

# ISOM 5280

## Course Introduction & Overview of Cybersecurity

Prof. Weiyin Hong  
Department of ISOM, HKUST Business School  
Fall 2024

# About Me



whong@ust.hk

- Associate Professor in ISOM
- 20+ years of teaching experience in UG, PG, Digital MBA, and Executive Courses
- Courses taught
  - Cybersecurity
  - AI and Deep Learning
  - Python
  - Database

# Table of Contents



## Course Overview

Course components

Course expectation



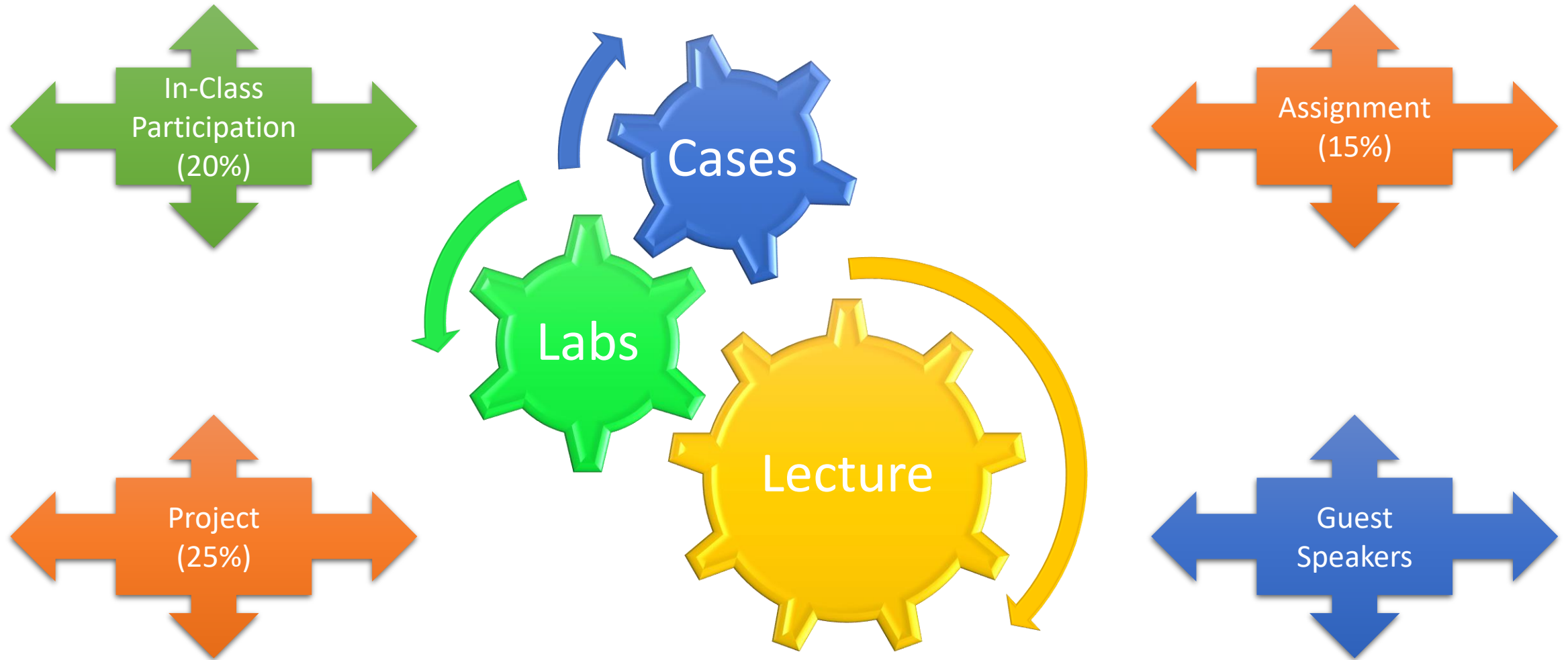
## Cybersecurity Overview

The offensive side

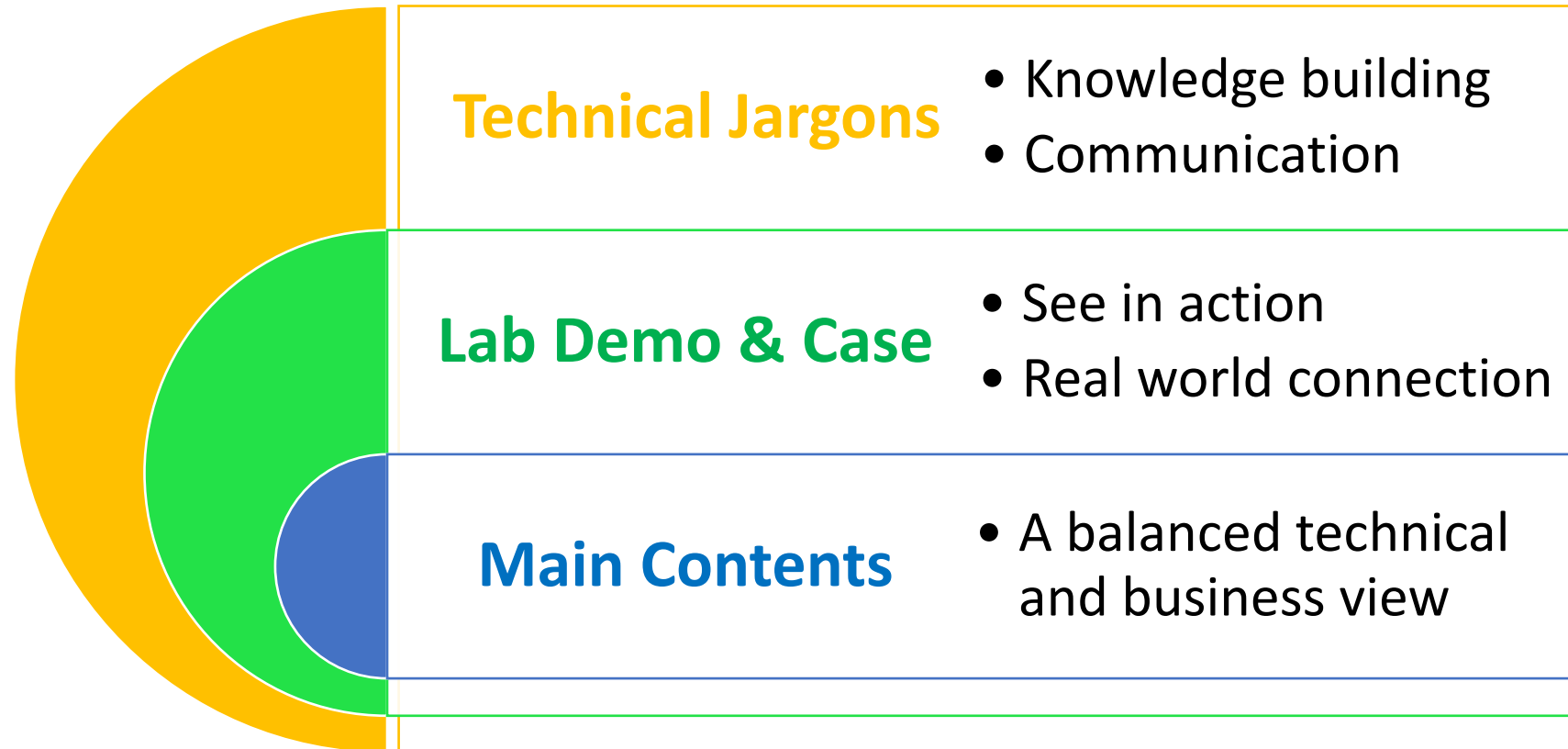
The defensive side

Job prospect

# Course Components



# Course Expectation



*\* Disclaimer: all materials and examples referred to in the class bear absolutely **NO political implications!***

