber Attack

5% of firms needed "Very Long Time" to recover

Recovery Time	Percentage
Very Long Time	5%
Long Time	15%
Moderate Time	43%
Short	38%

Cymulate Survey of 858 senior decision-makers Published June 2022

### 3<sup>rd</sup> Parties Top Cyber Fears

CISOs say 3<sup>rd</sup> Parties give them the greatest concern

Concern	Score
3 <sup>rd</sup> Parties, eg Suppliers	3.89
Unpatched Software	3.88
Cloud Security Gaps	3.73
Configuration Errors	3.72
User Error	3.48
Poor coding or testing	3.43
Weak Authentication	3.24

CISOs CONNECT Survey of 411 CISOs Published June 2022

### Third Party Cyber Risk

52% of business leaders had their suppliers breached

**52%** of our middle market business leaders had a key third-party service provider suffer from a data breach or cyber-attack. Of those, 17 per cent responded that the attack had an impact from a financial or operational perspective

RSM Published June 2022

### Cyber Risk Quantification

Firms recognise weakness in quantifying future risk

Task	Score
Quantify ROI on new initiatives	3.17
Quantify future risk in financial terms	3.11
Quantify total cost of a past incident	3.33

CISOs CONNECT Survey of 411 CISOs Published June 2022

### Cyber Risk Quantification

17% of IT & Security Pros use SecurityScorecard

Tool	Percentage
Risk Recon	3%
FICO	3%
RiskLens	6%
Bitsight	9%
Security Scorecard	17%

Google Survey of 600 IT and Security Pros Published 22<sup>nd</sup> June 2022

# Cyber Insights: Cyber Insurance

Click each image to see each report in full. All were published in month to July 2022

### Cyber Insurance Decisions

12% of firms ask IT or Cyber Leader to make decision

Department	Decision Maker	Part of team	Not involved
Risk Management	25	73	2
Finance	22	75	3
IT & Cyber	12	79	9
CEO & Board	29	64	6

**Marsh Microsoft** Published June 2022

### Cyber Insurance Forecast

Firms expected to spend more on Cyber Insurance

The chart shows projected spending in USD billion from 2016 to 2026. The U.S. segment is represented by a dark blue line, Europe by a light blue line, and the Rest of World (RoW) by a white line.

Year	U.S. (USD billion)	Europe (USD billion)	RoW (USD billion)
2016	2	1	1
2017	3	1.5	1.5
2018	5	2.5	2.5
2019	7	4	4
2020	10	6	6
2021	13	8	8
2022	16	10	10
2023E	19	12	12
2024E	22	14	14
2025E	25	16	16
2026E	28	18	18

**howden** Published June 2022

### Cyber Insurance Demand Up

89% of Insurers & Brokers say Demand still rising

Category	Q4 2021 (%)	Q1 2022 (%)
Employment Practices	42%	29%
Construction Risks	50%	32%
Umbrella	42%	38%
Commercial Property	41%	39%
Cyber	92%	89%

**THE COUNCIL**  
The Council of Insurance Agents & Brokers Published June 2022

### Cyber Insurance Prices Up

72% of Insurers and Brokers say Prices still rising

Category	Q4 2021 (%)	Q1 2022 (%)
Workers Compensation	23%	25%
Employment Practices	40%	28%
Commercial Property	42%	27%
Commercial Auto	43%	37%
Cyber	81%	72%

**THE COUNCIL**  
The Council of Insurance Agents & Brokers Published June 2022

### Cyber Insurance Pricing

Cost of Cyber Insurance is up 185% in two years

The chart shows a sharp upward trend from January 2020 to April 2022, with a callout indicating a 185% increase over two years.

Date	Cost Increase (%)
Jan 20	0
Jan 21	~10
Apr 22	185

**howden** Published June 2022

### Cyber Insurance Coverage

75% of firms pay for Business Interruption Cover

Coverage Type	Percentage
Business Interruption Coverage	75%
3rd Party Liability Coverage	68%
Ransom Coverage	66%

**HITACHI**  
Inspire the Next Online Survey of 620 IT & Cyber Professionals Across N. America & W. Europe Published June 2022

### # Claims on Cyber Insurance

Rate of Growth in Claims is slowing in USA

**Standalone:** claim made on a Policy for Cyber Insurance (only)  
**Packaged:** claim made on a General Policy including Cyber

Year	First-party (LHS)	Third-party (LHS)	First-party (RHS)	Third-party (RHS)
2015	~1,000	~500	~1,500	~500
2016	~1,500	~1,000	~2,000	~1,000
2017	~2,000	~1,500	~2,500	~1,500
2018	~3,000	~2,000	~3,500	~2,000
2019	~4,000	~2,500	~4,500	~2,500
2020	~5,000	~3,000	~5,500	~3,000
2021	~6,000	~3,500	~6,500	~3,500

**howden** Published June 2022

### \$ Claims on Cyber Insurance

Average claim size increased to over USD 100,000

The chart shows two trends: Standalone first-party (solid line) and Standalone third-party (dotted line), and Packaged first-party (solid line) and Packaged third-party (dotted line). The Standalone trends show a significant increase from 2015 to 2019, while the Packaged trends remain relatively flat around USD 100,000.

Year	Standalone first-party (LHS)	Standalone third-party (LHS)	Packaged first-party (RHS)	Packaged third-party (RHS)
2015	~1.5	~0.5	~1.5	~0.5
2016	~1.0	~0.5	~1.0	~0.5
2017	~2.0	~1.0	~1.5	~0.5
2018	~3.0	~1.5	~1.5	~0.5
2019	~4.0	~2.0	~2.0	~0.5
2020	~4.5	~1.5	~2.0	~0.5
2021	~4.0	~1.0	~2.5	~0.5

**howden** Published June 2022

# Cyber Insights: *Phishing & Whaling*

Click each image to see each report in full. All were published in month to July 2022

### Phishing on the Rise

75% annual rise in Phishing Attacks (unique sites)

Date	Unique Sites (approx.)
Apr-21	200,000
May-21	180,000
Jun-21	220,000
Jul-21	250,000
Aug-21	230,000
Sep-21	210,000
Oct-21	240,000
Nov-21	270,000
Dec-21	300,000
Jan-22	320,000
Feb-22	340,000
Mar-22	360,000

### Phishing leads Cyber Entries

56% of cyberattacks enter via a Phishing attack

Attack Type	Percentage
End User Phishing	56%
Third Party connected to the enterprise	37%
Direct attack of enterprise network	34%
Insider threat	29%
IoT Devices	19%
DevOps Depos (Like GitHub etc.)	14%
Hardware-based attacks	14%
Supply chain attack through SaaS	10%

### Sectors Targeted by Phish

23.6% of Phishing attacks are aimed at Finance

Sector	Percentage
Financial	23.6%
SAAS / Webmail	20.5%
eCommerce / Retail	14.6%
Social Media	12.5%
Crypto	6.6%

### Execs Impersonated in Phish

71% of impersonations pretend to be from Execs

Role	Percentage
Executive	71%
Employee	29%

### Execs attacked by Phish

VPs receive 51% of all impersonation attacks

Role	Percentage
VPs	51%
C-Suite	20%
Chief Engineers	16%
Other	13%

### Cyber Threats to Executives

27% of Execs have Malware on their devices

Threat	Percentage
Malware	27%
Leaking Data	76%
No Security Installed	87%

### Business Email Compromise

Language (ie just words) is how most BEC works

Method	Percentage
Language Based	74%
Graymail	15%
Business Workflows	7%
Malicious Payload	4%

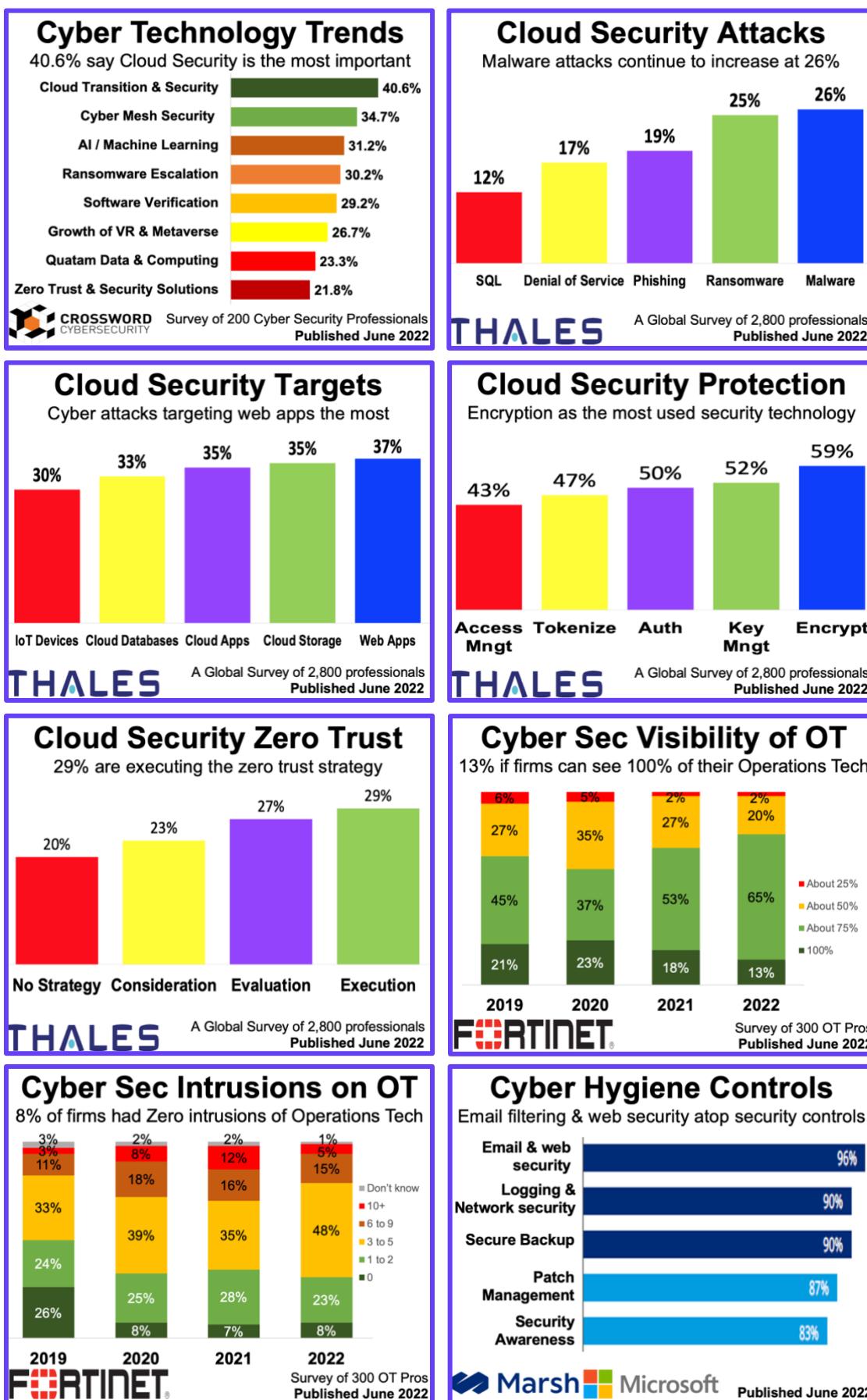
### Attacks Impersonate Vendors

52% of Business Email Compromise "from" Vendors

Date	Fraudster impersonates your Colleagues (%)	Fraudster impersonates your Vendors (%)
Jan '21	60	40
Feb '21	55	45
Mar '21	60	40
Apr '21	58	42
May '21	62	38
Jun '21	55	35
Jul '21	60	30
Aug '21	58	32
Sep '21	62	35
Oct '21	55	38
Nov '21	58	40
Dec '21	60	42
Jan '22	55	45
Feb '22	58	48
Mar '22	60	50
Apr '22	55	48

# Cyber Insights: Cyber on Cloud and OT

Click each image to see each report in full. All were published in month to July 2022



# Cyber Insights: CISO fears

Click each image to see each report in full. All were published in month to July 2022

### Cyber Threat Landscape

67% of Chief Information Security Officers: "Worse"

Perception	Percentage
SIGNIFICANTLY BETTER	2%
SOMEWHAT BETTER	12%
ABOUT THE SAME	19%
SOMEWHAT WORSE	49%
SIGNIFICANTLY WORSE	18%

### Material Harms from Cyber

75% of firms suffered "material harm" this year

Harm Level	Percentage
NONE	4%
ONCE	18%
2 TO 5 TIMES	48%
MORE THAN 5 TIMES	21%
CONFIDENTIAL / CAN'T RESPOND	9%

### Cyber Strategy Relevance

40.1% say Cyber Strategy is relevant for 1-2 years

Relevance Duration	Percentage
1-2 Years	40.1%
2-3 Years	37.1%
3-4 Years	14.4%
4-5 Years	4.5%
Out of Date	2.5%

### Cyber Security Challenges

18.3% say Supply Chain risk is "very challenging"

Challenge	Percentage
Supply Chain Management	18.3%
Restoring Impaired Services	15.3%
Identifying Cyber Threat	14.9%
Responding to Cyber Attack	13.9%
Develop Cyber Skills	11.4%

### Cyber External Threats

Supply chain attacks considered #1 risk by experts

Threat Type	Percentage
Zero Day Attacks	6%
Phishing	7%
Fileless Attacks	9%
Ransomware	13%
Supply Chain Attacks	14%

### Top Trends in Cybersecurity

Attack Surface Expansion vital due to remote work

- #1 = Attack Surface Expansion
- #2 = Identity System Defense
- #3 = Digital Supply Chain Risk
- #4 = Vendor Consolidation
- #5 = Cybersecurity Mesh

### Able to block Cyber Attack?

12% Execs highly confident they can block attacks

Confidence Level	Executive leaders (%)	Departmental leaders (%)
Highly confident	12%	17%
Fairly confident	64%	69%
Not confident	24%	14%

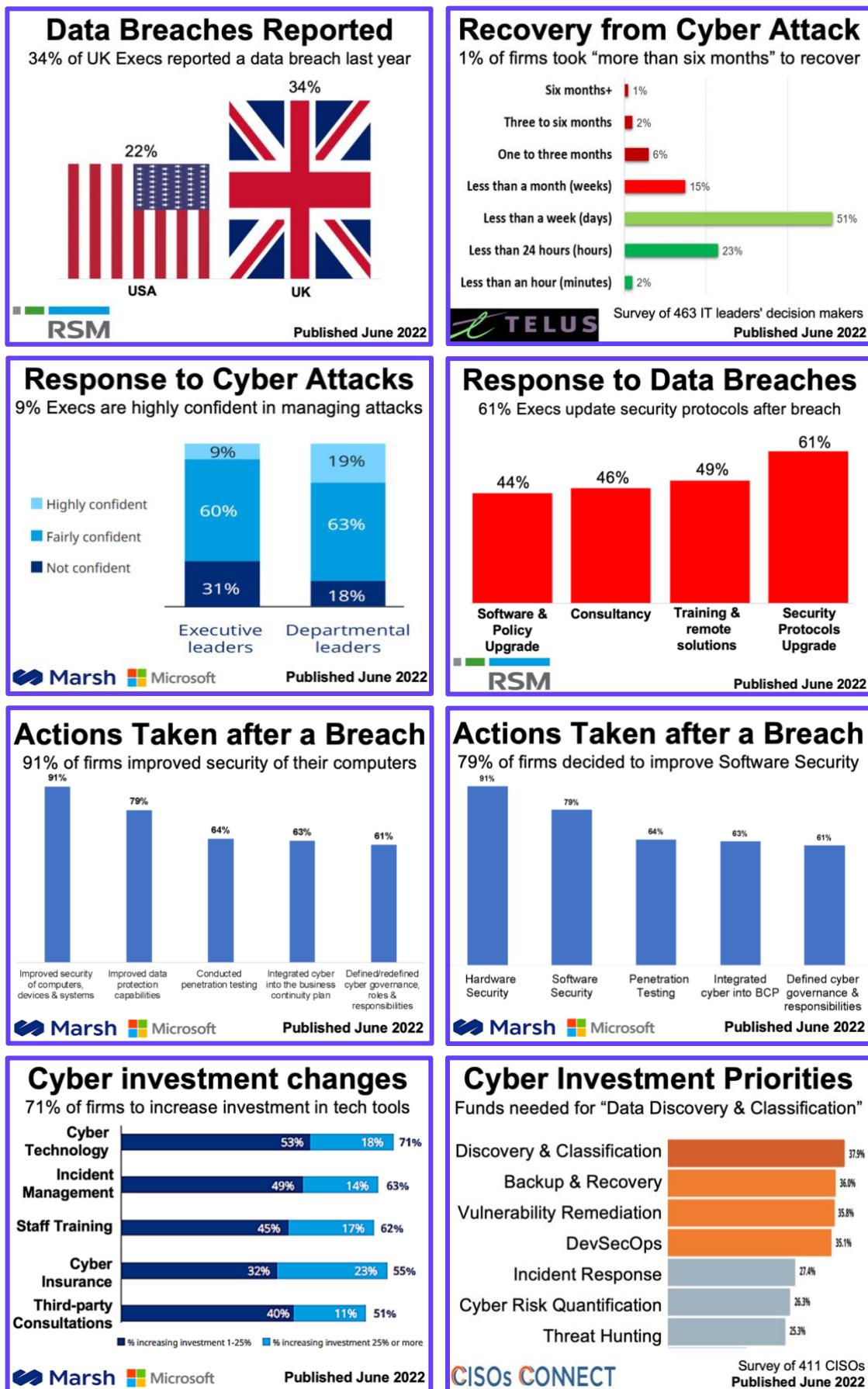
### Turning Off Cyber Alerts

1 in 4 respondents turn off alerts due to noise

Reason	Percentage
Turn off alerts due to noise	26%
Other	74%

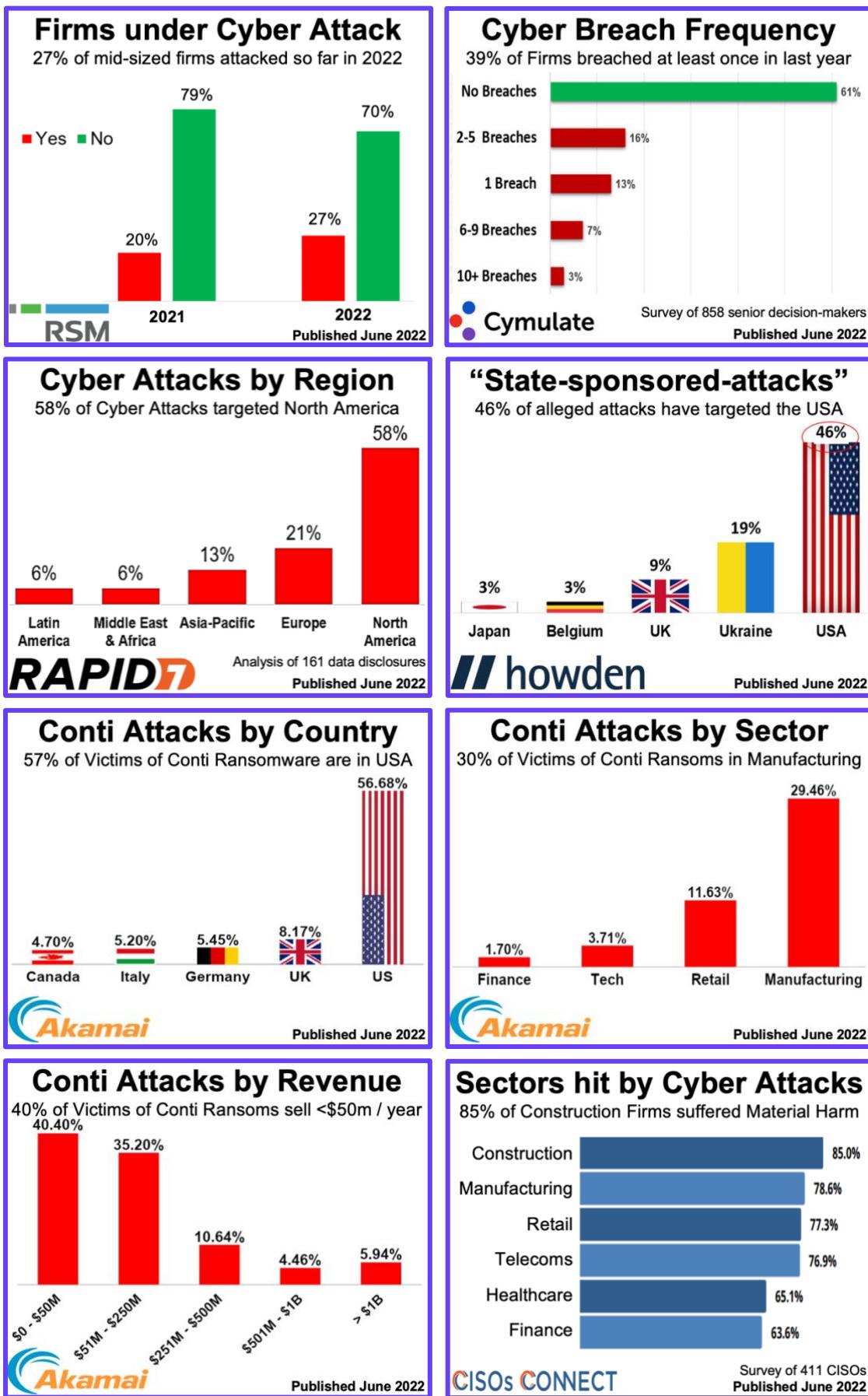
# Cyber Insights: After a Breach

Click each image to see each report in full. All were published in month to July 2022