# What do you think cybersecurity is about?



- Please go to [www.menti.com](https://www.menti.com)

# The Offensive Side



- ❑ Hong Kong and Global Trend
- ❑ Cybersecurity Incidents
- ❑ Cybersecurity Adversaries

# The Offensive Side

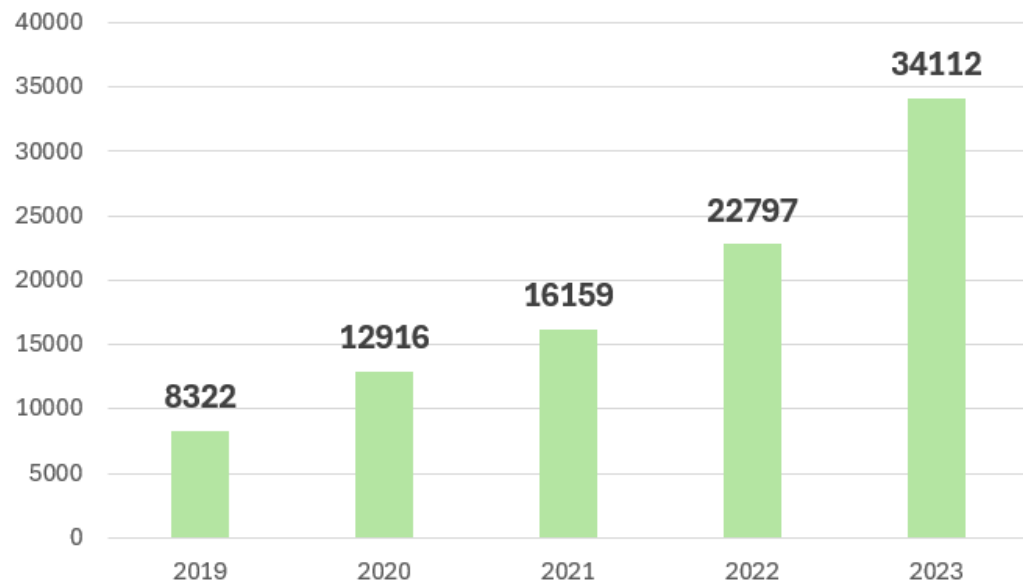


- ✓ Hong Kong and Global Trend
- ❑ Cybersecurity incidents
- ❑ Cybersecurity Adversaries

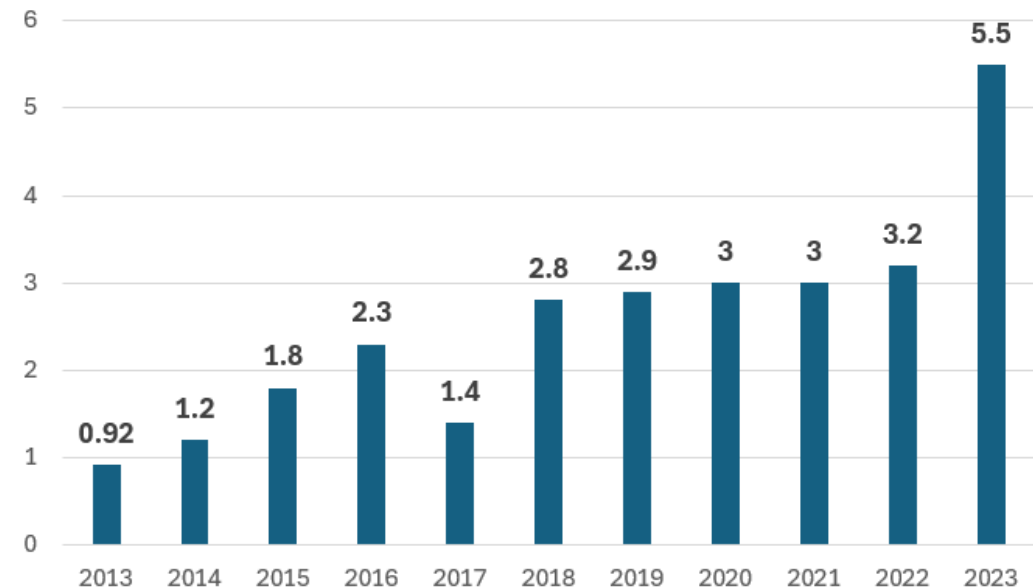


# Hong Kong Statistics

Technology Crime Cases (2019 - 2023)



Financial Losses of Technology Crime Cases in HK  
2013 - 2023 (HK\$ billion)



# Global Trend



What trend can we see here?  
- Per incident damage increased quickly. Elderly are more likely targets of attacks.