# Cyber Insights: Cyber Attack Trends

Click each image to see each report in full. All were published in month to July 2022



# Cyber Insights: Executives and Cyber

Click each image to see each report in full. All were published in month to July 2022

### Cyber Risk Awareness

66% of Boards said to be fully aware of Cyber Risks

Awareness Level	Percentage
Yes	66%
No	34%

**RSM**

Published June 2022

### Cyber Risk Assessments

23% Execs are confident in assessing cyber threats

Confidence Level	Executive leaders (%)	Departmental leaders (%)
Highly confident	23%	26%
Fairly confident	53%	61%
Not confident	24%	13%

**Marsh Microsoft**

Published June 2022

### Measure Cyber Threats well

16% of Execs "Highly Confident" in measurements

Confidence Level	Executive leaders (%)	Departmental leaders (%)
Highly confident	16%	20%
Fairly confident	57%	63%
Not confident	27%	17%

**Marsh Microsoft**

Published June 2022

### Cyber C-Suite Pressures

Most stress causes from securing remote workforce

Pressure Source	Percentage
Insufficient Resources	26%
Zero Day Attacks	30%
Hiring Challenges	35%
Ransomware Threats	48%
Securing Remote Workforce	52%

**deepinstinct**

1,000 Cyber Experts in USA + Europe  
Published June 2022

### MSPs not trusted on Cyber

37% of firms worry over Managed Service Provider

Response	Percentage
Strongly disagree	4%
Disagree	16,20%
Neutral	42,60%
Agree	32,10%
Strongly agree	5,10%

**jumpcloud™**

Published June 2022

### Reasons for Cyber Insurance

63% say Insurance is key to Cyber Strategy

Reason	Percentage
Key part of cyber strategy	63%
Worth paying for	58%
Industry best practice	34%
To cover cyber incident costs	29%
Consultant recommended	28%

**Marsh Microsoft**

Published June 2022

### Ransom Attack Payments

56% of Victim Firms admit paying ransom for data

Response	Percentage
Yes	56%
No	42%
Abstain	1%
Don't Know	1%

**HITACHI**  
Inspire the Next

Online Survey of 620 IT & Cyber Professionals Across N. America & W. Europe  
Published June 2022

### Attempted Ransom Attacks

Sporadic Ransom Attacks the highest at 32%

Attack Type	Percentage
Yes, Daily	13%
Yes, Weekly	17%
Yes, Monthly	17%
Yes, Sporadic (>month)	32%
No, Past year	21%

**HITACHI**  
Inspire the Next

Online Survey of 620 IT & Cyber Professionals Across N. America & W. Europe  
Published June 2022

# Cyber Insights: Cyber Developments

Click each image to see each report in full. All were published in month to July 2022

### Cyber Attack Prevention

Firms with MFA & Phishing Tests are breached least

Practice	Top Practices (%)	Number of Breaches (Avg)
Multi-Factor Authentication	67%	1.0
Phishing Awareness	53%	1.0
Incident Response Plans	44%	1.1
Least Privileges	43%	0.9
Application Security	20%	1.3
Moving to Cloud	15%	2.1
Hiring MSSP	10%	1.9

**Cymulate** Survey of 858 senior decision-makers Published June 2022

### Value of Penetration Testing

Firms with 3rd Party Pen Tests breached less often

Approach	Top Practices (%)	Number of Breaches (Avg)
3rd Party Pen Testing	62%	3.7
In-house Pen Testing	59%	3.8
Attack Surface Management	53%	3.9
Breach Attack Simulation	48%	4.2
Purple Teaming	34%	3.9
Continuous Automated Red Teaming	33%	4.3

**Cymulate** Survey of 858 senior decision-makers Published June 2022

### Cyber Risk Quantification

18% of firms have no method to gauge cyber risks

Method	Percentage
Systematically, via stages or implementation tiers within the NIST framework	29%
Visually or categorically, with colors or levels	28%
Financially, based on estimated potential losses of a cyberattack within a specific timeframe (value-at-risk modeling)	26%
Quantitatively, via numerical scores or rankings	22%
We have no method to measure cyber risk	18%

**Marsh Microsoft** Published June 2022

### Prevent & Mitigate Ransomware

55% of firms use Endpoint Detection & Response

Strategy	Percentage
Endpoint Detection & Response	55%
Data Protection	54%
Security Info & Event Management	54%
Extended Detection & Response	37%
Incident response firm	14%

**HITACHI** Online Survey of 620 IT & Cyber Professionals Across N. America & W. Europe Published June 2022

### Leveraging Cyber Insurance

62% of UK firms carry cyber insurance policy

Country	Percentage
USA	61%
UK	62%

**RSM** Published June 2022

### Insurance & Cyber Warfare

Insured firms can now choose 4 alternative options

	Clause 1 (LMA 5564)	Clause 2 (LMA 5565)	Clause 3 (LMA 5566)	Clause 4 (LMA 5567)
1	YES	NO	NO	NO
2	N/A	YES	YES	YES
3	N/A	YES	YES	YES
4	N/A	NO	YES	YES
5	N/A	NO	NO	YES

**howden** Published June 2022

### Financial Fraud on Firms

25% of fraud is from breached Vendor accounts

Type	Percentage
Payroll	44%
Payment	31%
Vendor	25%

**Armorblox** Published June 2022

### The Ransomware Ecosystem

Published June 2022

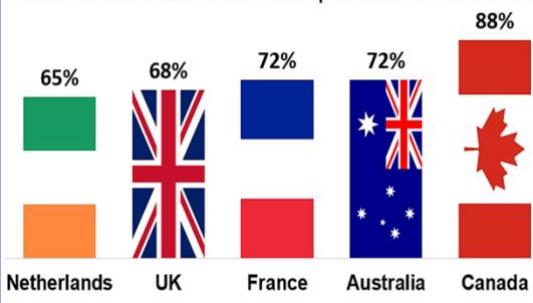
**Otenable** Published June 2022

# The Best Cyber Insights of 2022

Click each image to see each report in full. All published in month to June 2022

## Cyber Insurance Purchased

88% of Canadian firms have purchased Insurance



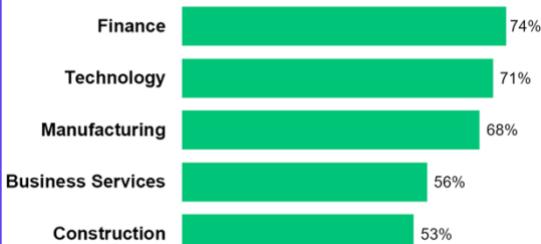
Survey of 1,400 Chief Information Security Officers

[proofpoint](#)

Published May 2022

## Cyber Insurance Purchased

74% of Finance firms now have Cyber Insurance

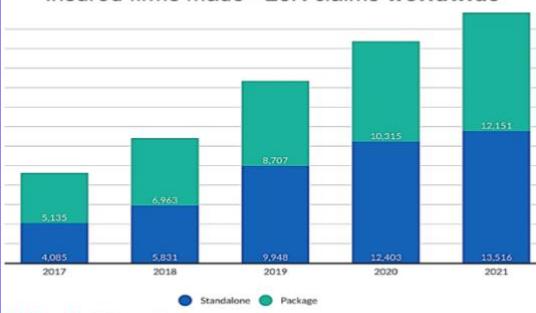


HISCOX

Published May 2022

## # of Cyber Insurance Claims

Insured firms made >25K claims worldwide

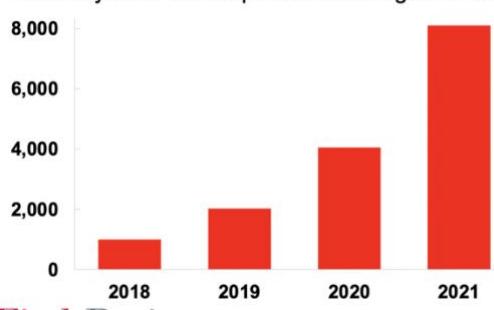


[FitchRatings](#)

Published May 2022

## # of Cyber Insurance Claims

Fitch says # of claims paid doubled again in USA

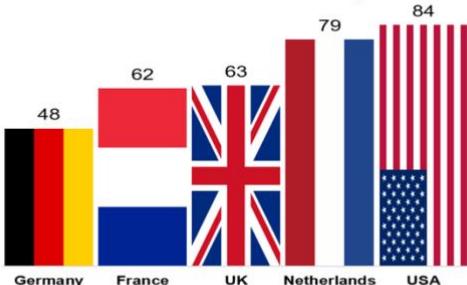


[FitchRatings](#)

Published May 2022

## Payment of Cyber Ransoms

84% of USA Victims of Ransomware paid Ransom

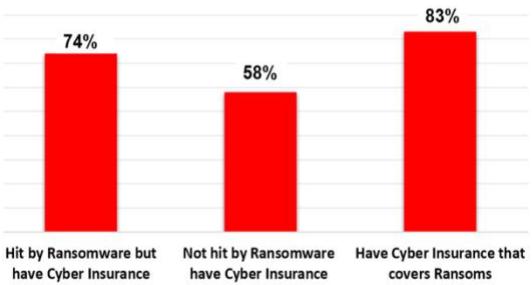


HISCOX

Published May 2022

## Cyber Insurance for Ransom

About 83% say their insurance covers ransom

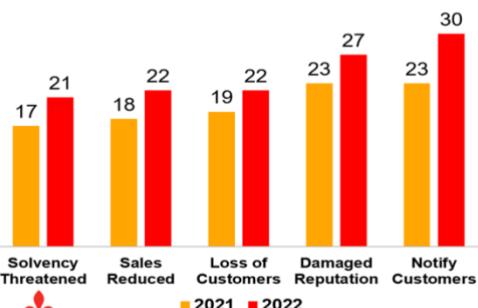


SOPHOS

Published May 2022

## Impacts of Cyber Attacks

22% of firms claiming on Insurance say lost clients

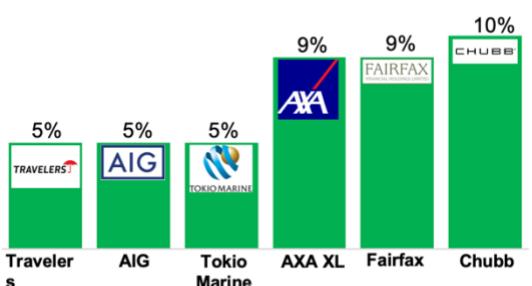


HISCOX

Published May 2022

## Cyber Insurance Underwriter

43% of Cyber Insurance underwritten by 6 firms



[FitchRatings](#)

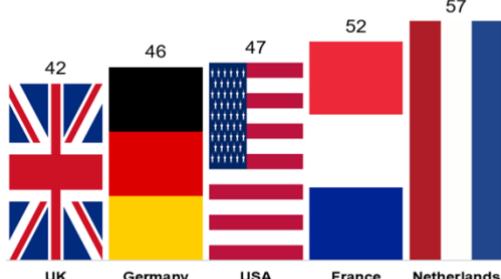
Published May 2022

# Cyber Insights: Ransomware

Click each image to see each report in full. All were published in month to June 2022

## Frequency of Cyber Attacks

57% Dutch firms have reported an attack to insurer

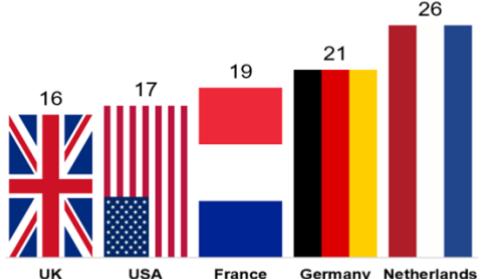


HISCOX

Published May 2022

## Frequency of Cyber Ransom

26% of Dutch firms had a Ransom attack this year



HISCOX

Published May 2022

## Ransom Demand vs Paid

Finance Sector victims pay most, average of \$2.6m



Arete

Published May 2022

## Average Ransom Payout

Size of each known payment +63% from Q3 in 2021

Average known  
Payout =



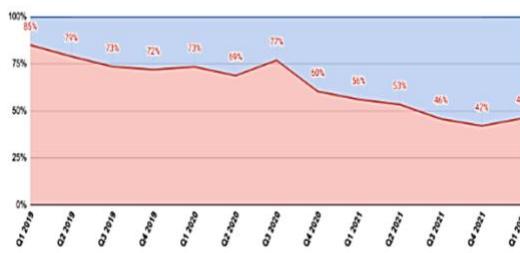
**USD \$322k**

BLACKFOG

Published May 2022

## Ransom Refusals Rising

Good News: 54% now refuse to pay, up from 15%

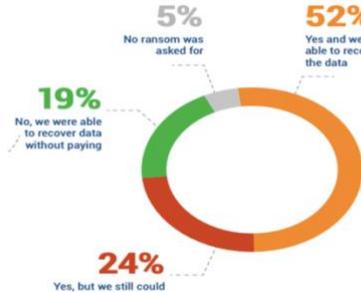


COVWARE

Published May 2022

## Payment of Ransom for Data

24% of firms unable to recover data after payout



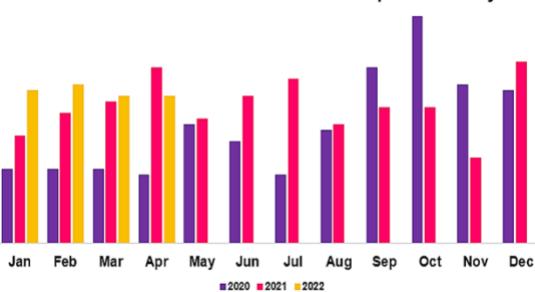
veeAM

Published May 2022

Survey of 1,000 IT leaders

## Successful Ransom Attacks

Good news: fewer "successes" in April vs last year

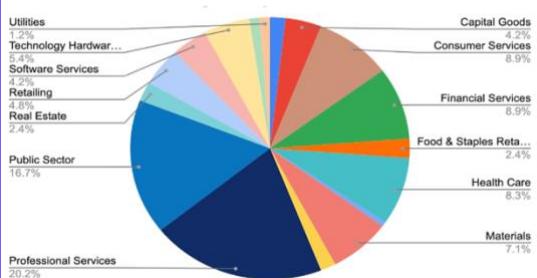


BLACKFOG

Published May 2022

## Target Industries of Ransom

Professional Services firms hit most frequently



COVWARE

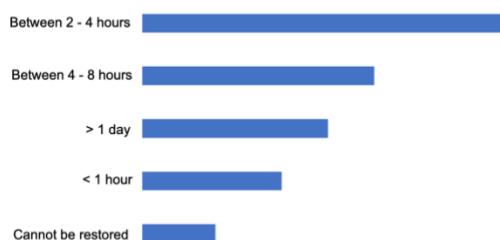
Published May 2022

# Cyber Insights: How to Recover from Ransom

Click each image to see each report in full. All were published in month to June 2022

## Data Recovery after Ransom

55% of firms restore data in <5 hours after attack

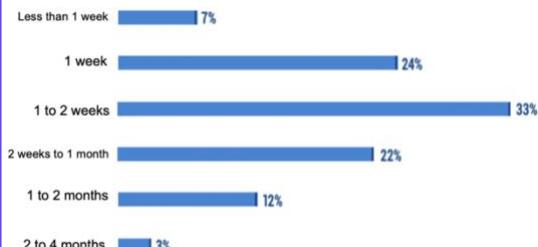


veeAM

Published May 2022  
Survey of 1,000 IT leaders

## Full Recovery after Ransom

70% of firms need > 1 week to fully recover

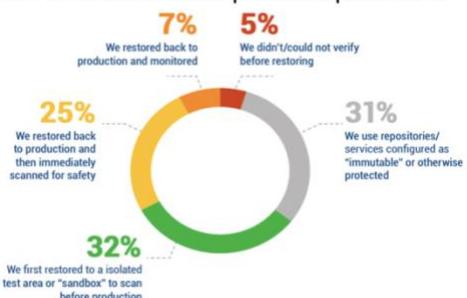


veeAM

Published May 2022  
Survey of 1,000 IT leaders

## Check Backup after Ransom

32% of firms tested backups before production

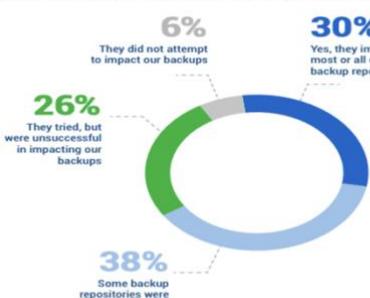


veeAM

Published May 2022  
Survey of 1,000 IT leaders

## Backups hit by Ransomware

68% of Ransom Victims had their backup impacted

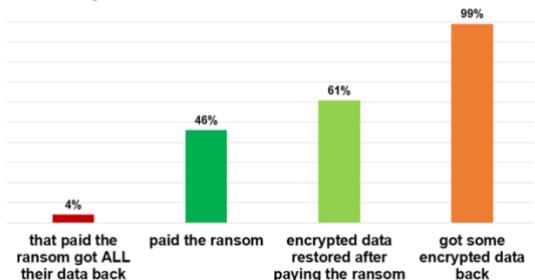


veeAM

Published May 2022  
Survey of 1,000 IT leaders

## Restored Data after Ransom

99% say retrieved SOME data after ransom attack

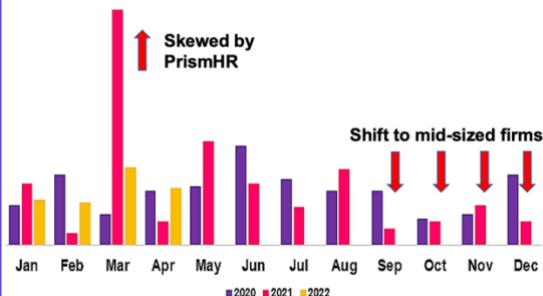


SOPHOS

Published May 2022

## Size of Firms hit by Ransom

Hackers continue to focus on mid-sized firms

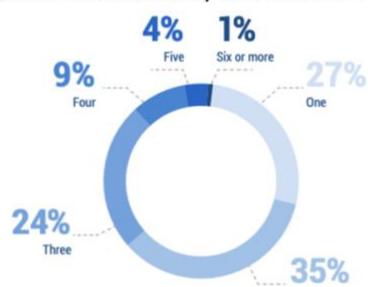


BLACKFOG  
Privacy. Security. Prevention.

Published May 2022

## Ransom Attack Frequency

73% of firms attacked by ransomware >1 / year

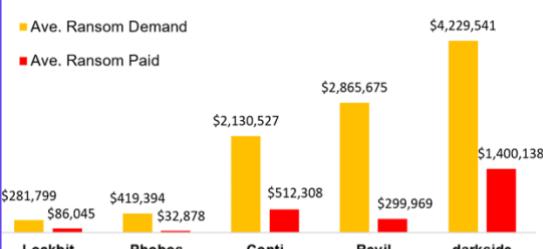


veeAM

Published May 2022  
Survey of 1,000 IT leaders

## Ransom Demand vs Paid

Most gangs accept payment of < 50% of Demand

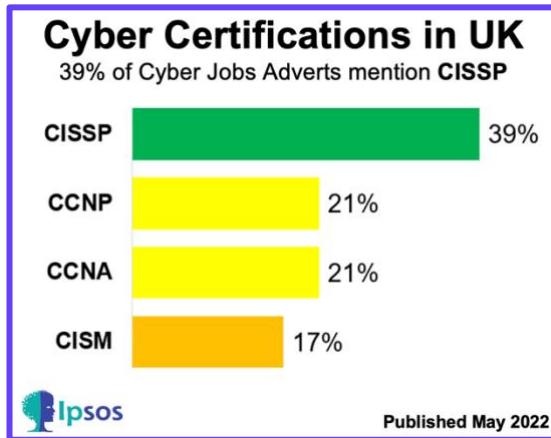
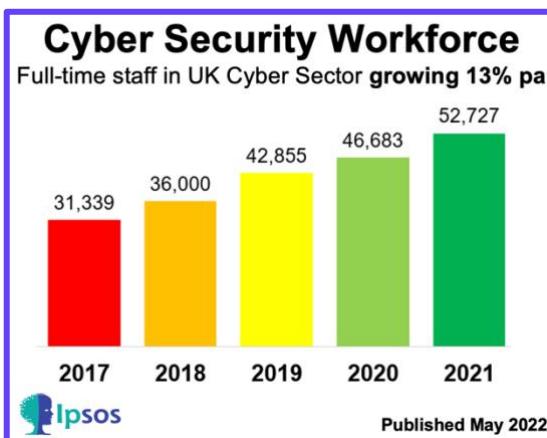


Arete

Published May 2022

# Cyber Insights: Jobs & Salaries in Cyber

Click each image to see each report in full. All were published in month to June 2022

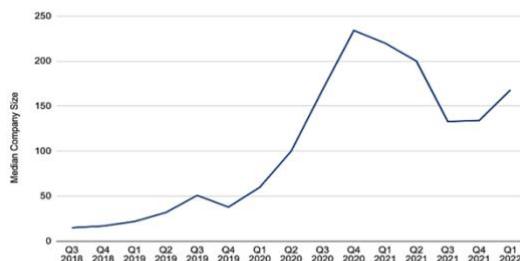


# Cyber Insights: Defence against Ransomware

Click each image to see each report in full. All were published in month to June 2022

## Size of Firms hit by Ransom

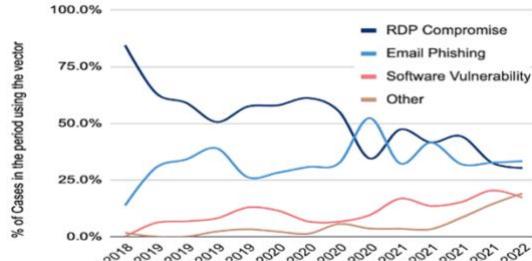
Typical Firm hit by Ransom now has about 170 staff



Published May 2022

## How Firms hit by Ransom

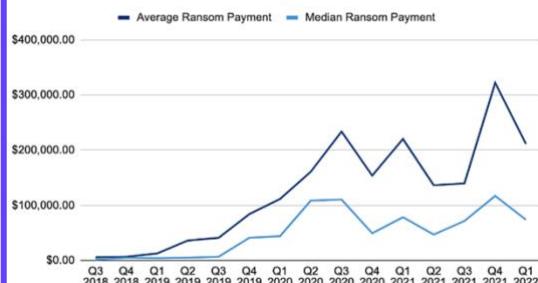
Email Phishing is now the top attack vector



Published May 2022

## Typical Ransom Payments

Median Ransom actually Paid is about \$80,000



Published May 2022

## Top Ransomware Variants

Conti is still the most common ransomware variant

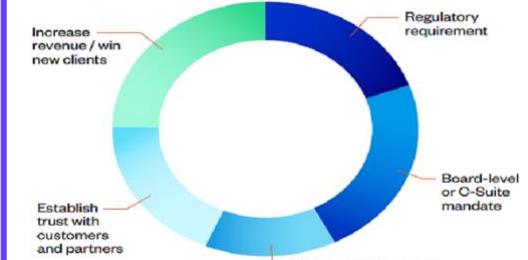
Rank	Ransomware Type	Market Share %
1	Conti V2	16.1%
2	LockBit 2.0	14.9%
3	BlackCat	7.1%
4	Hive	5.4%
5	AvosLocker	4.8%
6	Karakurt	4.1%



Published May 2022

## Cyber Security Compliance

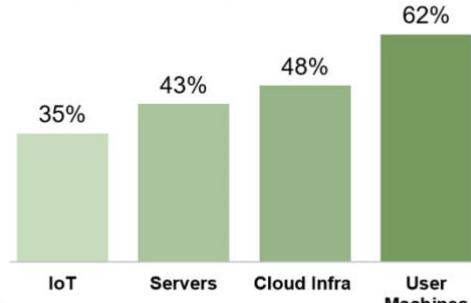
Firms agree compliance will result in higher revenue



Survey of 700 IT Professionals  
Published May 2022

## Cyber Security Controls

Security control mostly found in User machines



Published May 2022

## Effective Ransom Defense

Multifactor Authentication tops the chart at 50%



Published May 2022

## Top Investments for Security

Investments made by Firms with No Breaches

- #1 = Email Security, eg MFA
- #2 = Protect against Denial of Service
- #3 = Cloud Access Security Broker
- #4 = Network Security Policy Mgmt
- #5 = Identity & Access Mgmt



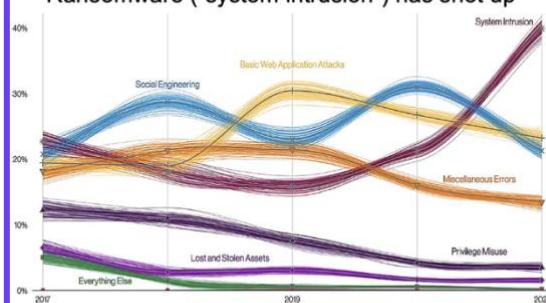
Survey of 1,200 Global Firms  
Published May 2022

# Cyber Insights: Ransomware Statistics

Click each image to see each report in full. All were published in month to June 2022

## How Breaches are Changing

Ransomware ("system intrusion") has shot up

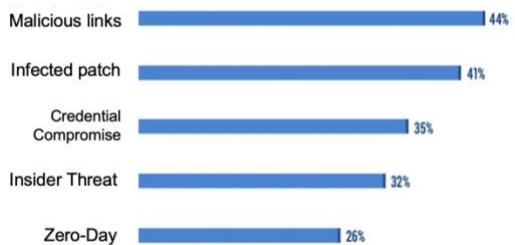


**verizon**

Published May 2022

## How Ransomware gets in

Phishing ranks as a top entry point for ransomware

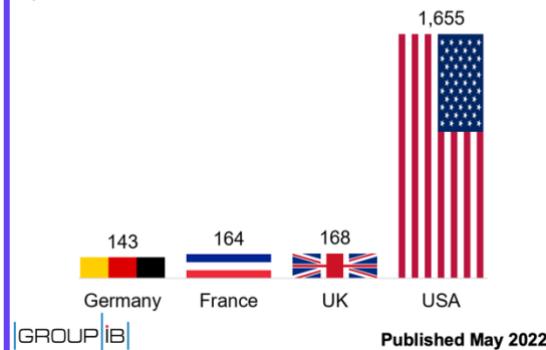


**veeam**

Published May 2022

## Ransomware Victims

1,655 victims of ransomware from the USA in 2021

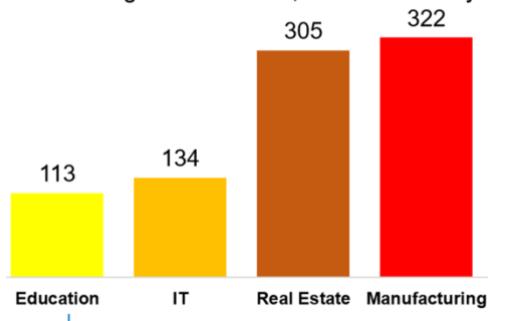


**GROUP iB**

Published May 2022

## Ransomware Victims

'Manufacturing' now has most, with 322 in last year

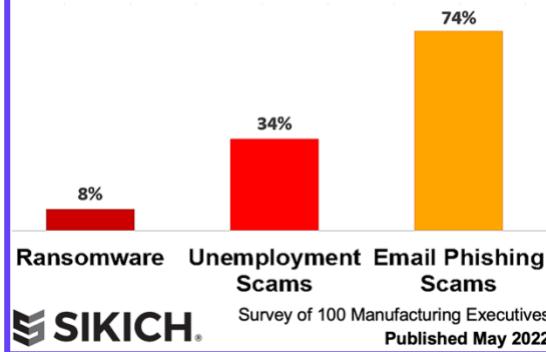


**GROUP iB**

Published May 2022

## Cyber Incidents in Factories

74% of Manufacturing Execs hit by Phish this year

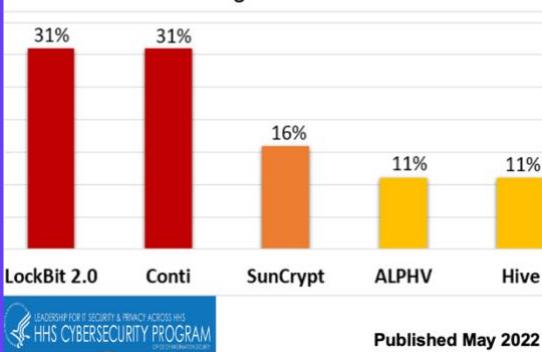


**SIKICH.**

Survey of 100 Manufacturing Executives  
Published May 2022

## Ransomoms in Health Sector

LockBit & Conti Gangs attack Health Sector most

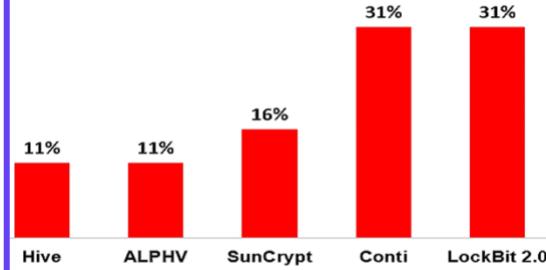


**LEADERSHIP FOR SECURITY & PRIVACY ACCESS HHS CYBERSECURITY PROGRAM**

Published May 2022

## Top Ransomware Groups

Attacks on the Healthcare & Public Health Sector

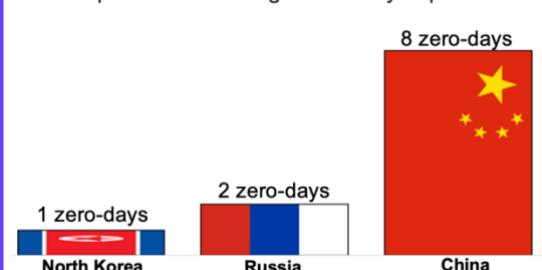


**U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES**

Published May 2022

## Zero-Days used by Country

China tops the list with eight zero-day exploits used

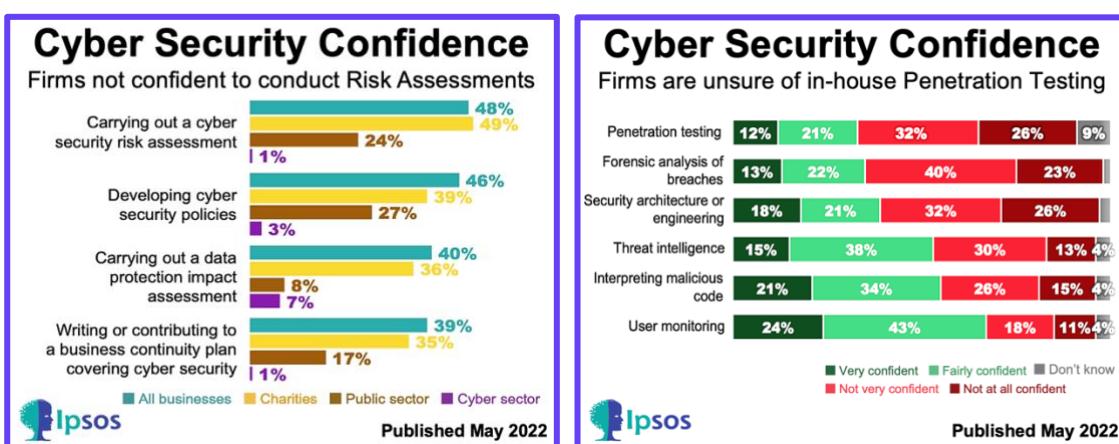
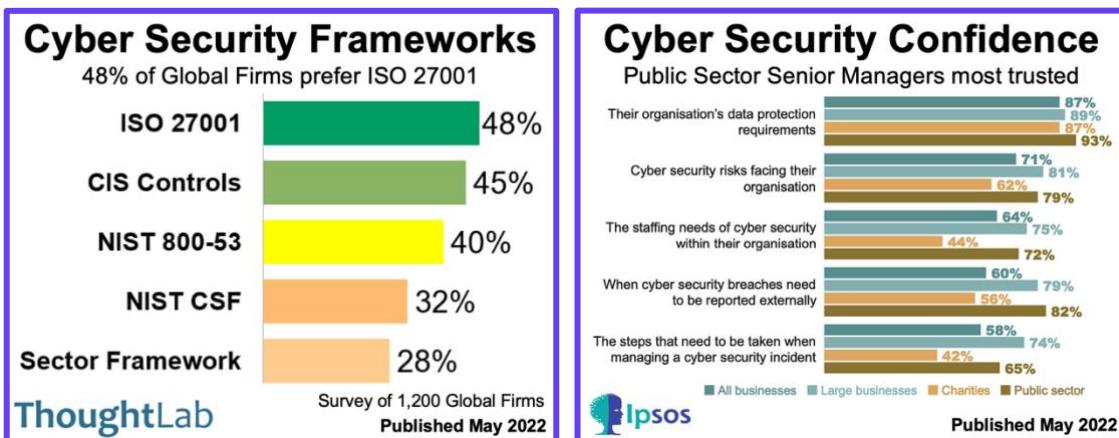
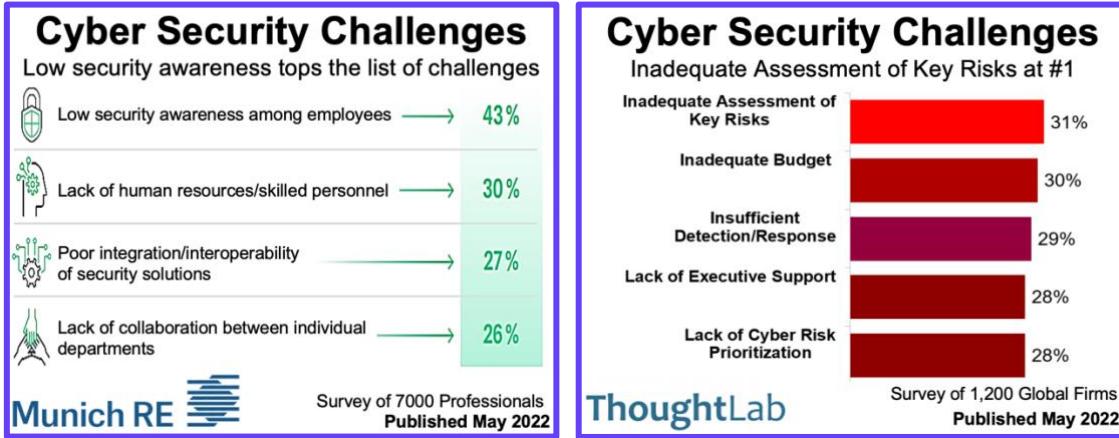
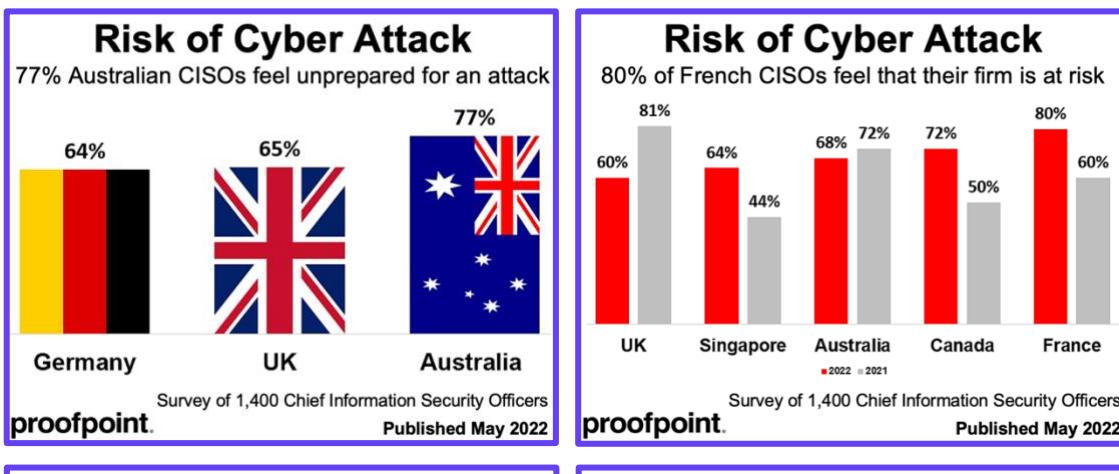