## 2023 - COMPLAINANTS BY AGE GROUP <sup>13</sup>

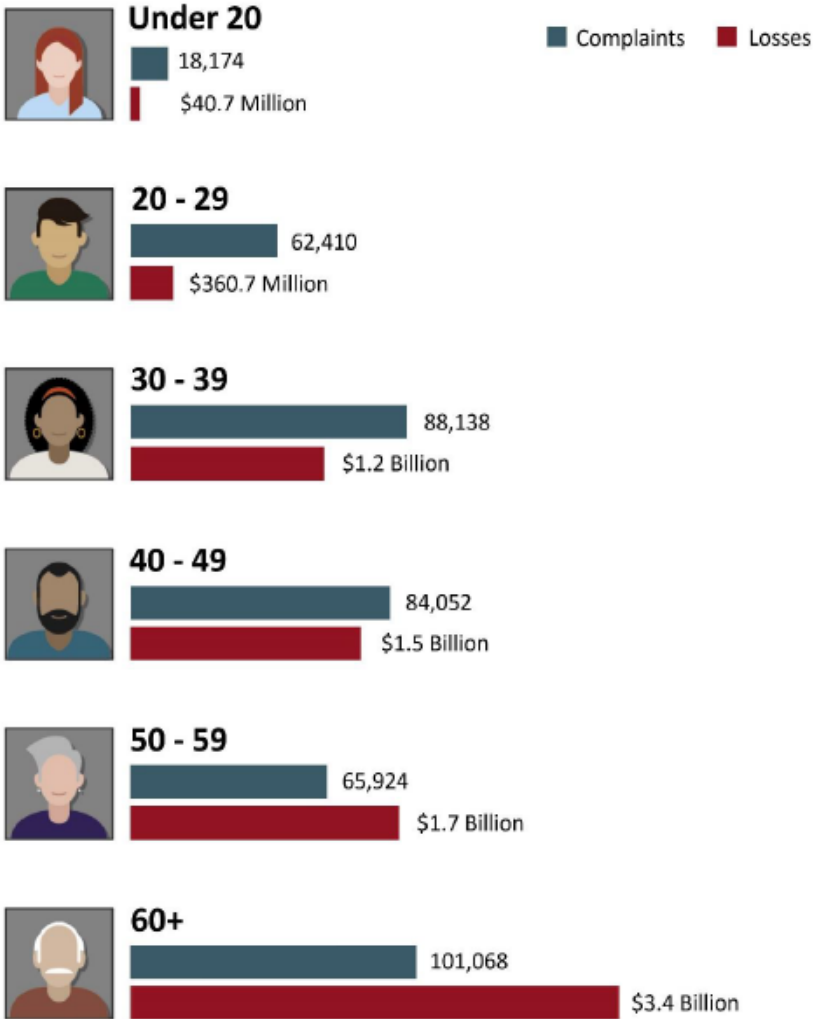
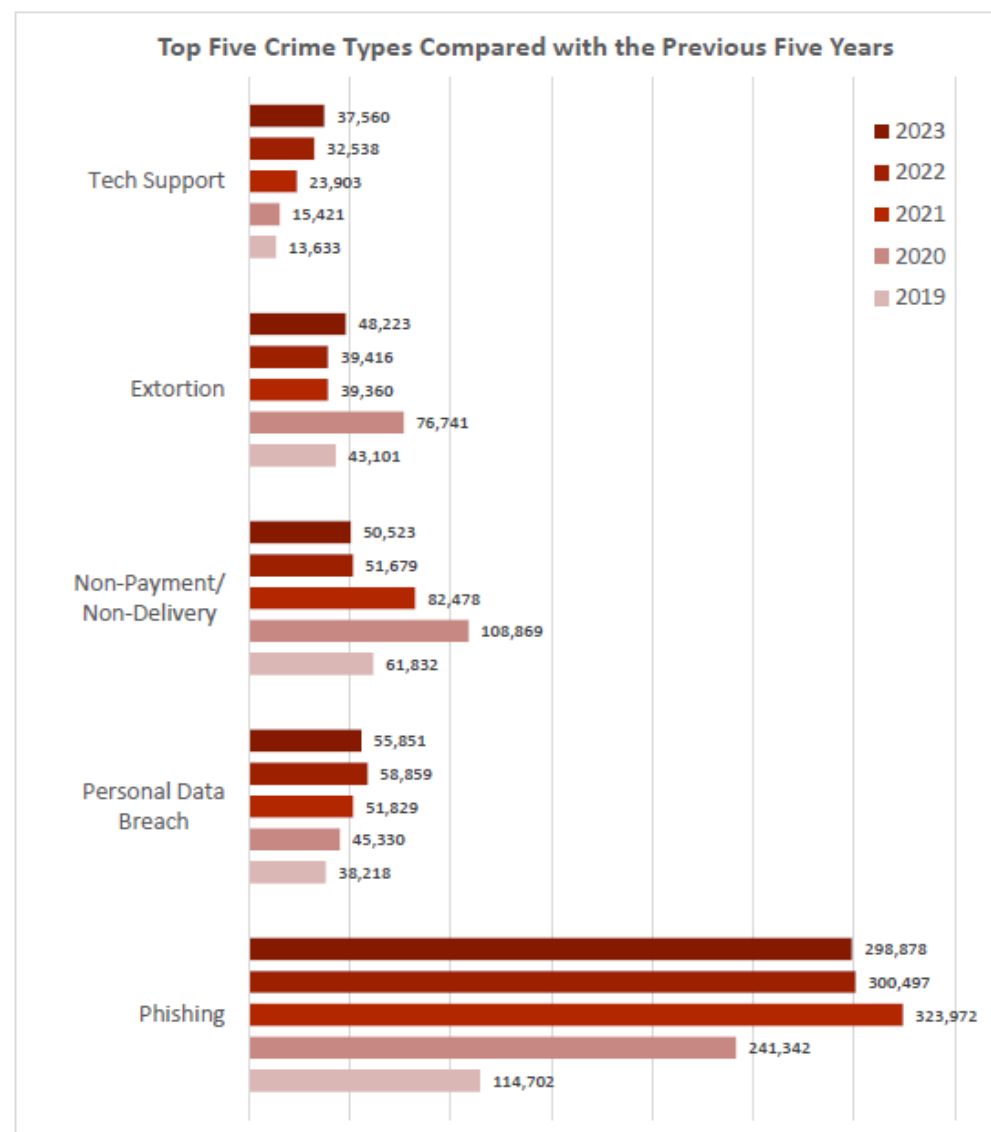


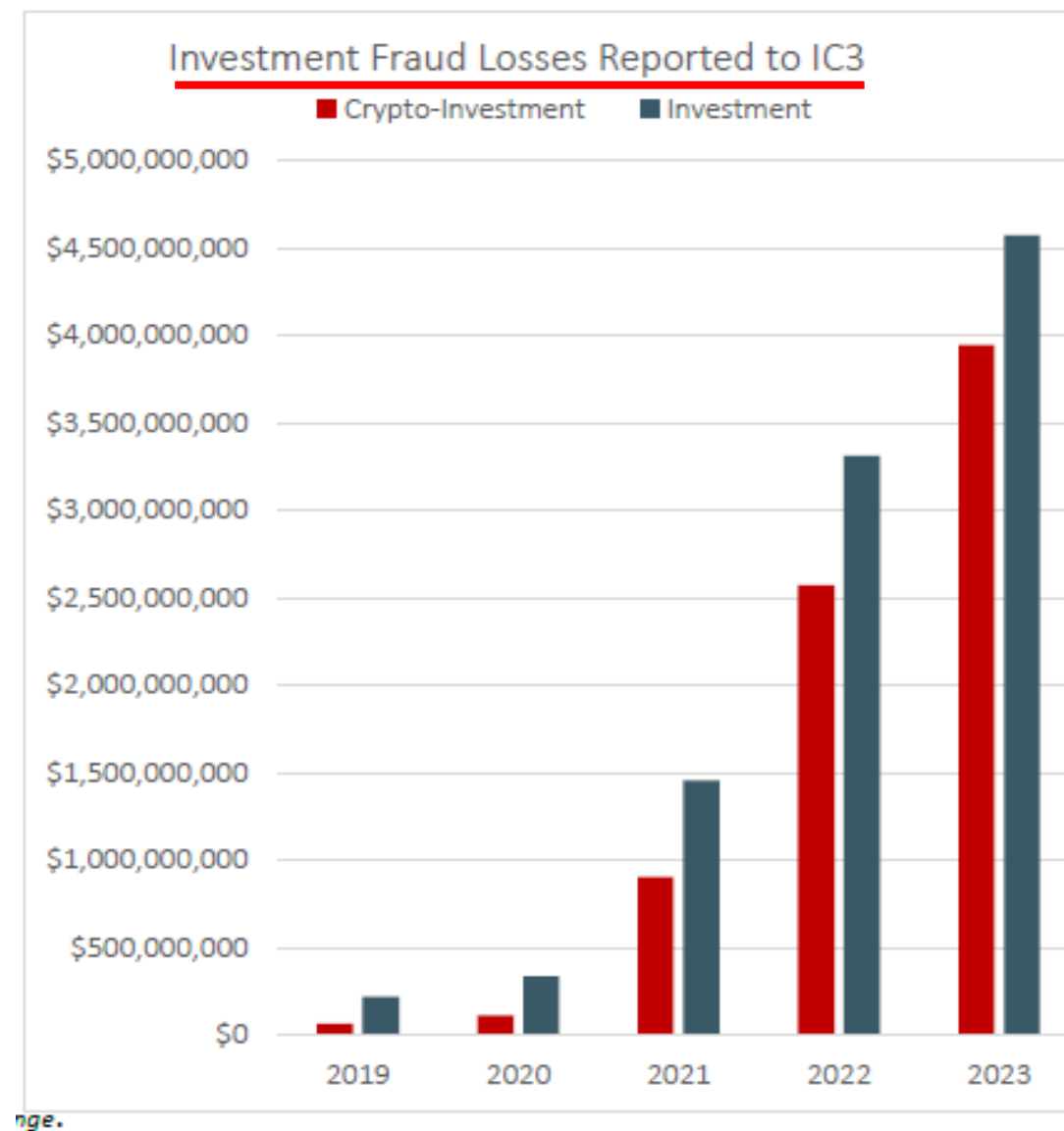
Image source: FBI

## TOP FIVE CRIME TYPE COMPARISON<sup>4</sup>



<sup>4</sup> Accessibility description: Chart includes a loss comparison for the top five reported crime types for the years of 2019 to 2023.