**MANDIANT**

Published May 2022

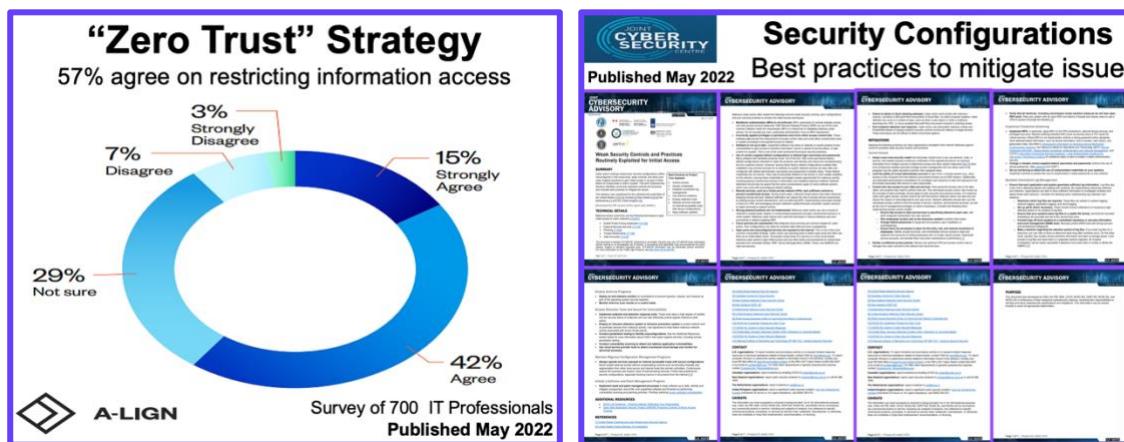
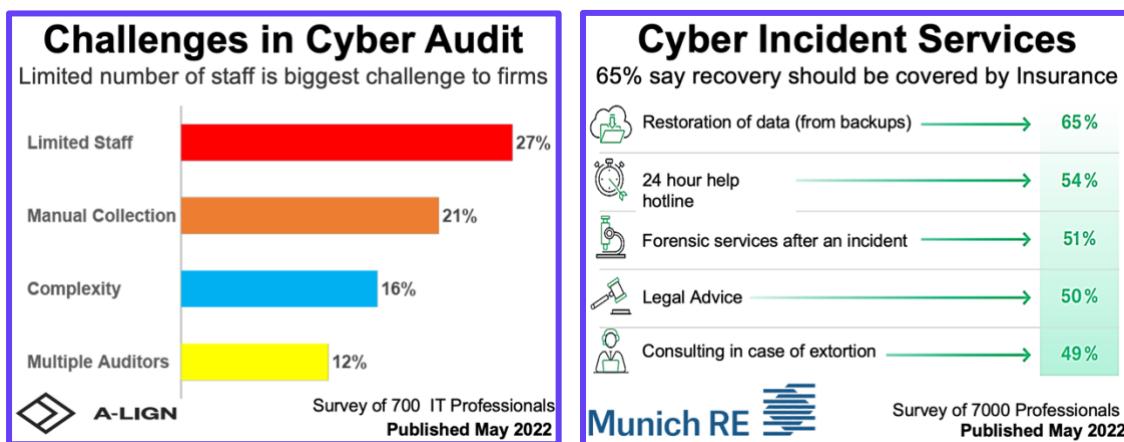
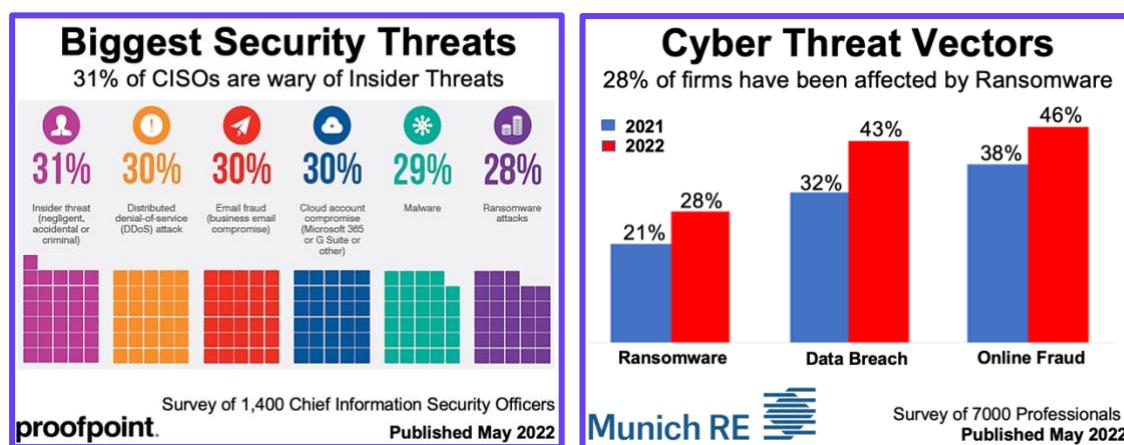
# Cyber Insights: Cyber Risk & Confidence

Click each image to see each report in full. All were published in month to June 2022



# Cyber Insights: Threats & Strategies

Click each image to see each report in full. All were published in month to June 2022



# Cyber Insights: *Malware & Phishing*

Click each image to see each report in full. All were published in month to June 2022

### Top Malware File Types

EXE/DLL files represent the plurality of downloads

File Type	Percentage
EXE/DLL	46%
ZIP	16%
PDF	2%
Office	9%
Others	19%

netskope Published May 2022

### Top Malware Categories

Trojan tops at 77%

Category	Percentage
Trojan	77%
Phishing	10%
Exploit	2%
Rootkit	2%
Downloader	2%
Others	7%

netskope Published May 2022

### Top Malware Downloads

Technology sites lead referrers

Referrer	Percentage
Technology	27%
Search Engines	15%
News & Media	11%
Video Sites	11%
Shareware Sites	8%

netskope Published May 2022

### PCs infected by Malware

25% of Manufacturers have at least 1 infected PC

Industry	Percentage
Manufacturing	Highest
Education	Second Highest
Transport	Third Highest
Agriculture	Fourth Highest
Finance	Lowest

BrightCloud Threat Intelligence Published May 2022

### Malware Trends

Published May 2022

netskope Published May 2022

### Staging of Phishing Sites

35% use compromised sites to stage phishing

Staging Method	Percentage
Compromised Sites	35.1% (+3.3%)
Paid Domain Registrations	16.7% (+3.2%)
Free Hosting	18.3% (+2.4%)
Tunnelling Services	15.1% (+0.8%)
URL Shorteners	7.7% (+2.4%)
Developer Tools	1.3% (-)

PHISHLABS by HelpSystems Published May 2022

### Threats in Social Media

Nearly 50% of threat involves impersonation

Threat Type	Percentage
Impersonation	46.8% (+0.7%)
Fraud	28.3% (+1%)
Cyber Threat	25.6% (+3.9%)
Data Leak	1.8% (+1.8%)
Physical Threat	0.4% (+0.1%)

PHISHLABS by HelpSystems Published May 2022

### Breached Passwords

Published May 2022 Many come from popular media

TechRepublic Published May 2022

# Cyber Insights: *Maturity of Response*

Click each image to see each report in full. All were published in month to June 2022

**Cyber Maturity Model**

Increase Maturity to reduce Probability of a breach

The dashed red line represents breach likelihood and relative cost remediation  
The solid blue line represents awareness/culture maturity gains at each stage of the model

**Cyber Maturity Model**

Education still has lowest score on cyber maturity

Industry	2019	2020	2021
Consulting	~78	~78	~75
Education	~70	~70	~70
Healthcare & Pharmaceuticals	~72	~74	~74
Legal	~70	~72	~72
Technology	~76	~75	~75

**Cyber Maturity Model**

Published May 2022

**KnowBe4**  
Human error. Conquered.

**Cyber Maturity Model**

Published May 2022

**KnowBe4**  
Human error. Conquered.

**CROWDSTRIKE** How Cybercriminals Monetize Ransomware Attacks

Published May 2022

**APRICORN** Global IT Security Annual Survey 2022

Published May 2022

**SpyCloud** Fortune 1000 Identity Exposure Report

Published May 2022

**Remote Work Vulnerability**

87% of Canadian CISOs report more attacks

Region	2022 (%)	2021 (%)
Germany	55%	64%
UK	56%	60%
France	61%	56%
Australia	66%	45%
Canada	87%	63%

Survey of 1,400 Chief Information Security Officers  
**proofpoint.** Published May 2022

**Cyber Security Readiness**

% of firms unprepared for changing threat landscape

Industry	Percentage
Healthcare	35%
Public Sector	34%
Telecoms	31%
Life Sciences	31%
Insurance	31%

Survey of 1,200 Global Firms  
**ThoughtLab** Published May 2022

**Cyber Maturity by Sector**

Comparison of Industries

Sector	Percentage
Education	70%
Construction	71%
Health	74%
Banking	76%
Insurance	76%

**KnowBe4**  
Human error. Conquered. Published May 2022

# Cyber Insights: Attack Trends

Click each image to see each report in full. All were published in month to June 2022

### PCs infected by Malware

1.6% of PCs now infected in UK, down from 3.7%

**BrightCloud Threat Intelligence**

Published May 2022

### Account Takeover Attacks

Financial Services attacked most in 2021

Sector	Percentage
Financial Services	34.6%
Travel	23.2%
Business Services	11.4%
Retail	8.1%
Entertainment & the Arts	6.0%
Telecom and ISPs	5.0%
Law & Government	2.8%
Gaming & Gambling	2.8%
Computing & IT	2.6%
Food & Beverage	2.5%
Sports	.9%
Education	.1%

**imperva**

Published May 2022

### Advanced Bot Attacks

Travel & Retail firms most targeted

Sector	Percentage
Travel	34.2%
Retail	33.8%
Financial Services	8.8%
Business Services	6.4%
Computing & IT	4.5%
Automotive	2.9%
Gaming & Gambling	2.8%
Healthcare	1.4%
Food & Beverage	1.2%
Society	1.1%
Education	0.7%
Law & Government	0.7%
Telecom & ISPs	0.6%
Sports	0.3%
Entertainment & Arts	0.3%
News	0.2%

**imperva**

Published May 2022

### Ransomware Trends

Health Sector

**HHS CYBERSECURITY PROGRAM**

Published May 2022

### How Breaches happen

10% still due to human error, 70% via web hacking

Cause	Percentage
Carelessness (Error)	10%
Software Update (Malware)	18%
Partner (Malware)	18%
Email (Social & Malware)	18%
Web Application (Hacking)	70%

Survey of 1,400 Chief Information Security Officers

**verizon**

Published May 2022

### Ransomware Vulnerabilities

Trending vulnerabilities surged by 6.8% in Q1 2022

Vulnerability count tied to ransomware

7.6

Trending vulnerabilities

6.8

**CSW Cyber SecurityWorks**

Published May 2022

### Ransomware Vulnerabilities

3.5% decline in vulnerabilities missed by scanners

Ransomware vulnerabilities missed by scanners

3.5%

CISA KEVs with ransomware associations missed by scanners

1.5%

**CSW Cyber SecurityWorks**

Published May 2022

### “Five Eyes” alert to MSPs

New Cyber Threats to Managed Service Providers

New warning from Governments of Australia, Canada, NZ, UK & USA

Published 11<sup>th</sup> May 2022

*Credit: Dreamstime*

# Cyber Insights: Further Reports & Insights

Click each image to see each report in full. All were published in month to June 2022

### 43 Ransomware Gangs by Main Country of Origin

Country	Count
APT Groups For Hire	14
Russia	11
China	8
Iran	3
US	2
North Korea	2
Germany	1
Ukraine	1
Nigeria	1

Published May 2022

**ivanti CSW Cyber SecurityWorks**

### Access Credentials for Sale

\$64K USD, the highest price for access credentials

Sector	Lowest Asking Price	Highest Asking Price
Legal	\$1,000	\$15,000
Finance	\$100	\$20,000
Education	\$350	\$25,000
Government	\$300	\$26,000
Industrial	\$200	\$64,000

Survey of 100 Manufacturing Executives

Published May 2022

**CROWDSTRIKE**

### Known Exploited Vulnerabilities

0.1% of all Vulnerabilities are "Known Exploited"

Category	Count
Total NVD Vulnerabilities	142,133
Weaponized Vulnerabilities	10,463
Vulnerabilities with Dangerous Capabilities	3,312
Vulnerabilities Tied to Ransomware	310
Vulnerabilities Trending with Active Exploits	157
CISA KEVs	141

Published May 2022

**ivanti CSW Cyber SecurityWorks**

### TALOS Cyber Threat Insights on Ransomware Operations

Published May 2022

### edpb Calculating GDPR Fines New Guide for Regulators

Published May 2022

### Deloitte Reimagining OT Cybersecurity Strategy 2022

Published May 2022

### Ipsos Cyber Skills in UK

Published May 2022

### Breaches "detected" faster

75% now detected fast (as hacker wants payment)

verizon

Published May 2022

# Best Cyber Insights of 2022

Click each image to see each report in full. All were published in month to May 2022

### Cyber Insurance Ransom

42% of UK firms say their insurance covers ransom

Country	Percentage
Turkey	32%
Saudi Arabia	36%
UK	42%
USA	50%
Austria	66%

**SOPHOS**

Survey of 5,600 firms  
Published April 2022

### Cyber Insurance Prices: x2

Price of Insurance rising at 110% per year in USA

Region	Annual Increase (%)
S. America	35%
EU	80%
UK	102%
USA	110%

**Marsh**

Global Insurance Market Index  
Published 27th April 2022

### Successful Ransom Attacks

74% of professionals experienced successful attack

Experience	Percentage
No	26%
Once	41%
Yes, More than once	32%

**Zerto**

Survey of 620 IT & Cyber professionals  
Published April 2022

### Insurance Paying Ransoms

Insurer paid Ransom for 30% of Manufacturers

Industry	Percentage
Lower Education	53%
Government	46%
Business Services	40%
Finance	32%
Manufacturing	30%

**SOPHOS**

Survey of 5,600 firms  
Published April 2022

### Average Ransom Payout

Size of each known payment +63% from Q3 in 2021

Average known Payout = **USD \$168k**

**BLACKFOG**  
Privacy. Security. Prevention.

Published April 2022

### Data Recovery after Ransom

14% of firms recovered all their data after paying

Recovery Percentage	Percentage
25% or less recovered	3%
26%-50% recovered	16%
51%-75% recovered	42%
76%-99% recovered	26%
100% recovered	14%

**Zerto**

Survey of 620 IT & Cyber professionals  
Published April 2022

### Successful Ransom Attacks

Numbers are up in the first 3 months of 2022

Month	2020	2021	2022
Jan	10	12	18
Feb	10	15	20
Mar	10	18	22
Apr	10	22	25
May	15	15	18
Jun	15	18	20
Jul	10	22	25
Aug	15	15	18
Sep	25	18	22
Oct	20	18	25
Nov	22	10	25
Dec	20	25	25

**BLACKFOG**  
Privacy. Security. Prevention.

Published April 2022

### Ransomware Reports to FCA

20% rise in reports to the UK's Finance Regulator

Month	2020	2021
Jan	2	2
Feb	3	3
Mar	5	8
Apr	6	12
May	8	14
Jun	10	15
Jul	12	15
Aug	14	15
Sep	16	18
Oct	18	20
Nov	20	22
Dec	22	25

**PICUS** **FCA**  
FINANCIAL CONDUCT AUTHORITY

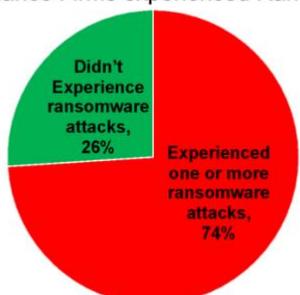
Published April 2022

# Cyber Insights: Ransoms & Suppliers

Click each image to see each report in full. All were published in month to May 2022

## Attempted Ransom Attacks

74% of Finance Firms experienced Ransom Attack

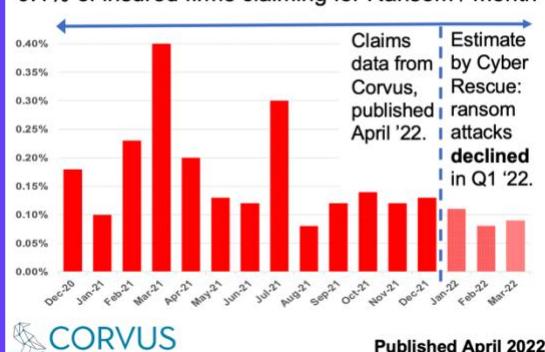


**vmware**

Survey of 130 financial security leaders & CISOs  
Published April 2022

## Successful Ransom %s

0.1% of insured firms claiming for Ransom / month

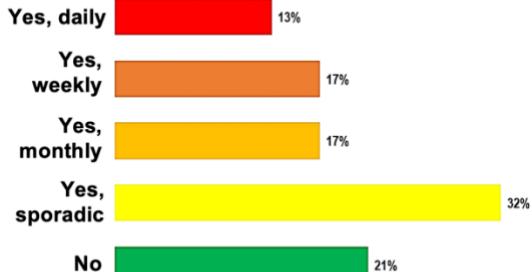


**CORVUS**

Published April 2022

## Attempted Ransom Attacks

79% of professionals had ransomware experience



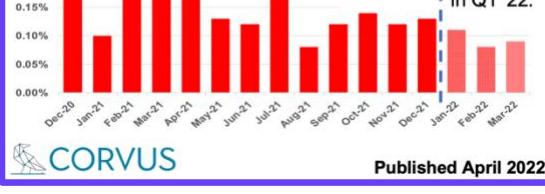
**Zerto**

Survey of 620 IT & Cyber professionals  
Published April 2022

## Successful Ransom %s

0.1% of insured firms claiming for Ransom / month

Claims data from Corvus, published April '22. Estimate by Cyber Rescue: ransom attacks declined in Q1 '22.