## Global Trend



# 2023 Cyberthreat Defense Report

North America | Europe | Asia Pacific | Latin America  
Middle East | Africa

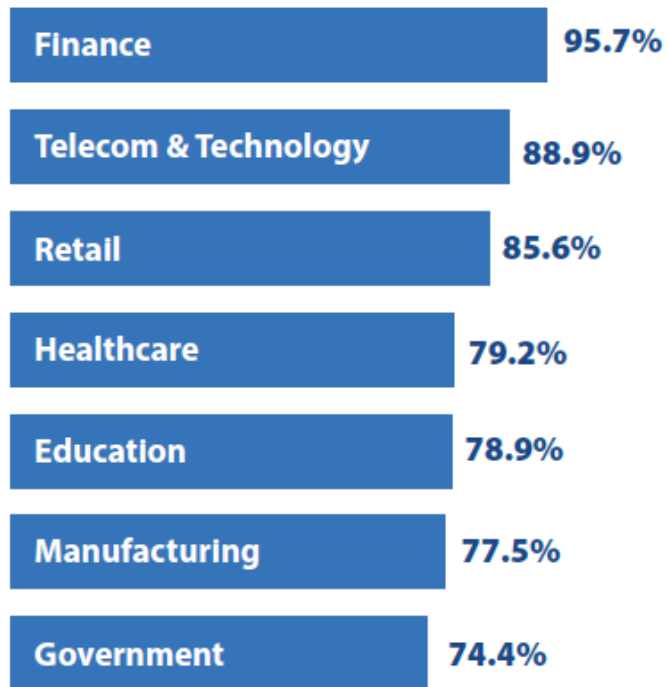


Figure 3: Percentage compromised by **at least one** successful attack in the past 12 months, by industry. Image source: CyberEdge Group



What's alarming here? – Financial institutions and critical infrastructures are more at risk.

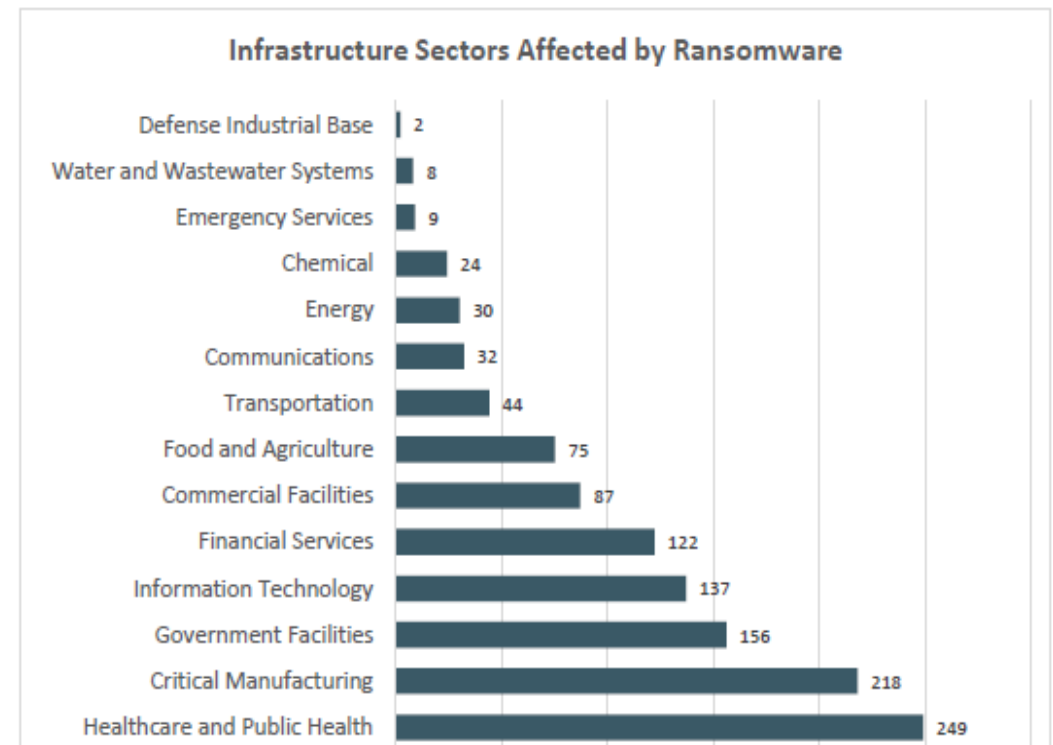
## RANSOMWARE



In 2023, the IC3 received 2,825 complaints identified as ransomware with adjusted losses of more than \$59.6 million. Ransomware is a type of malicious software, or malware, that encrypts data on a computer, making it unusable. In addition to encrypting the network, the cyber-criminal will often steal data off the system and hold that data hostage until the ransom is paid. If the ransom is not paid, the entity's data remains unavailable.

### Ransomware and Critical Infrastructure Sectors

The IC3 received 1,193 complaints from organizations belonging to a critical infrastructure sector that were affected by a ransomware attack. Of the 16 critical infrastructure sectors, IC3 reporting indicated 14 sectors had at least 1 member that fell to a ransomware attack in 2023.<sup>9</sup>



# The Offensive Side



- ☐ Hong Kong and Global Trend
- ✓ Cybersecurity Incidents
- ☐ Cybersecurity Adversaries

# Colonial hack: How did cyber-attackers shut off pipeline?

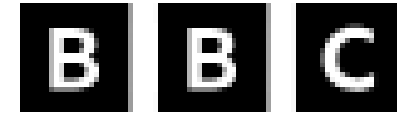
11 May 2021

Share ↗ Save +

Joe Tidy  
Cyber reporter



Investigators at the largest fuel pipeline in the US are working to recover from a devastating cyber-attack that cut the flow of oil.



- On May 7, 2021, a ransomware attack was launched on the largest refined oil products pipeline in the United States.
- A five-day shutdown of the pipeline, which disrupted the delivery of gasoline, diesel fuel, and jet fuel across the East Coast.
- Significant consequences, including reputational damage, legal ramifications, and recovery costs.
- Highlight the vulnerability of critical infrastructure to cyber attacks.

# Cyberport Hong Kong

Date	Event
Aug 6 2023	The hacker exploited a user account with administrative privileges to gain access to Cyberport's network.
Aug 14 2023	The files contained in Cyberport's servers were attacked by ransomware and maliciously encrypted.
Aug 14 2023	Cyberport took remedial actions, including a password reset for all user accounts.
Aug 17 2023	Cyberport received a ransom note from the hacker, who demanded a ransom of US\$300,000 - approximately HK\$2.35 million - for the leaked 400 gigabytes of information.
Aug 18 2023	Cyberport submitted a data breach notification to the PCPD. The PCPD immediately commenced a compliance check into the incident and recommended that Cyberport promptly notify all affected individuals.
Sept 5 2023	Trigona claimed on its website to have obtained data from Cyberport, amounted over 400GB, and publicly released samples of the data for sale.
Sept 6 2023	Cyberport issued media statements regarding the incident, follow-up actions including shutting down the affected computer equipment, and engaging an independent cybersecurity expert to conduct the investigation.



# Consumer Council



- 20 Sept 2023 – Ransomware attack (involving leakage of over 450 personal data)
- 23 Sept 2023 – Public release

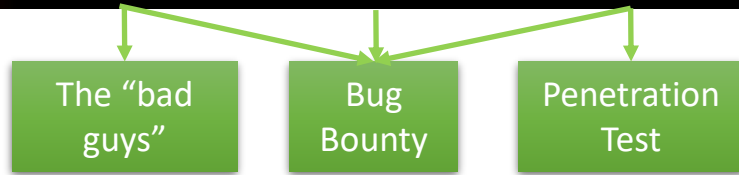


# The Offensive Side



- ☐ Hong Kong and Global Trend
- ☐ Cybersecurity Incidents
- ✓ Cybersecurity Adversaries

# Cyber Security Adversaries



- ✓ **Google** paid out **over \$10 million** in bug bounties in 2023.
- ✓ **Microsoft** paid **\$16.6 million** worth of bug bounties in 2023.