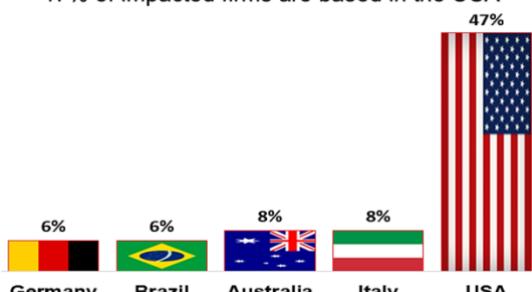


**CORVUS**

Published April 2022

## Ransom Success by Country

47% of impacted firms are based in the USA

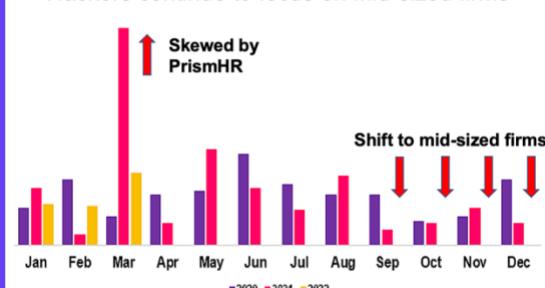


**accenture**

Published April 2022

## Size of Firms hit by Ransom

Hackers continue to focus on mid-sized firms

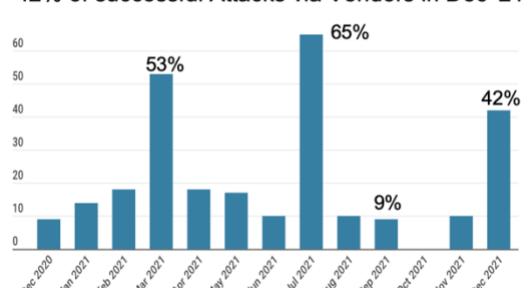


**BLACKFOG**  
Privacy. Security. Prevention.

Published April 2022

## Ransoms via Vendors

42% of successful Attacks via Vendors in Dec '21

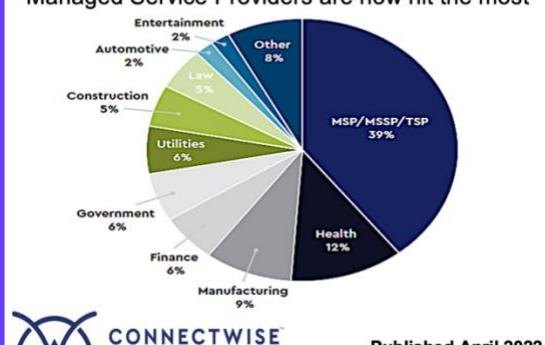


**CORVUS**

Published April 2022

## Industries hit by Ransoms

Managed Service Providers are now hit the most

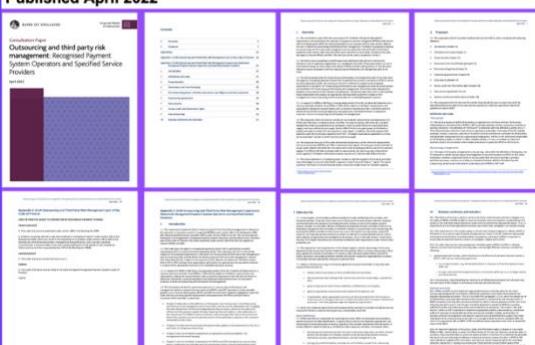


**CONNECTWISE**

Published April 2022

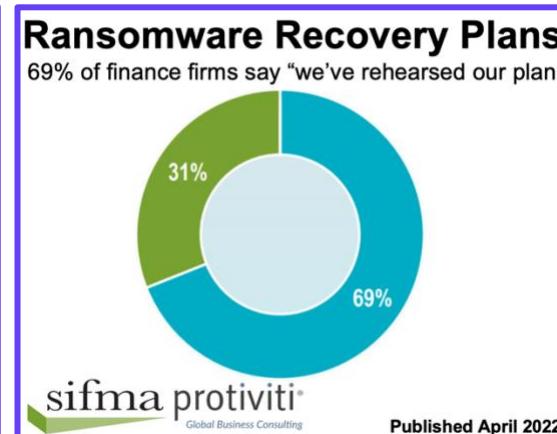
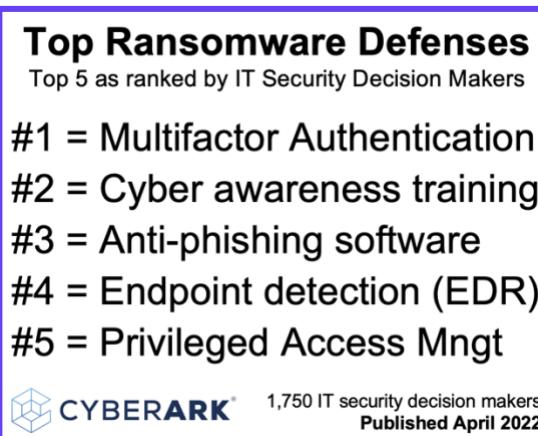
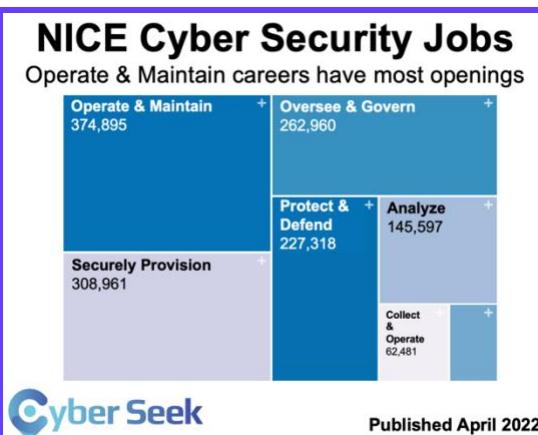
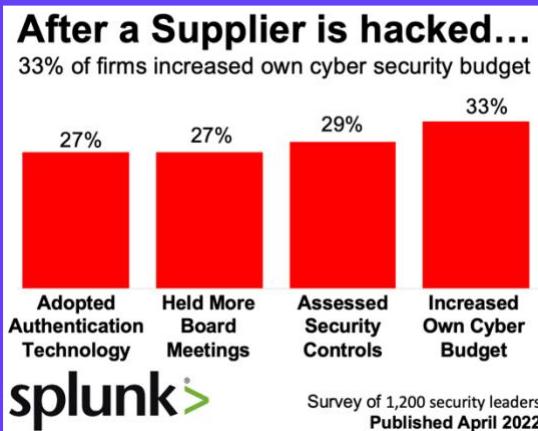
## Third Party Risk Mngt

Bank of England's Code of Practice



# Cyber Insights: *Investment for Resilience*

Click each image to see each report in full. All were published in month to May 2022

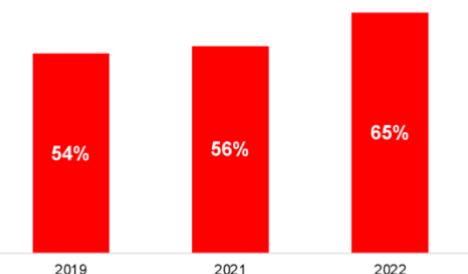


# Cyber Insights: *Significance & Impact*

Click each image to see each report in full. All were published in month to May 2022

## Firm Directors & Cyber Risk

Directors who say "Very" or "Extremely" significant



CLYDE&CO

Survey of directors & risk managers in > 40 countries  
Published April 2022

## Top 5 Risks to Firms today

Ranked by Directors in over 40 countries

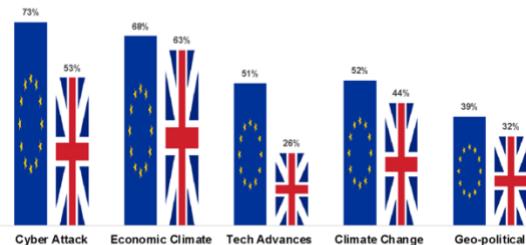
- #1 = Cyber Attack
- #2 = Data Loss
- #3 = Cyber Extortion
- #4 = Regulatory Risk
- #5 = Risk to Health & Safety

CLYDE&CO

Survey of directors & risk managers in > 40 countries  
Published April 2022

## Risks most feared by Firms

Cyber Attacks & Economic Climate most feared

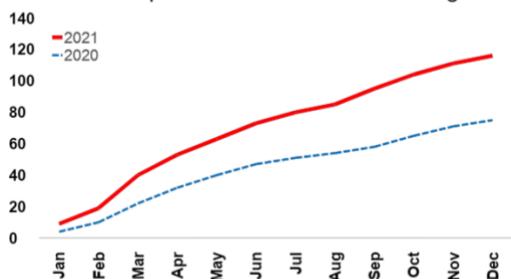


CLYDE&CO

Survey of directors & risk managers in > 40 countries  
Published April 2022

## Cyber Attack Reports to FCA

55% rise in reports to the UK's Finance Regulator

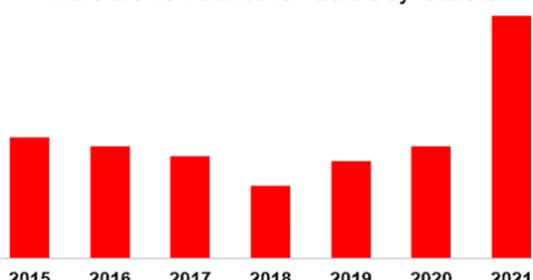


FCA FINANCIAL CONDUCT AUTHORITY

Published April 2022

## "Zero Day" Attacks Doubled

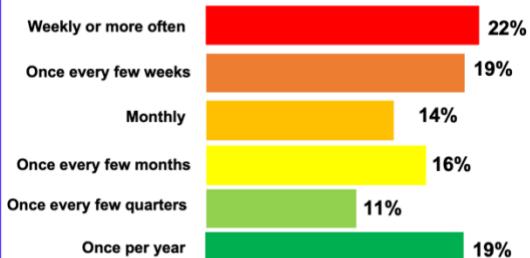
There are no Patches for "Zero Day" attacks



Published April 2022

## Frequency in Cyber Attacks

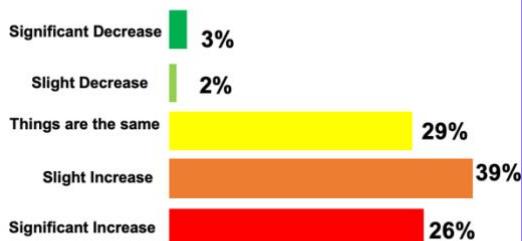
22% of firms hit by Cyber Attacks at least weekly



Published April 2022

## Downtime caused by Cyber

64% say Downtime caused by Cyber Attacks is Up



Published April 2022

## Financial Conduct Authority

FCA's new Strategy pushes Operational Resilience



FCA FINANCIAL CONDUCT AUTHORITY



Published April 2022

## 4. Cyber Insights: *Vulnerabilities & Attackers*

Click each image to see each report in full. All were published in month to May 2022

### Ransomware Entry Points

36% of ransomware caused by vulnerable software

Email	27%
Exposed devices	31%
Poor access control	31%
Vulnerable systems	33%
Vulnerable software	36%

**Zerto** Survey of 620 IT & Cyber professionals Published April 2022

### Top Clicked Phishing Tests

10 Email Categories

**KnowBe4** Human error. Conquered. Published April 2022

### Top Phishing Brands in 2022

LinkedIn at number 1 with 52%

**CHECK POINT** Published April 2022

### Remote Work has doubled

Post Covid-lockdowns, 34% of work is still remote

**CISCO SECURE** Published April 2022

### Ransom Gangs hitting MSPs

Managed Service Providers hit most by LockBit

**CONNECTWISE** Published April 2022

### Ransomware Preparedness

52% of firms "much stronger" incase of an attack

**Zerto** Survey of 620 IT & Cyber professionals Published April 2022

### Web Credit Card Skimmers

Malware tripled on WordPress (WooCommerce)

**SUCURI** Review of malware on e-commerce platforms Published April 2022

### Vulnerabilities Report

Small & Medium-Sized Businesses

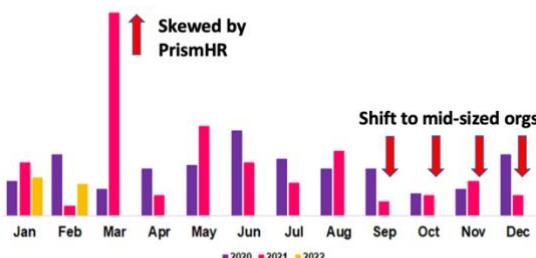
**CyberCatch** Published April 2022

## 4. Cyber Insights: *Ransom Attacks*

Click each image to see each report in full. All were published in month to April 2022

### Size of Firms hit by Ransom

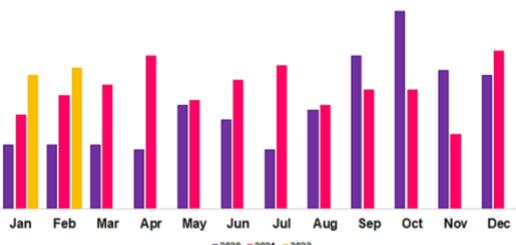
Mid-sized firms still the focus of Hackers



Published March 2022

### Successful Ransom Attacks

Number is up again in February 2022



Published March 2022

### Average RANSOM Demand

Conti makes biggest demands, averaging \$8.7m



Published March 2022

### Ransom Gangs seen by FBI

Top 3 Gangs that attack Critical Infrastructure

REvil / \$oDINoKIBI

51

LOCKBIT 2.0

58

CONTI

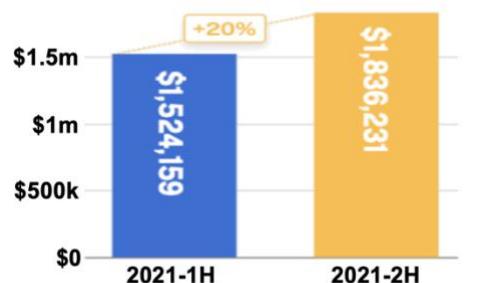
87



Published March 2022

### Size of RANSOM Demanded

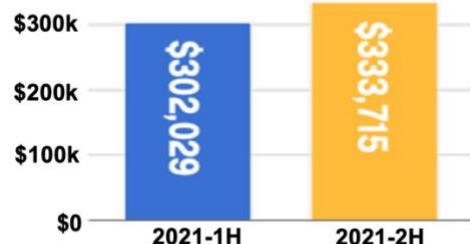
Average Ransom demand rose 20% in 6 months



Published March 2022

### Size of RANSOM Paid

Average Ransom Paid rose 10% in 6 months

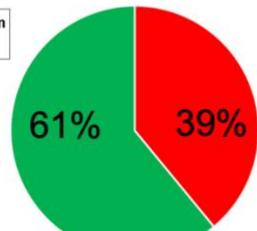


Published March 2022

### Ransom Payments

61% of CISOs refused to pay Ransom

■ Paid the Ransom  
■ Refused to Pay



Survey of 500 Phishing Victims in IT  
Published Mar 2022

### Average Ransom Payout

Significant Increase by 63% for Feb. 2022

Average known  
Payout =

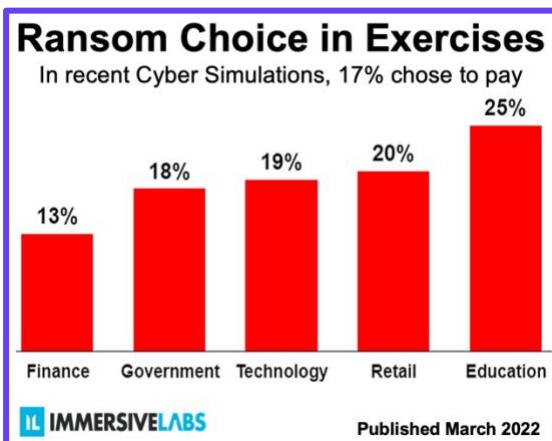
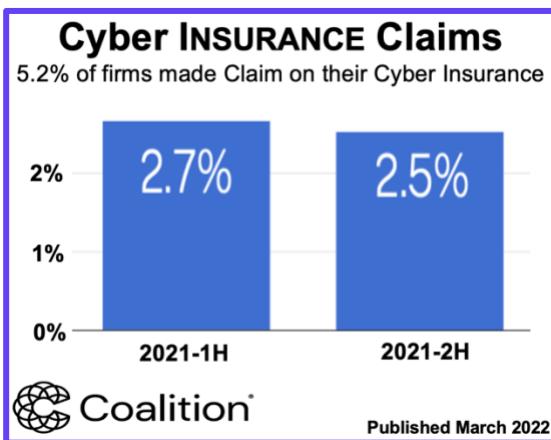
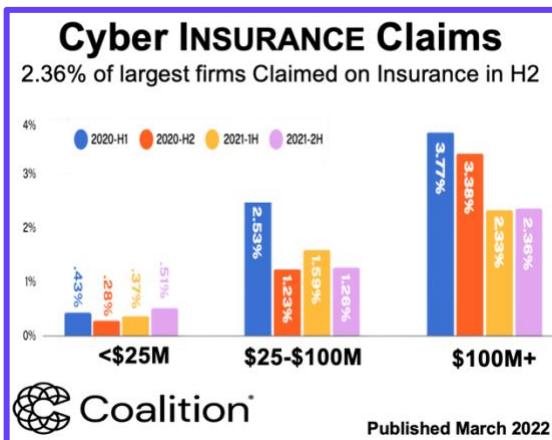
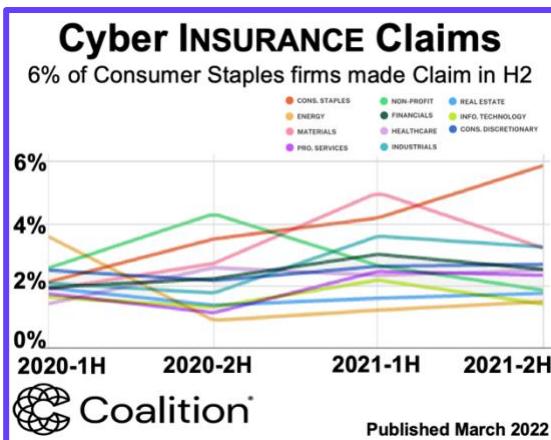
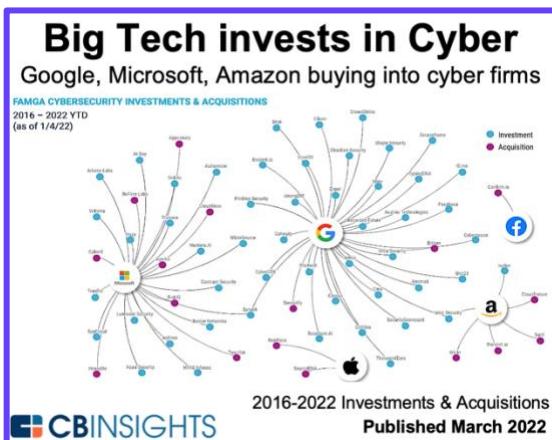
USD \$322k



Published March 2022

## 4. Cyber Insights: Insurance and Investments

Click each image to see each report in full. All were published in month to April 2022

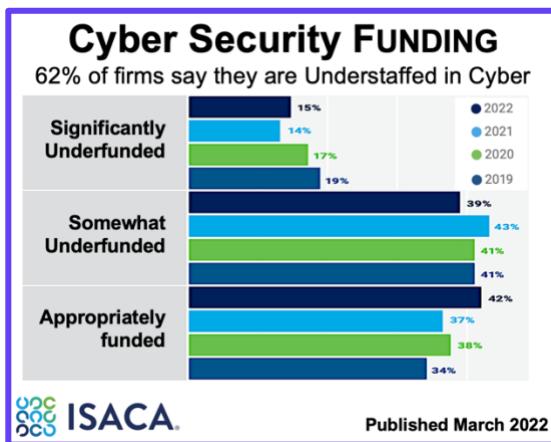
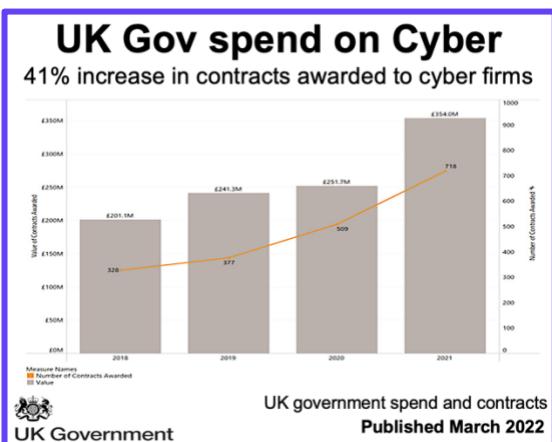


### 1,838 Cyber Firms in the UK

Cyber firms have £10bn revenue & 53,000 staff

Size	Number of Firms	Estimated Revenue (Cyber Security Related)	Estimated GVA (Cyber Security Related)	Estimated Employment (FTE) (Cyber Security Related)	Estimated Revenue per employee	Estimated GVA per employee
Large	156	£7,599m	£3,739m	33,630	£225,959	£111,180
Medium	184	£1,357m	£780m	9,357	£147,086	£83,341
Small	447	£857m	£556m	6,738	£127,235	£82,542
Micro	1,051	£313m	£251m	3,002	£104,364	£83,762
Grand Total	1,838	£10,146m	£5,326m	52,727	£192,423	£101,019

UK Economic Contribution  
UK Government  
Published March 2022



## 4. Cyber Insights: Attacks and Techniques

Click each image to see each report in full. All were published in month to April 2022

### Microsoft Account Takeover

20% of firms using M365 suffered a compromise



Barracuda.  
Your journey, secured.