- Cyber Criminals
- Hacktivists
- Nation-state acts



Any other types of people that may present threats to a company's cyber security? – insider threats



Do you think the hackers tend to work alone or together? - together

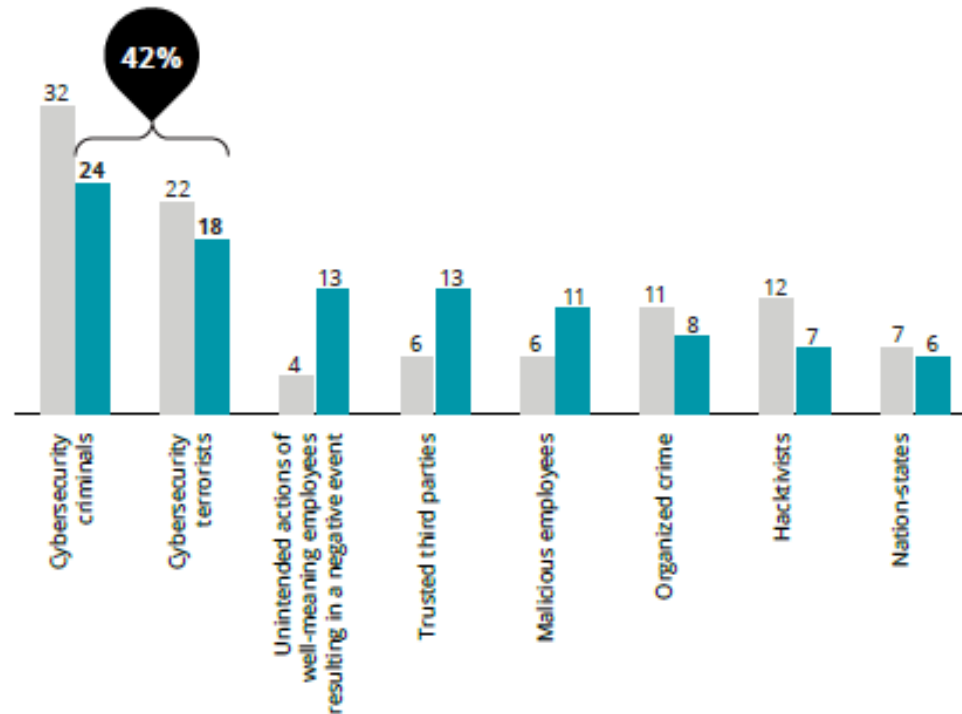
# Cyber Security Adversaries - Insider threats

## THE THREATS THAT ARE BREAKING THROUGH (FIGURE 5)

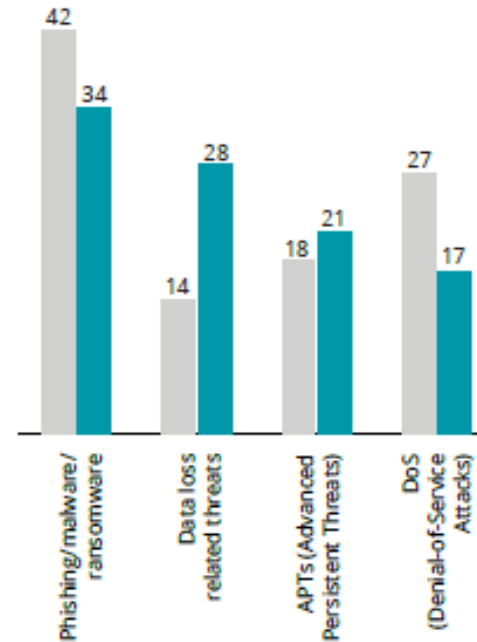
Where cybersecurity breaches are coming from—and how many organizations are experiencing them.

(Percentage, 3rd edition vs. 4th edition)

### Actors/sources



### Tools/techniques



● 3rd Edition (n=1,110) ● 4th Edition (n=1,196)

Source: Deloitte 2024

# eCrime Ecosystem

2021 Global Threat Report

CrowdStrike

31

## eCrime ecosystem

A tectonic shift toward big game hunting has been felt across the entire eCrime ecosystem. Ransom payments and data extortion became the most popular avenues for monetization in 2020.

While many established criminal actors still operate out of Russia and Eastern Europe, the complete ecosystem is truly global, with newly uncovered marketplaces arising and maturing in Latin America, Asia, Middle East and Africa.

Many criminal actors develop relationships within the ecosystem to acquire access to essential technology that enables their operations or maximizes their profits.

Although the methods used for malware distribution largely remain the same, criminal actors are finding novel ways to bypass security measures.

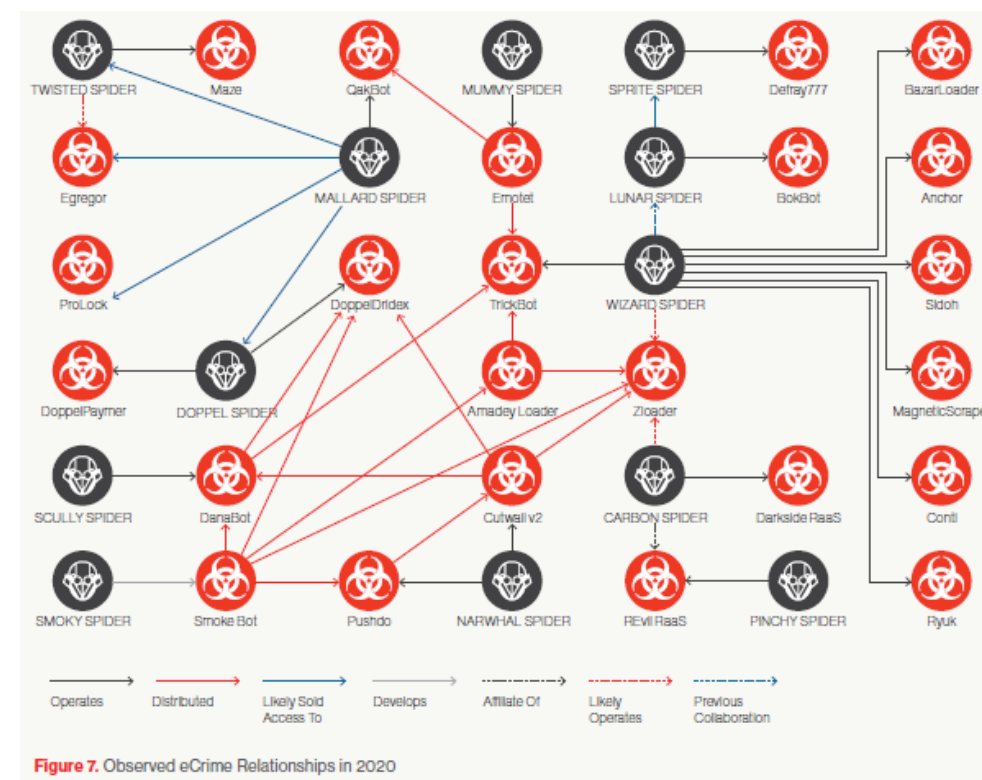
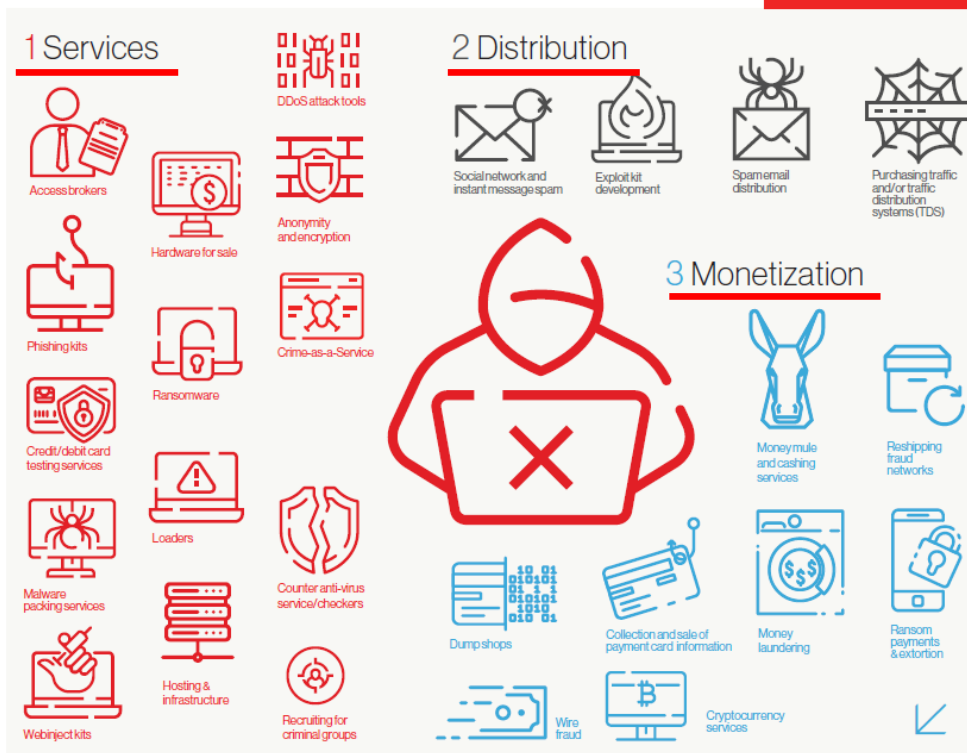