Published March 2022

### Cyber Hijacking Web Chat

Increase in volume of online conversations attacked

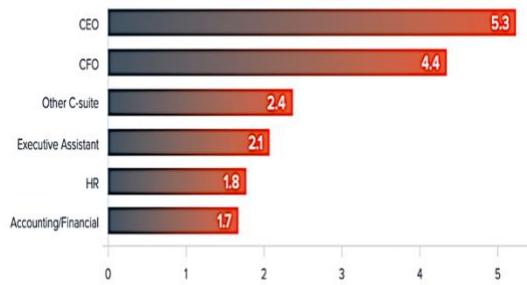


Barracuda.  
Your journey, secured.

Published March 2022

### Executive Account Takeover

Cyber Criminals target CEOs and CFOs the most

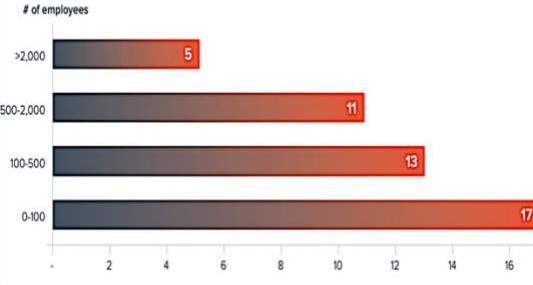


Barracuda.  
Your journey, secured.

Published March 2022

### Social Engineering Attacks

Firms with <100 staff suffer most attacks / mailbox

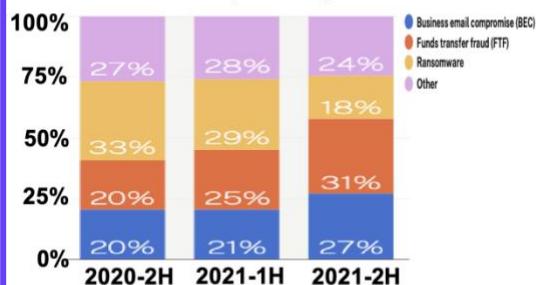


Barracuda.  
Your journey, secured.

Published March 2022

### Frequency of Cyber Attacks

Business Email Compromise grew fast in 2021-H2

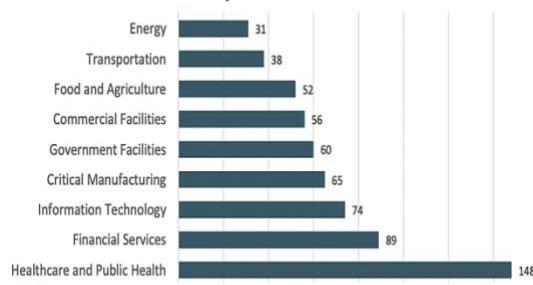


Cybersecurity Coalition

Published March 2022

### Ransomware reported to FBI

Health & Finance report Ransomware most often

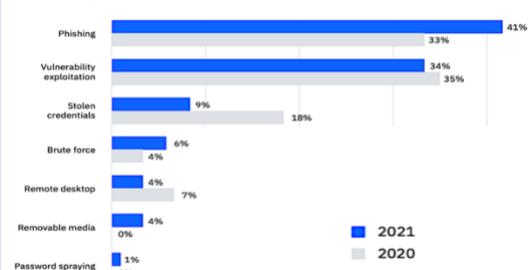


FBI

Published March 2022

### Vectors for Cyber Infection

Phishing Emails overtake Vulnerability Exploitation

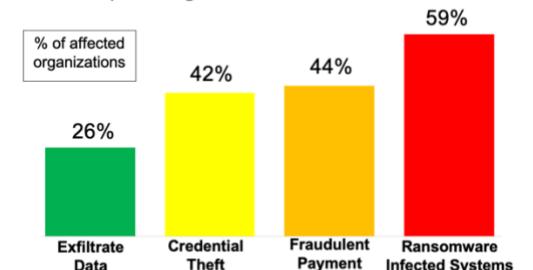


IBM

Published March 2022

### Phishing Attacks Outcomes

59% of phishing attacks leads to Ransomware

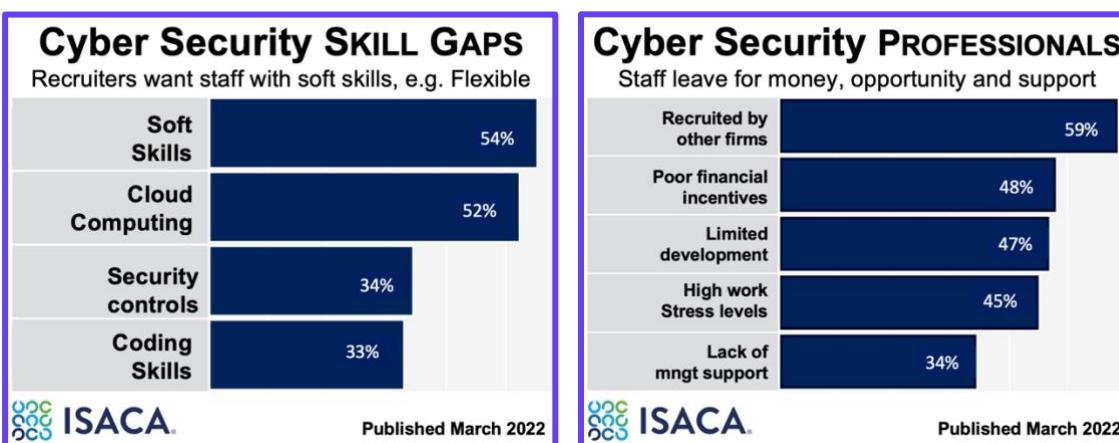
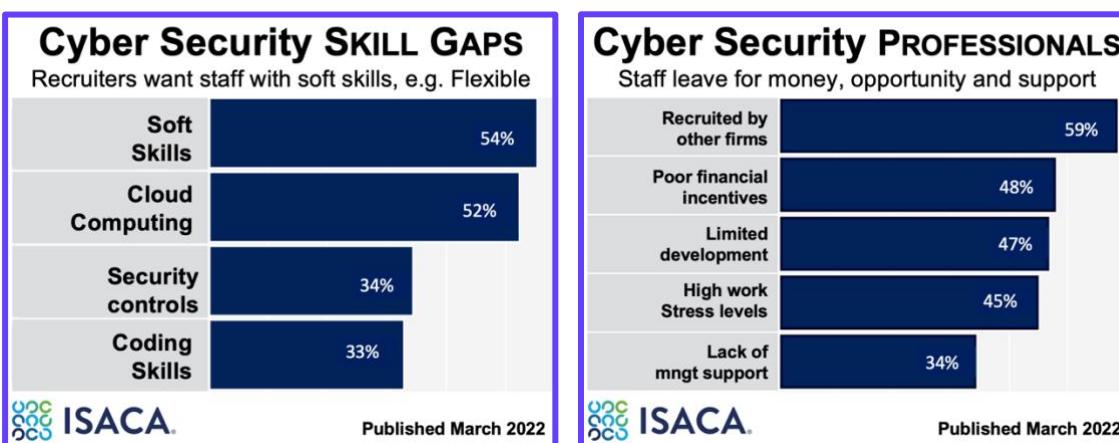
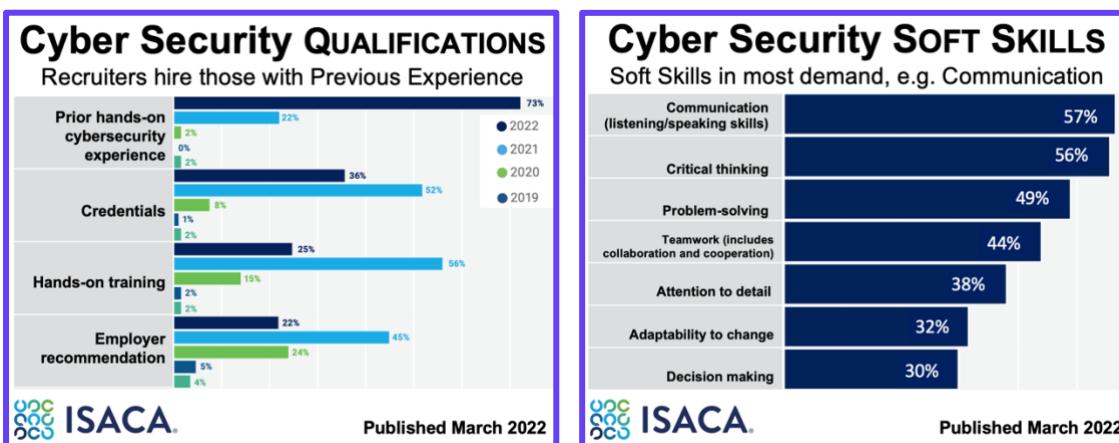
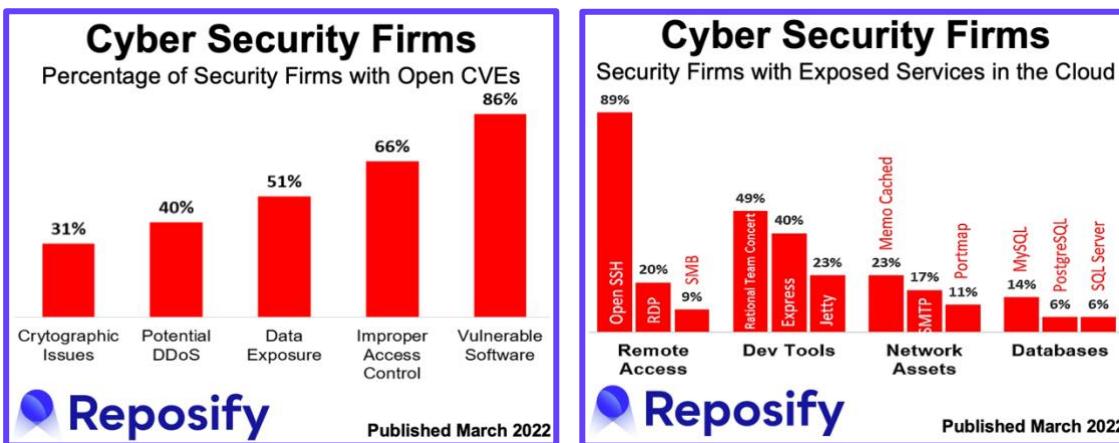
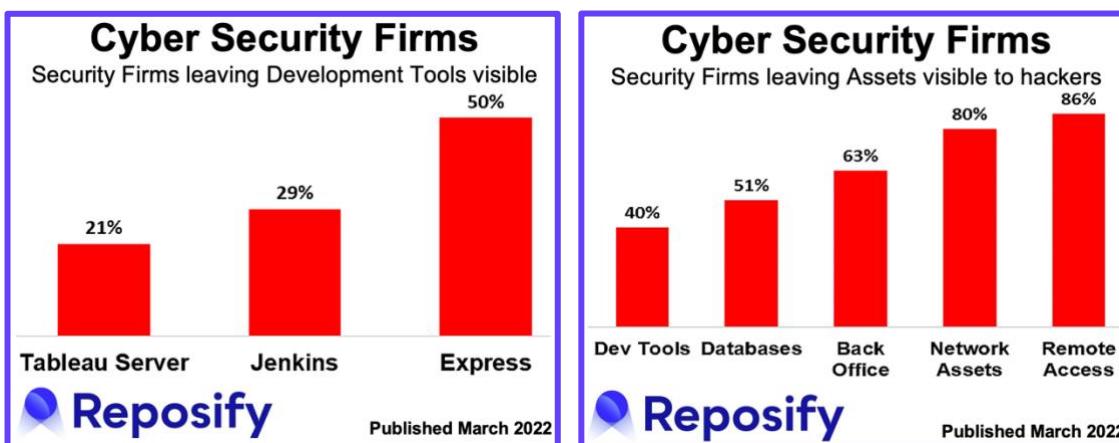


egress®

Survey of 500 Phishing Victims in IT  
Published Mar 2022

## 4. Cyber Insights: Cyber Professionals & Security Firms

Click each image to see each report in full. All were published in month to April 2022

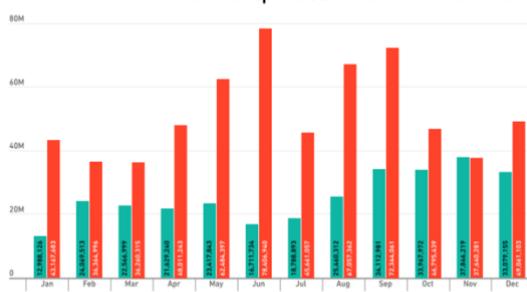


# Cyber Insights: Ransomware Volumes

Click each image to see each report in full. All were published in month to March 2022

## Global Ransomware Volume

Ransomware attacks up 60% in last 12 months

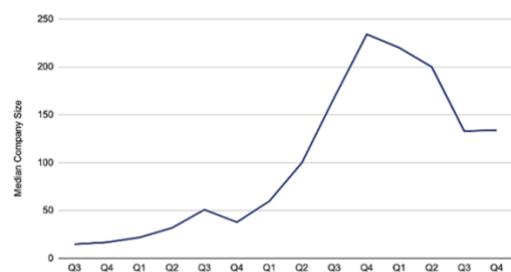


SONICWALL

Published Feb 2022

## Ransomware TARGET SIZE

Typical Firm breached by Ransom has 133 staff



COVEWARE

Published February 2022

## Ransomware Strains

17% rise in active Ransomware types

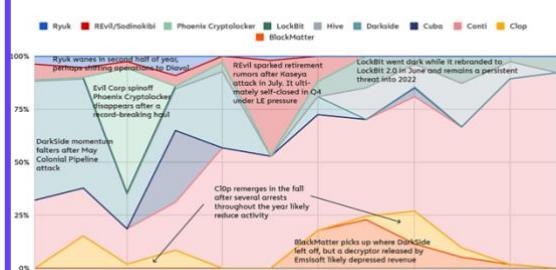


Chainalysis

Published Feb 2022

## Ransomware Strains

Payments per month over last year

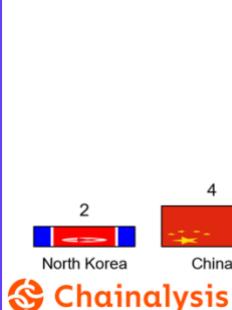


Chainalysis

Published Feb 2022

## Ransomware Strains

Iran & Russia linked to most strains

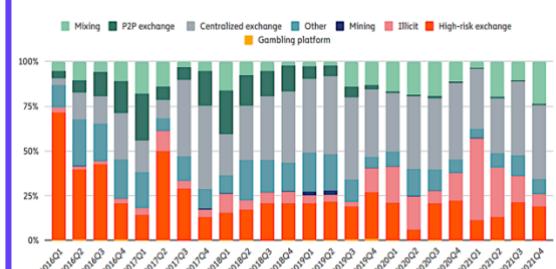


Chainalysis

Published Feb 2022

## Ransom Laundering

Centralized Exchange the top choice

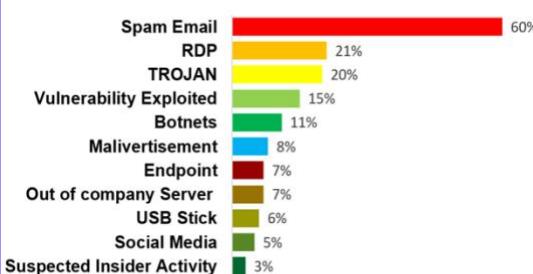


Chainalysis

Published Feb 2022

## Ransomware INFECTIONS

Most Ransomware infections enter firms via Email

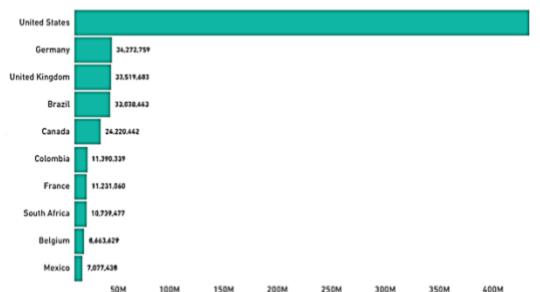


VEEAM

Published February 2022  
Survey of 1,700 hit by Ransom Attack

## Ransomware by Country

USA suffers vast majority of Ransomware Attacks



SONICWALL

Published Feb 2022

# Cyber Insights: Ransom Costs

Click each image to see each report in full. All were published in month to March 2022

### Ransom Payments

34% rise to average of \$118k paid

Value in thousands of USD

Year	Value (k USD)
2016	8
2017	15
2018	12
2019	25
2020	88
2021	118

**Chainalysis** Published Feb 2022

### Ransoms PAID by Industry

Industrial firms in USA pay twice as often as in EU

Region	PAID (%)	DID NOT PAY (%)
U.S.	64.6%	15.6%
APAC	39.7%	34.3%
Europe	34.3%	32.3%

**CLAROTY** Published February 2022 Survey of 1,100 IT & ICS Professionals

### Ransoms PAID by Region

Industrial firms in USA most likely to pay >\$5m

Value Range	EU	China	USA	Other
< \$100K	12.8%	11.8%	13.4%	
\$100K - \$500K	28.5%	31.5%	22.8%	
\$500K - \$1M	24.2%	23.6%	25.1%	
\$1M - \$5M	5.0%	10.5%	14.9%	
> \$5M	2.8%	0.7%	8.4%	

**CLAROTY** Published February 2022 Survey of 1,100 IT & ICS Professionals

### Ransoms COST by Region

Industrial firms in USA most likely to suffer >\$5m

Value Range	EU	China	USA	Other
< \$100K	14.7%	18.7%	16.1%	
\$100K - \$500K	22.5%	23.1%	21.7%	
\$500K - \$1M	15.9%	16.9%	19.5%	
\$1M - \$5M	8.8%	11.2%	13.5%	
> \$5M	5.1%	3.6%	10.3%	

**CLAROTY** Published February 2022 Survey of 1,100 IT & ICS Professionals

### Ransoms COST in Industry

Downtime losses when Ransomware detonates

Value Range	Losses (millions of USD)
<\$100,000	~100
\$100,000 - \$500,000	~300
\$500,000 - \$1,000,000	~250
\$1,000,000 - \$5,000,000	~150
>\$5,000,000	~100

**CLAROTY** Published February 2022 Survey of 1,100 IT & ICS Professionals

### Ransom Payments

\$602m paid via Crypto in 2021

Cryptocurrency value in millions of USD

Year	Value (millions of USD)
2016	\$24
2017	\$0.06
2018	\$39
2019	\$152
2020	\$692
2021	\$602