Figure 7. Observed eCrime Relationships in 2020

**Romanians100-dms**

Joined: Jun 14, 2012

Messages: 35

Reaction score: 0

Sep 6, 2012

FRS2H 400 RDP's 505\$ - VALUO RATE (200 RDP's)

Replacement Available Only in 24 Hours Not more

Zoominfo And other things I didn't checked I don't have time

200/100%

Mix Country / Bulk Selling

99% Administrator Rights

90% NO ANTI VIRUS

Local / Shares / Neighbour PCs

90% Asian Country Korea / China / HK / India . etc

Workgroup

100 \$ RDP

start 2 000\$

step 500\$

bits 4 000\$

Guarantee will always be accepted here!

SophosXOps

Fig. 3. An access broker, seeking a quick sale, touts its wares.

**VPN-RDP / TOP-EU / 5kk**

By Lumma, Tuesday at 08:45 AM in Auctions

**Lumma**

byte

Paid registration

4 posts

Joined

03/05/22 (ID: 126577)

Activity

хакинг / hacking

Posted Tuesday at 08:45 AM

Geo: EU BE Belgium

Access: VPN - RDP

Revenue: 5kk

Activity: Wholesale Industry, supply to EU, busy active company

Rights: DA Admin

AV: Bit Defender

Start: 250\$

Step: 250\$

BLTZ: 750\$

PPS: 24 hours

Дам доступ тем кто с репой или с депозитом, остальные через гарант

SophosXOps

**Helium**

Malware Services

Paid registration

68 posts

Joined

08/10/21 (ID: 119109)

Activity

выпускания / malware

Posted 16 hours ago (edited)

Our WD crypting service is one of a kind. You won't have to go through the hassle of finding a reputable crypting service any longer.

With our exclusive .bat encryption - your executable (.exe) will be transformed into a small, 6-25 kb batch (.bat) file.

This ensures the best results for manual file distribution.

Using a .bat file has many advantages over the classic .exe file.

- **Guaranteed WD Bypass**
- **Bypass ChromAlert & SmartScreen** (bypasses SmartScreen with non-passworded .zip or .rar file)
- **Easy to run** and your file will stay undetected for much longer than with a classic .exe
- **No need for an EV Signing Certificate** compared to regular .exe files

**Features:**

- Adds a **Windows Defender exclusion** for your file when ran on a computer - this way you won't lose connection.
- Loads your executable from an external host straight to the computer when the .bat file is executed.
- Your file will receive a ripped signature for further anti-detection.

SophosXOps

Fig. 8. Looking to dodge detection, a specialty service offers to turn .exe files into .bat files.

**Phider**

kalobyte

Active arbitrage

27 posts

Joined

06/24/22 (ID: 1322613)

Activity

кодинг / coder

Posted June 24 (edited)

**Every Phisher Dream**

**Hello,**

We offer our services for every phisher that want to success his campaigns. We decided to help you in creation and maintenance for your projects/campaigns with our long experience in phishing.

- We can create/clone any page
- Live panel can be done for the page
- Customizing the live panel for any feature needed
- Anti-bot system that protects the page for days and even weeks 24/7

**We can help you hosting your page on our personal servers with anti-bot and auto domain changer** with extra fees. Just relax and see your campaigns running successfully.

**Why us?**

- Client's satisfaction is our priority
- Online 24/7 hours on TG
- We deliver your project/page ASAP
- Edits are done and delivered immediately
- Any features you dream of can be implemented in your page

**Our mission?**

Simply we are created to help in carrying out your fishing projects in a professional way.

SophosXOps

**Mr.Wizard**

byte

User

19 posts

Joined

03/17/18 (ID: 86273)

Activity

кодинг / coder

Posted August 18 (edited)

**Renting a Voice SYSTEM TO RECEIVE CALLS With Live Panel to get CC + OTP.**

The victim will call the number then will follow the steps during the calls.

Also there AI system Incase your victim to speak to the bot.

All Language.

All Accent.

1 Month = \$1500 ( 1 Bank or Service ).

Guarantor Accepted ( Buyer pay the fees )

I can customize it to your needs.

Contact me to show you a demo.

SophosXOps

Fig. 9. A vishing-as-a-service offering includes "all language, all accent."

★ Spreading your Virus (Install) ★

**ZoroxPalace**

Junior Member

10

01-20-2022, 02:49 PM

Greetings,

Welcome to our new service. We are spreading your viruses/loppers (.exe) all over the world, including USA, EU, CA, AU, NZ, GB.

The virus will be spread by a webmaster.

You can specify which regions you would like to spread your virus. We can do the following regions:

(prices for 1000 downloads)

- World - 200\$
- Europe - 1500\$
- USA - 2000\$
- CA, AU, NZ, GB - 1200\$

Minimum download volume is 500.

Maximum download volume we can parse is 20.000 (more can be discussed privately)

We will provide the statistics.

Bulk orders receive good discounts.

We do not load these types of viruses: Lockers, Encryptors, Ransomware

Note for orders: Include the region you would like to spread your virus and direct link to .exe

SophosXOps

Access-as-a-service

Malware distribution-as-a-service

Phishing-as-a-service

Crypting-as-a-service

Scamming-as-a-service

Vishing-as-a-service

Spamming-as-a-service

Scanning-as-a-service

# How much do they make?

## Dark Web Price Index 2023




By Miklos Zoltan · 23 April 2023  
Founder - Privacy Affairs



Shanika W.  
Fact-Checked this

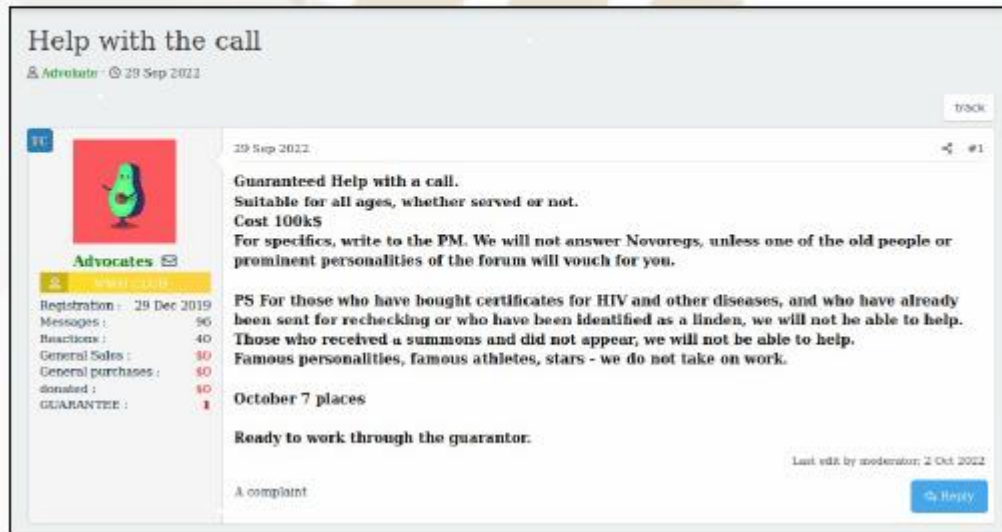
4 Comments

Category	Product	Avg. Dark Web Price (USD) 2023
Credit Card Data	Credit card details, account balance up to \$5,000	<ul style="list-style-type: none"><li>What do you think is the highest price range here?</li><li>Which one is the most expensive?</li></ul> 
	Stolen online banking logins, minimal \$2,000 on account	
	USA hacked credit card details with CVV	
Payment Processing	Stolen PayPal account details, minimal \$1,000 balance	
Crypto Accounts	Crypto.com verified account	
Social Media	Hacked Facebook account	
	Hacked Gmail account	
Hacked service	Netflix account, 1-year subscription	
	Uber hacked account	
Forged documents	New York driver's license	
Malware	Android OS per 1,000 installs	
Email database dump	10 million USA email addresses	
DDoS attack	Unprotected website, 10~50k requests per second, 24 hours	
	Premium protected website, 20~50k requests per second, 24 hours	

# How much do they make?



Figure 8: Threat actor offering a method to circumvent Russian conscription for US\$100,000



- Cyber criminals are acquiring, laundering, spending and reinvesting about **\$1.5tn** in profits a year
- Cyber criminals makes:
  - ✓ Master-level: 2~7 million
  - ✓ Mid-level: \$250k~\$900k
  - ✓ Lowest-level: ~\$50k
- Cybercrime damage expected to reach **\$8tn** in 2023

Source: Deloitte Cyber Threat Trends 2023



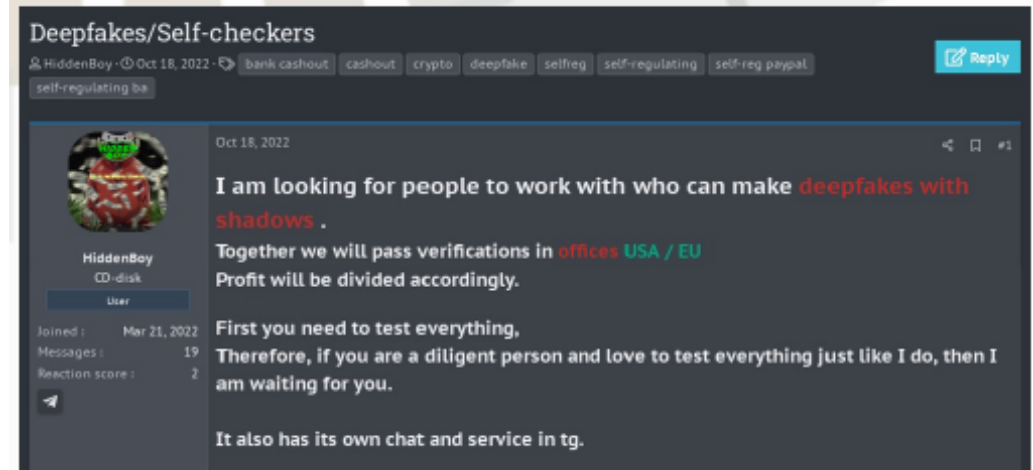
# Deepfake

A deepfake is an artificial image or video (a series of images) generated by a special kind of *machine learning* called “deep” learning (hence the name).



<https://www.youtube.com/watch?v=CDMVaQOvtxU>

**Figure 10: Threat actor seeking individuals with experience in deepfake technologies to target organizations in Europe and the United States**





# Arup's AI Deepfake Video Scam

- UK engineering group Arup, which employs about 18,000 people globally and has annual revenues of more than £2bn, **lost HK\$200mn (\$25mn)** after fraudsters used **a digitally cloned version of a senior manager to order financial transfers during a video conference.**
- According to police, the worker had initially suspected he had received a phishing email from the company's UK office, as it specified the need for a secret transaction to be carried out. However, the worker put aside his doubts after the video call because **other people in attendance had looked and sounded just like colleagues he recognized.**



# New Gold Pickaxe Malware Aims To Steal Users' Faces



- Android and iOS users. The malware lures victim users into downloading it via social engineering.
  - Threat actors impersonating government officials convince the victim to use messaging app Line to communicate and trick them into downloading a Trojan-laden app disguised as a “digital pension” application, or one providing other government services.
  - Trojan requests the victim’s ID documents and prompts the victim to record a video as a ‘confirmation method’ in the fake app. This is then used to create a deepfake video, which can be deployed in addition to the other collected data to enable a cybercriminal to bypass banking logins.

# The Defensive Side

Who would you go to if you encounter a cybersecurity related issue?