**Chainalysis** Published Feb 2022

### Ransom-related Data Leaks

82% rise in Data Leaks caused by Ransomware

Year	Leaks
2020	1,474
2021	2,686

**CROWDSTRIKE** Review of ransom attacks by CrowdStrike Intelligence Published February 2022

### Ransom-related Data Leaks

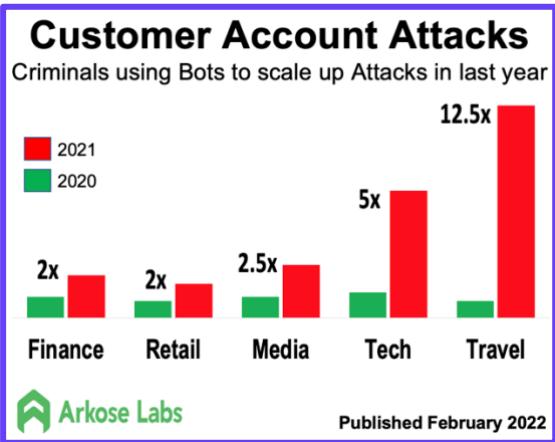
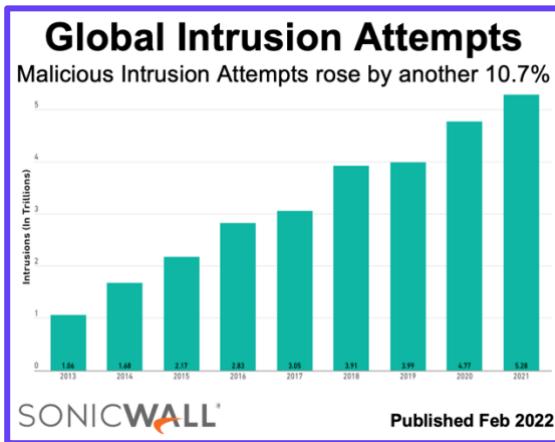
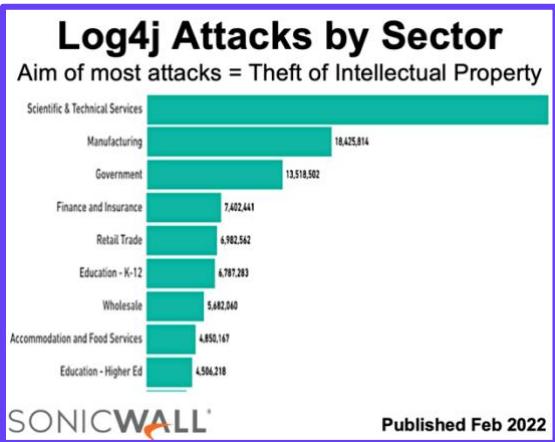
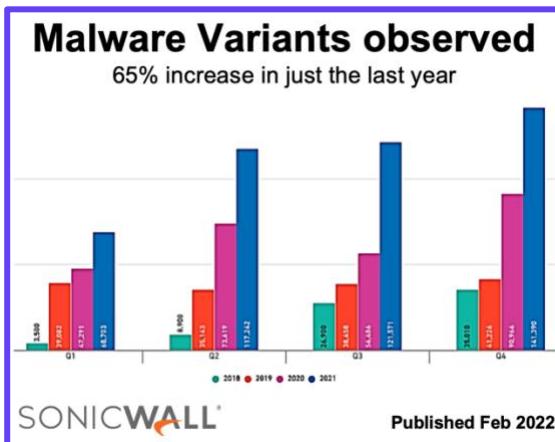
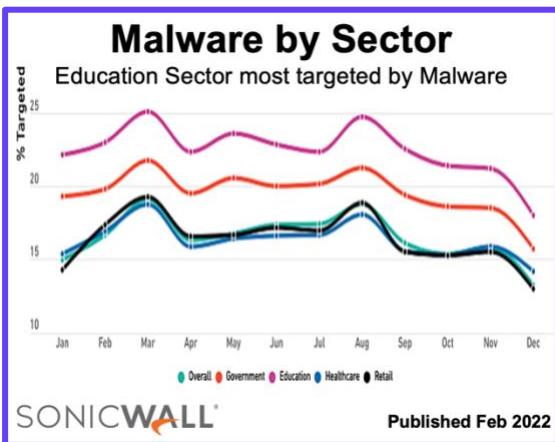
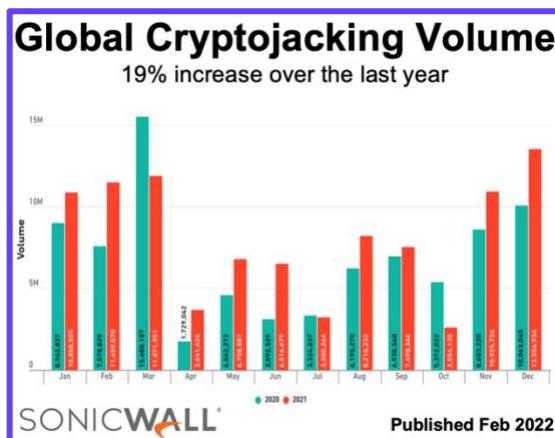
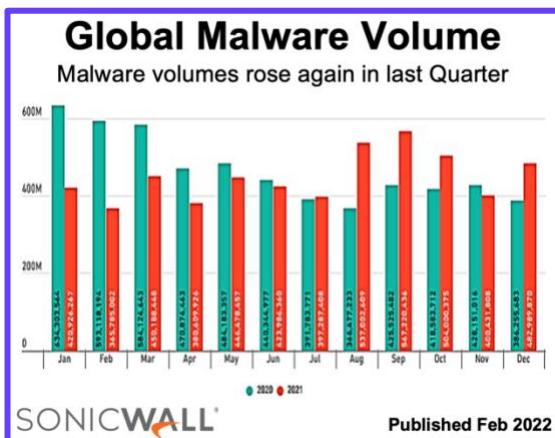
Engineers most likely to have stolen data leaked

Industry	2020	2021
Engineering	~220	~400
Manufacturing	~200	~280
Tech	~150	~200
Services	~70	~180

**CROWDSTRIKE** Review of cyber attacks in 2020 & 2021 Published February 2022

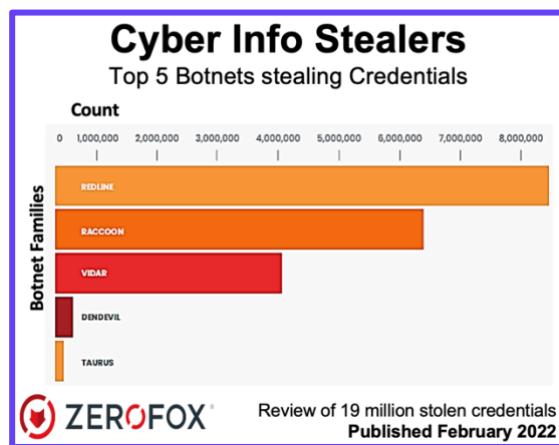
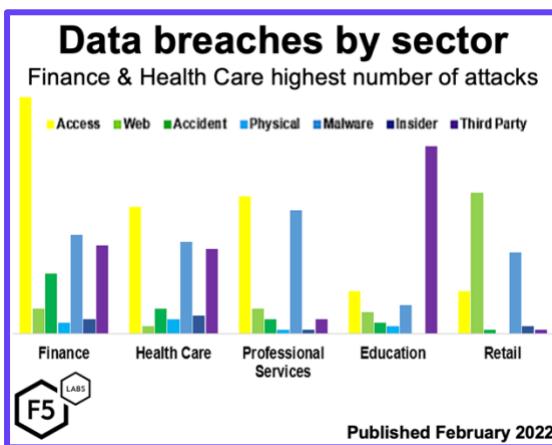
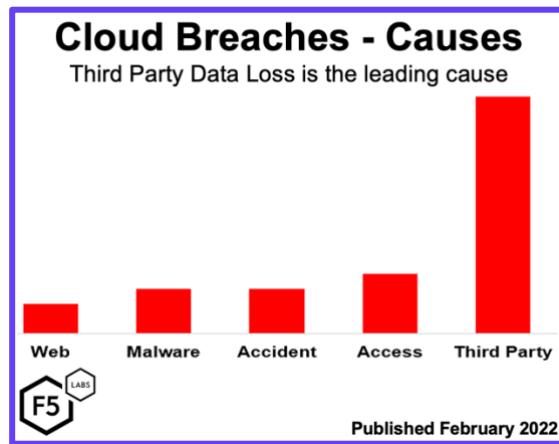
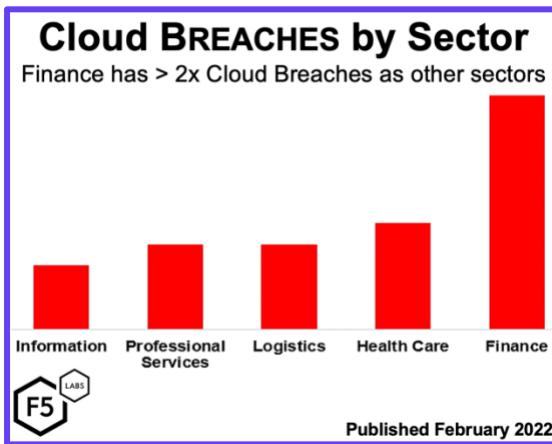
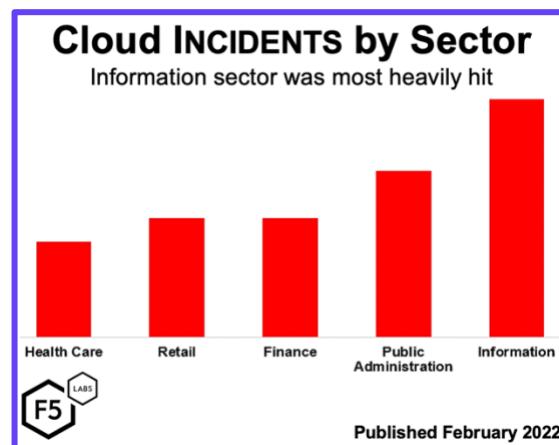
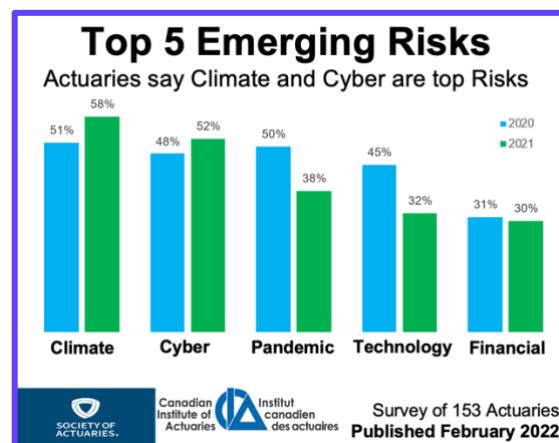
# Cyber Insights: Malwares & Attacks

Click each image to see each report in full. All were published in month to March 2022



# Cyber Insights: Risks & Breaches

Click each image to see each report in full. All were published in month to March 2022



# Cyber Insights: Cyber Pros & Insurance

Click each image to see each report in full. All were published in month to March 2022

## Security Engineer CONCERN

Changing Technologies & New Threats worry most



Survey of 309 security engineers  
Published February 2022

## Security Engineer BURNOUT

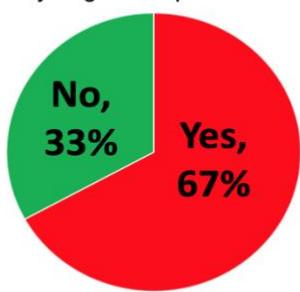
What % feel "burnt-out" by their work in Cyber?



Survey of 309 security engineers  
Published February 2022

## Security Engineer LOYALTY

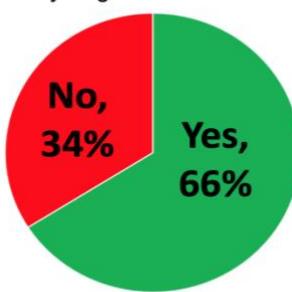
67% of Security Engineers "plan to leave" employer



Survey of 309 security engineers  
Published February 2022

## Security Engineer SALARIES

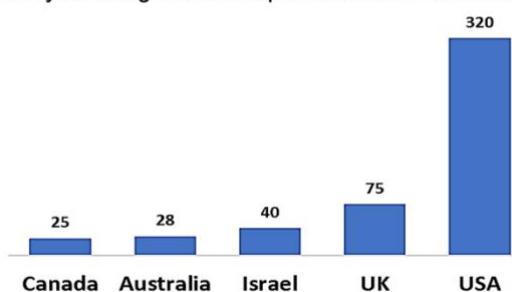
66% of Security Engineers satisfied with their pay



Survey of 309 security engineers  
Published February 2022

## Cyber M&A

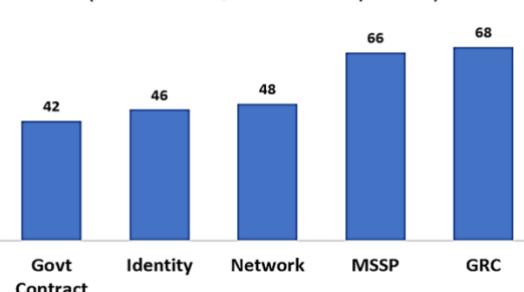
320 cyber mergers were reported in the USA in 2021



Review of 430 cyber M&As  
Published February 2022

## Cyber M&A

GRC (Governance, Risk & Compliance) leads

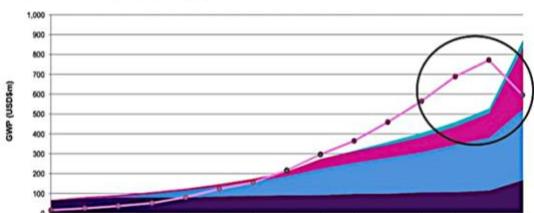


Review of 430 cyber M&As  
Published February 2022

## Cyber INSURANCE GROWTH

UK Market Leader sold almost \$900m in last year

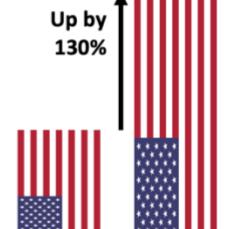
- 20% ransomware frequency reduction per policy
- 60% ransomware frequency reduction per premium



Published February 2022  
Annual Results by UK's leader in Cyber Insurance, with almost \$900m in Premiums

## Cyber Insurance Prices: x2

Price of Insurance rose 130% in 12 months in USA



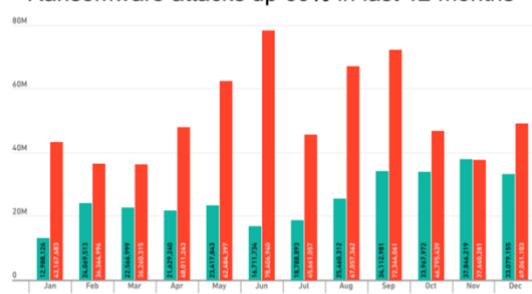
Global Insurance Market Index  
Published February 2022

# Best Cyber Insights of 2022

Click each image to see each report in full. All were published in month to March 2022

## Global Ransomware Volume

Ransomware attacks up 60% in last 12 months

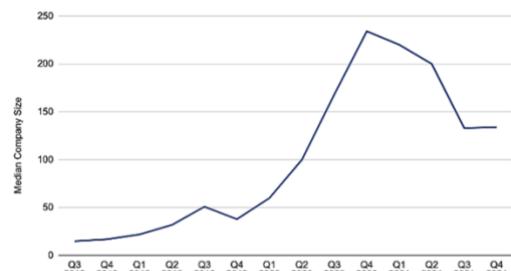


SONICWALL

Published Feb 2022

## Ransomware TARGET SIZE

Typical Firm breached by Ransom has 133 staff

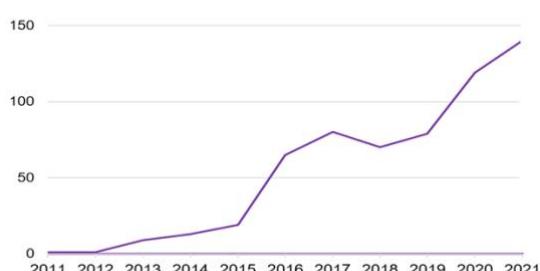


COVWARE

Published February 2022

## Ransomware Strains

17% rise in active Ransomware types

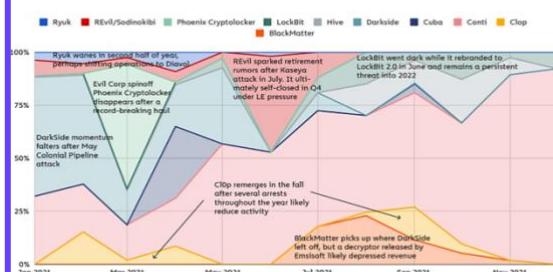


Chainalysis

Published Feb 2022

## Ransomware Strains

Payments per month over last year

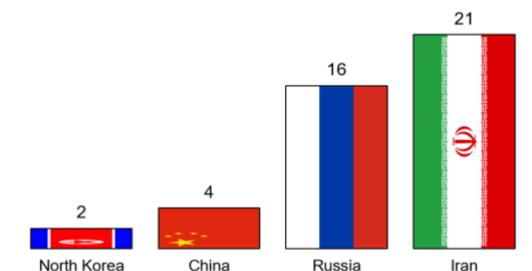


Chainalysis

Published Feb 2022

## Ransomware Strains

Iran & Russia linked to most strains

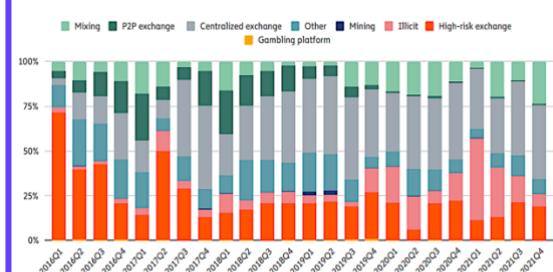


Chainalysis

Published Feb 2022

## Ransom Laundering

Centralized Exchange the top choice

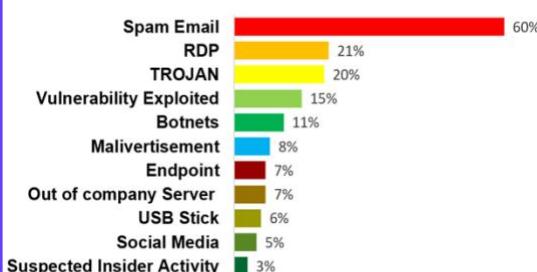


Chainalysis

Published Feb 2022

## Ransomware INFECTIONS

Most Ransomware infections enter firms via Email



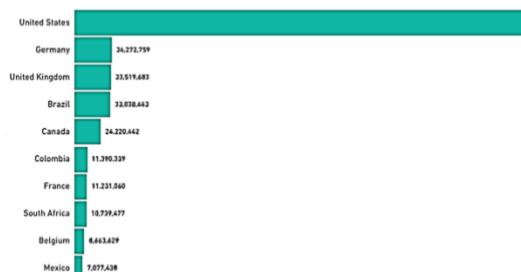
VEEAM

Published February 2022

Survey of 1,700 hit by Ransom Attack

## Ransomware by Country

USA suffers vast majority of Ransomware Attacks



SONICWALL

Published Feb 2022

# Cyber Insights: Ransom Costs

Click each image to see each report in full. All were published in month to March 2022

### Ransom Payments

34% rise to average of \$118k paid

Value in thousands of USD

Year	Value (k USD)
2016	8
2017	15
2018	12
2019	25
2020	88
2021	118

**Chainalysis** Published Feb 2022

### Ransoms PAID by Industry

Industrial firms in USA pay twice as often as in EU

Region	Percentage
U.S.	64.6%
APAC	39.7%
Europe	34.3%
U.S.	15.6%
APAC	34.3%
Europe	32.3%

**DID NOT PAY**

**CLAROTY** Published February 2022 Survey of 1,100 IT & ICS Professionals

### Ransoms PAID by Region

Industrial firms in USA most likely to pay >\$5m

Value Range	EU	China	USA
< \$100K	12.8%	11.8%	13.4%
\$100K - \$500K	28.5%	31.5%	22.8%
\$500K - \$1M	24.2%	23.6%	25.1%
\$1M - \$5M	5.0%	10.5%	14.9%
> \$5M	2.8%	0.7%	8.4%

**CLAROTY** Published February 2022 Survey of 1,100 IT & ICS Professionals

### Ransoms COST by Region

Industrial firms in USA most likely to suffer >\$5m

Value Range	EU	China	USA
< \$100K	14.7%	18.7%	16.1%
\$100K - \$500K	22.5%	23.1%	21.7%
\$500K - \$1M	15.9%	16.9%	19.5%
\$1M - \$5M	8.8%	11.2%	13.5%
> \$5M	5.1%	3.6%	10.3%

**CLAROTY** Published February 2022 Survey of 1,100 IT & ICS Professionals

### Ransoms COST in Industry

Downtime losses when Ransomware detonates

Loss Range	EU	China	USA
< \$100,000	~10%	~10%	~10%
\$100,000 - \$500,000	~25%	~25%	~25%
\$500,000 - \$1,000,000	~20%	~20%	~20%
\$1,000,000 - \$5,000,000	~10%	~10%	~10%
> \$5,000,000	~5%	~5%	~5%

**CLAROTY** Published February 2022 Survey of 1,100 IT & ICS Professionals

### Ransom Payments

\$602m paid via Crypto in 2021

Cryptocurrency value in millions of USD

Year	Value (m USD)
2016	\$24
2017	\$0.06
2018	\$39
2019	\$152
2020	\$692
2021	\$602

**Chainalysis** Published Feb 2022

### Ransom-related Data Leaks

82% rise in Data Leaks caused by Ransomware

Year	Leaks
2020	1,474
2021	2,686

**CROWDSTRIKE** Review of ransom attacks by CrowdStrike Intelligence Published February 2022

### Ransom-related Data Leaks

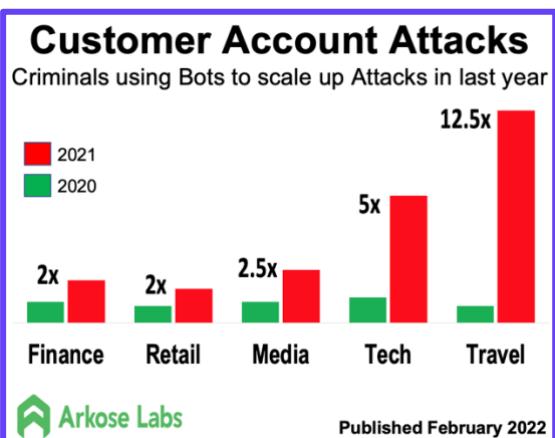
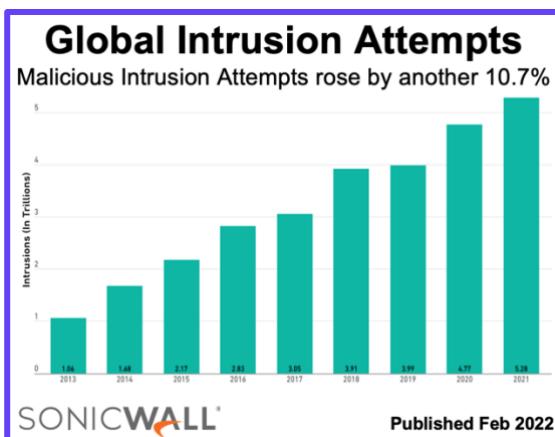
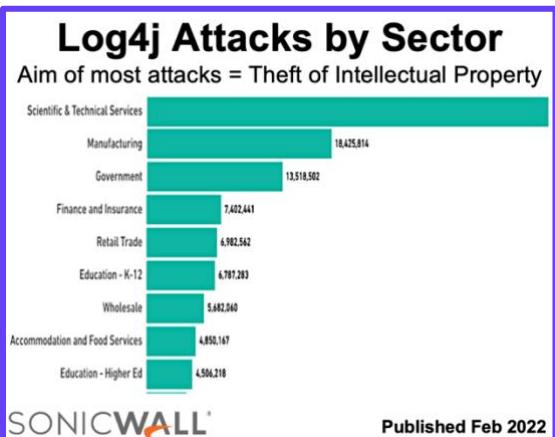
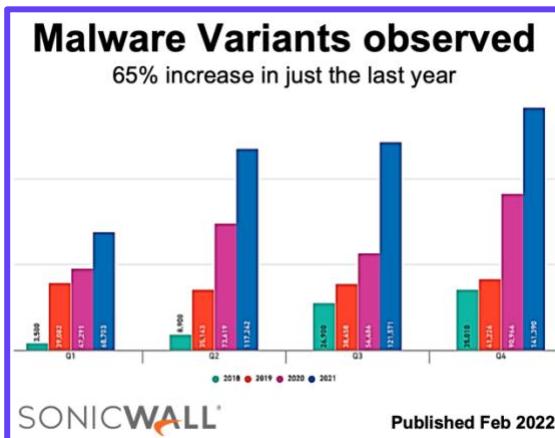
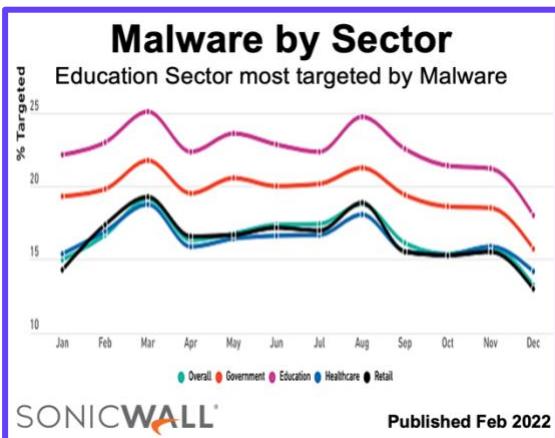
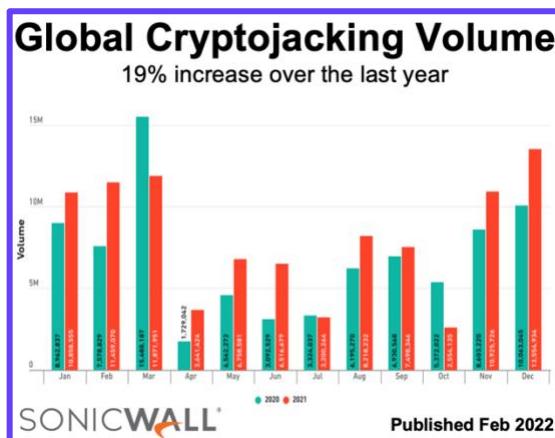
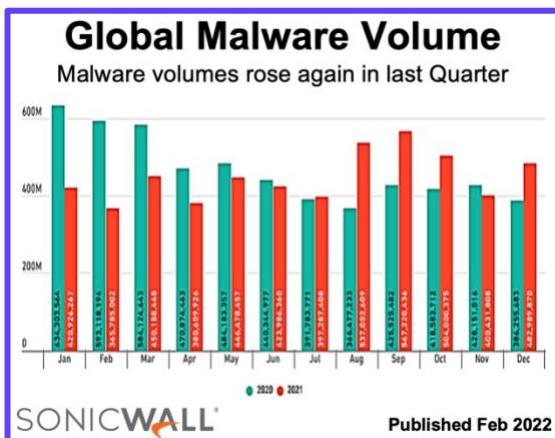
Engineers most likely to have stolen data leaked

Industry	2020	2021
Engineering	~220	~400
Manufacturing	~200	~290
Tech	~150	~210
Services	~70	~180

**CROWDSTRIKE** Review of cyber attacks in 2020 & 2021 Published February 2022

# Cyber Insights: Malwares & Attacks

Click each image to see each report in full. All were published in month to March 2022



# Cyber Insights: Risks & Breaches

Click each image to see each report in full. All were published in month to March 2022

### Cyber Risk in 2022

82% see a marked increase in Cyber Risk

Response	Percentage
Disagree	3%
Neutral	15%
Agree	31%
Strongly Agree	51%

**Control Risks**

Survey of 342 Professionals  
Published February 2022

### Top 5 Emerging Risks

Actuaries say Climate and Cyber are top Risks

Risk	2020 (%)	2021 (%)
Climate	51%	58%
Cyber	48%	52%
Pandemic	50%	38%
Technology	45%	32%
Financial	31%	30%

SOCIETY OF ACTUARIES • Canadian Institute of Actuaries • Institut canadien des actuaires

Survey of 153 Actuaries  
Published February 2022

### 3rd Party Cyber Risks

55% fear Ransoms via Suppliers

Risk Type	Percentage
Ransomware via 3rd party access points	55%
Data leakage via 3rd party	48%
Business disruption via 3rd party	47%
Supply chain disruption	45%
Reputational damage via 3rd Party breach	30%
Supply Chain Attack exposure or use	30%

**Prevalent™**

Published February 2022

### Cloud INCIDENTS by Sector

Information sector was most heavily hit

Sector	Incidents
Health Care	Low
Retail	Medium
Finance	Medium
Public Administration	High
Information	Very High

F5 LABS

Published February 2022

### Cloud BREACHES by Sector

Finance has > 2x Cloud Breaches as other sectors

Sector	Breaches
Information	Low
Professional Services	Medium
Logistics	Medium
Health Care	High
Finance	Very High

F5 LABS

Published February 2022

### Cloud Breaches - Causes

Third Party Data Loss is the leading cause

Cause	Percentage
Web	Low
Malware	Medium
Accident	Medium
Access	Medium
Third Party	Very High

F5 LABS

Published February 2022

### Data breaches by sector

Finance & Health Care highest number of attacks

Sector	Access	Web	Accident	Physical	Malware	Insider	Third Party
Finance	Very High	Low	Medium	High	Low	Medium	High
Health Care	High	Low	Low	Medium	Low	Medium	High
Professional Services	High	Low	Low	Very High	Low	Low	Medium
Education	Low	Low	Low	Low	Medium	Very High	Low
Retail	Low	Low	High	Low	Low	Low	Low

F5 LABS

Published February 2022

### Cyber Info Stealers

Top 5 Botnets stealing Credentials

Botnet Family	Count
REDLINE	8,500,000
RACCOON	6,500,000
VIDAR	4,000,000
DENDEVIL	1,000,000
TAURUS	500,000

ZEROFOX

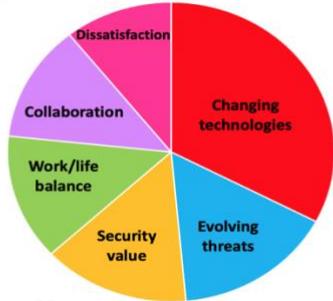
Review of 19 million stolen credentials  
Published February 2022

# Cyber Insights: Cyber Pros & Insurance

Click each image to see each report in full. All were published in month to March 2022

## Security Engineer CONCERN

Changing Technologies & New Threats worry most



Survey of 309 security engineers  
Published February 2022

## Security Engineer BURNOUT

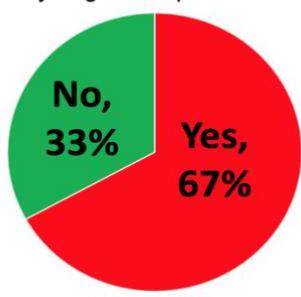
What % feel "burnt-out" by their work in Cyber?



Survey of 309 security engineers  
Published February 2022

## Security Engineer LOYALTY

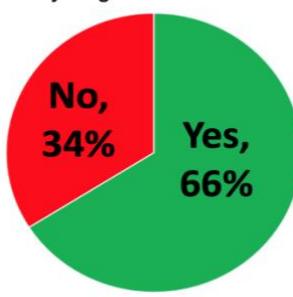
67% of Security Engineers "plan to leave" employer



Survey of 309 security engineers  
Published February 2022

## Security Engineer SALARIES

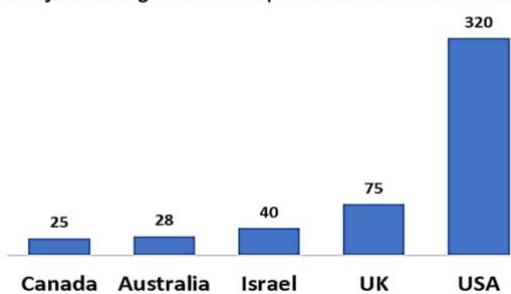
66% of Security Engineers satisfied with their pay



Survey of 309 security engineers  
Published February 2022

## Cyber M&A

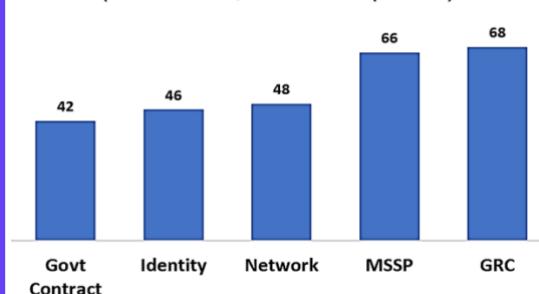
320 cyber mergers were reported in the USA in 2021



Review of 430 cyber M&As  
Published February 2022

## Cyber M&A

GRC (Governance, Risk & Compliance) leads

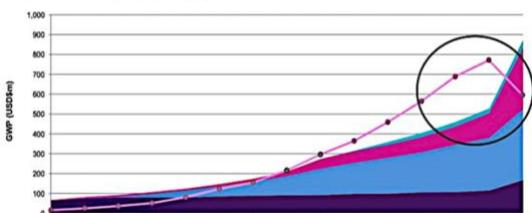


Review of 430 cyber M&As  
Published February 2022

## Cyber INSURANCE GROWTH

UK Market Leader sold almost \$900m in last year

- 20% ransomware frequency reduction per policy
- 60% ransomware frequency reduction per premium



Published February 2022  
Annual Results by UK's leader in Cyber Insurance, with almost \$900m in Premiums

## Cyber Insurance Prices: x2

Price of Insurance rose 130% in 12 months in USA



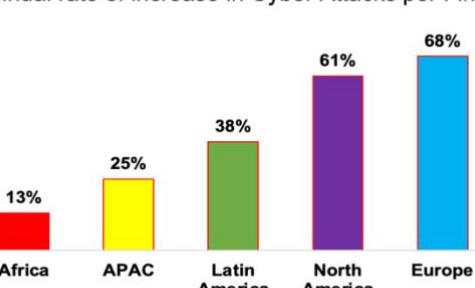
Global Insurance Market Index  
Published February 2022

# New Cyber Insights: *Growth Rates*

Click each image to see each report in full. All were published in month to Feb 2022

## Growth in Cyber Attacks

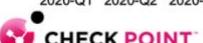
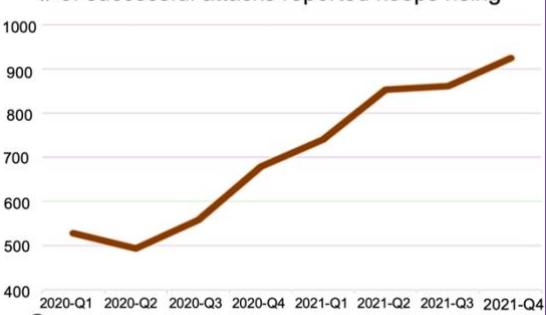
Annual rate of increase in Cyber Attacks per Firm



Published January 2022

## Growth in Attack Successes

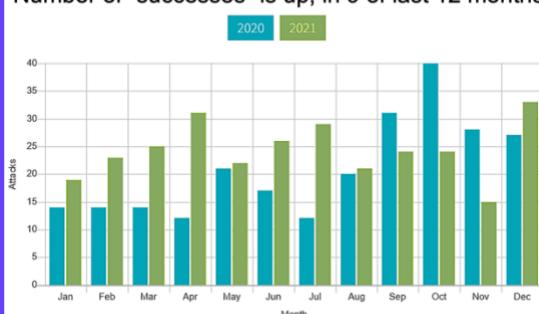
# of successful attacks reported keeps rising



Published January 2022

## Growth in Ransom Attacks

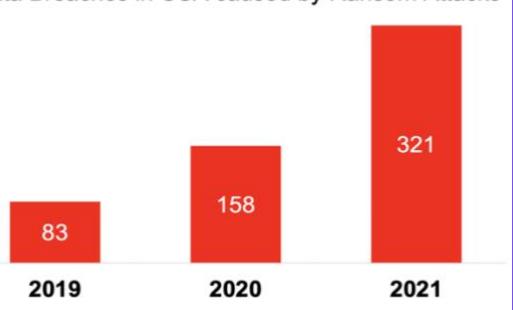
Number of "successes" is up, in 9 of last 12 months



Published January 2022

## Breaches by Ransomware

Data Breaches in USA caused by Ransom Attacks

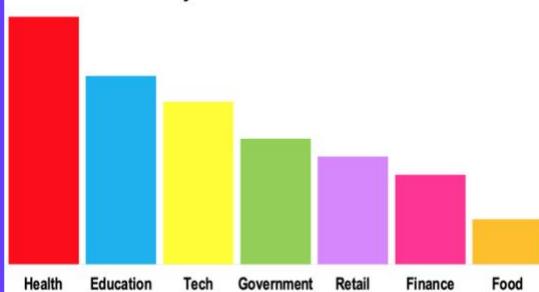


IDENTITY THEFT  
RESOURCE CENTER

Published Jan 2022

## Most Targeted Industries

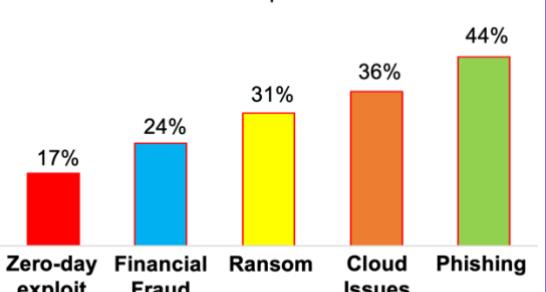
Over 24% of Cyber Breaches now in Healthcare



Published January 2022

## Cyber Security Threats

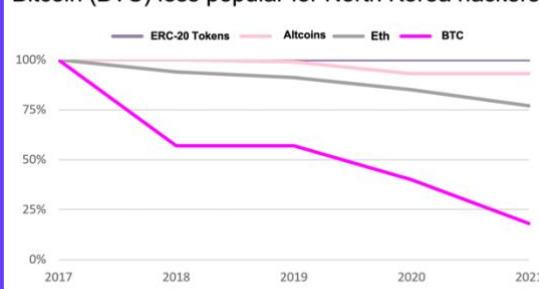
31% of IT Pros have experienced Ransomware



Survey of > 5,000 IT professionals  
Published January 2022

## The Currency of Ransoms

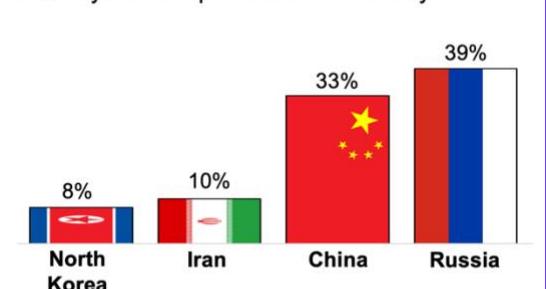
Bitcoin (BTC) less popular for North Korea hackers



Published Jan 2022

## State-run Cyber Threats

39% says Russia poses most serious cyber threat



Survey of > 5,000 IT professionals  
Published January 2022