-- Security firms and related government authorities

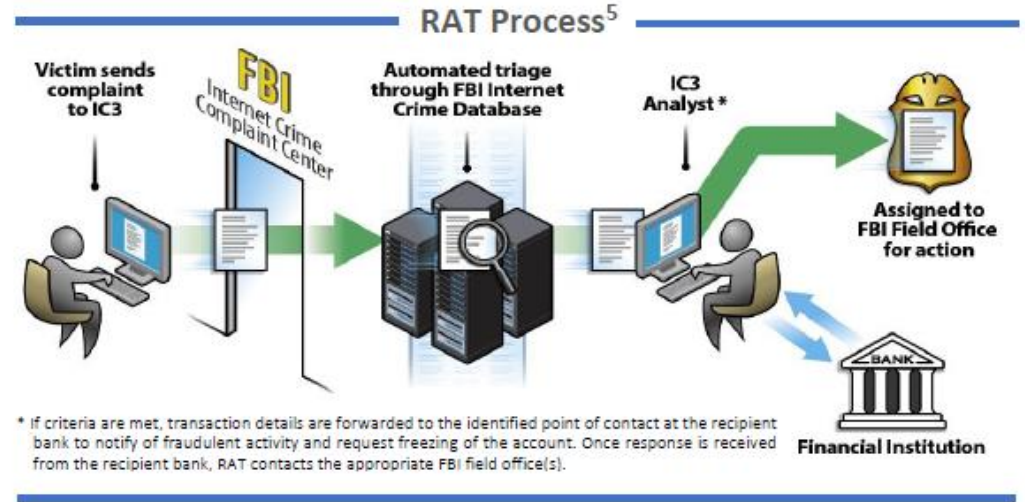


# The Government's Role

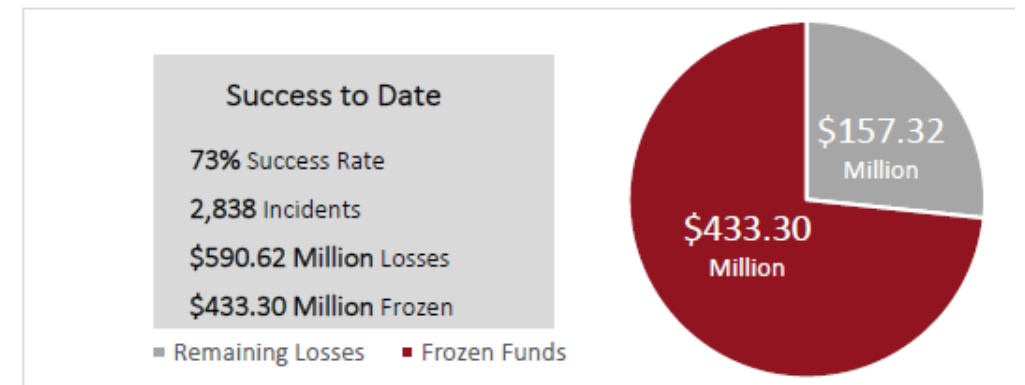
## Cyber Security and Technology Crime

### THE IC3 RECOVERY ASSET TEAM (RAT)

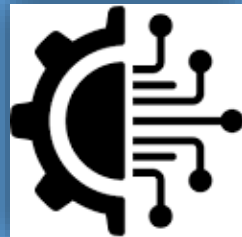
The Internet Crime Complaint Center's Recovery Asset Team (RAT) was established in February 2018 to streamline communication with financial institutions and assist FBI field offices with the freezing of funds for victims who made transfers to domestic accounts under fraudulent pretenses.



### RAT SUCCESSES<sup>6</sup>

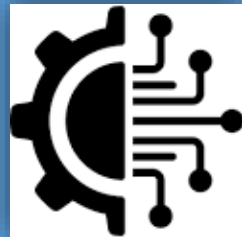


# The Defensive Side



- ☐ Damage from Cyber Attacks
- ☐ Manage Cybersecurity
- ☐ Industry Best Practice

# The Defensive Side



✓ Damage from Cyber Attacks

❑ Manage Cybersecurity

❑ Industry Best Practice

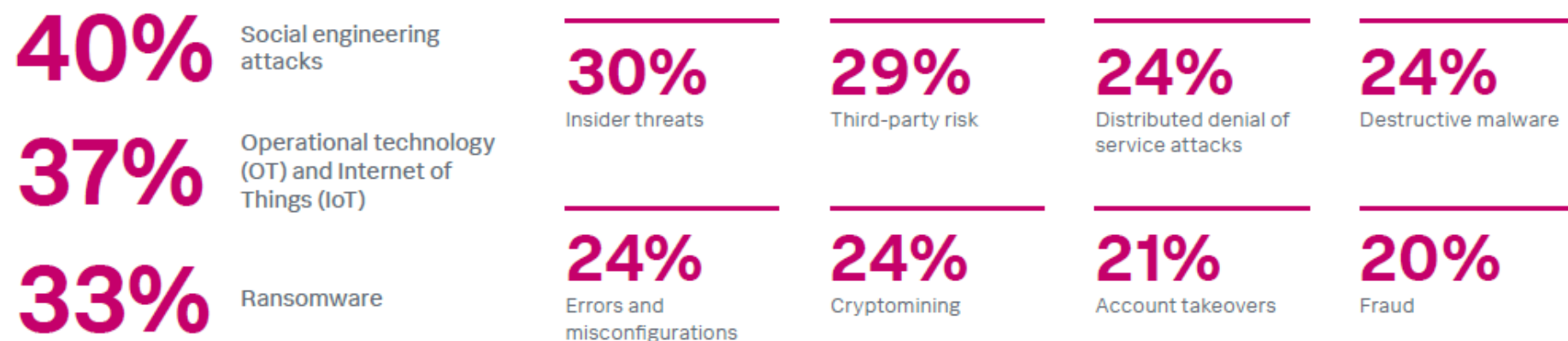
CISOs are likely going to face a major attack — *a staggering 90% reported suffering at least one disruptive attack in their organization over the last year* (43% at least once, 34% “a couple of times,” and 13% “several times.”)

It should be no surprise that social engineering, OT/IoT, and ransomware are top-of-mind concerns for CISOs — threats that are not only featured prominently in the media, but are also financially devastating. “Your decisions impact how the business runs,” says the CISO of a healthcare organization. “If you make bad choices, you might kill the business.”

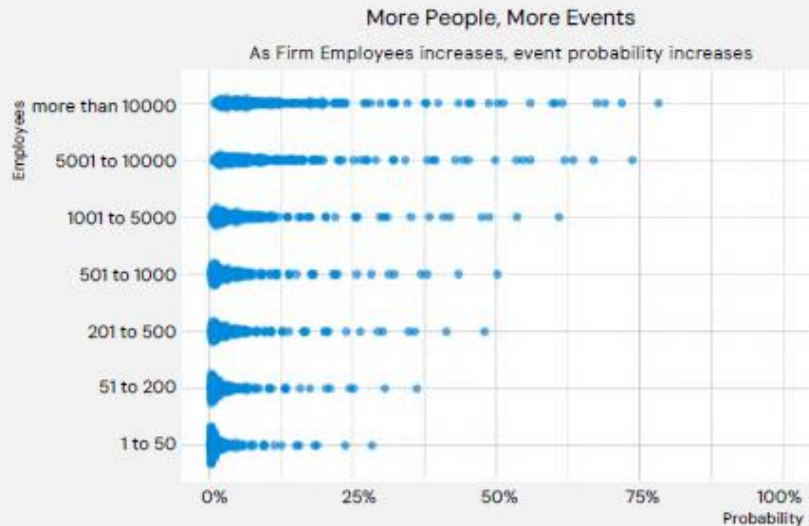
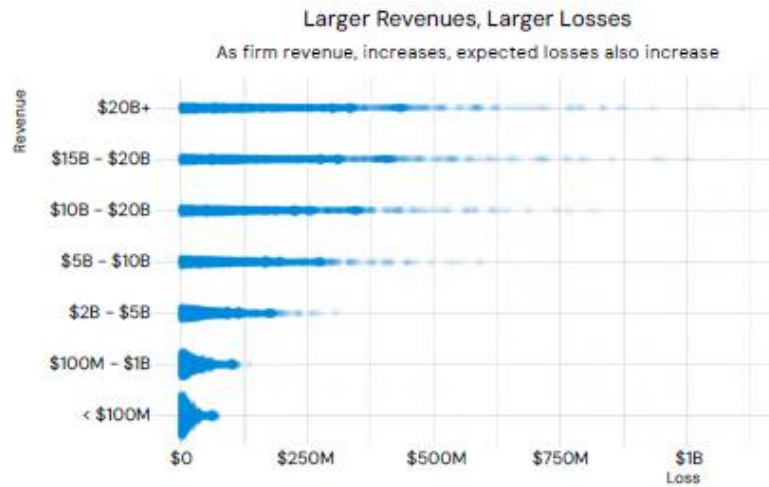


**reported at least one disruptive attack**

## Most Concerning Cyber Threats



*Image source: The CISO Report*



## Data Sources

Inputs for this simulation study incorporate security scans, events, and loss data from several industry sources in 2023, including:

- 2023 Verizon Data Breach Investigations Report (DBIR)
- VERIS Community Database (VCDB)
- SecurityScorecard
- Zywave
- St. Louis Federal Reserve Economic Data (FRED)

*Image Source: Cybersecurity Risk Report 2024 by SAFE & EY*



Industry	Loss*	Prob	Exposure
Public Administration	\$27.0M	15.8%	\$4.9M
Healthcare	\$25.3M	9.0%	\$2.7M
Educational Services	\$24.1M	5.4%	\$1.6M
Finance & Insurance	\$24.5M	3.7%	\$1.3M
Retail	\$31.0M	2.3%	\$1.1M
Accommodation & Food	\$29.7M	2.6%	\$872.1K
Professional Services	\$26.5M	2.2%	\$738.1K
Information	\$23.6M	1.9%	\$639.3K
Manufacturing	\$31.7M	1.3%	\$632.6K

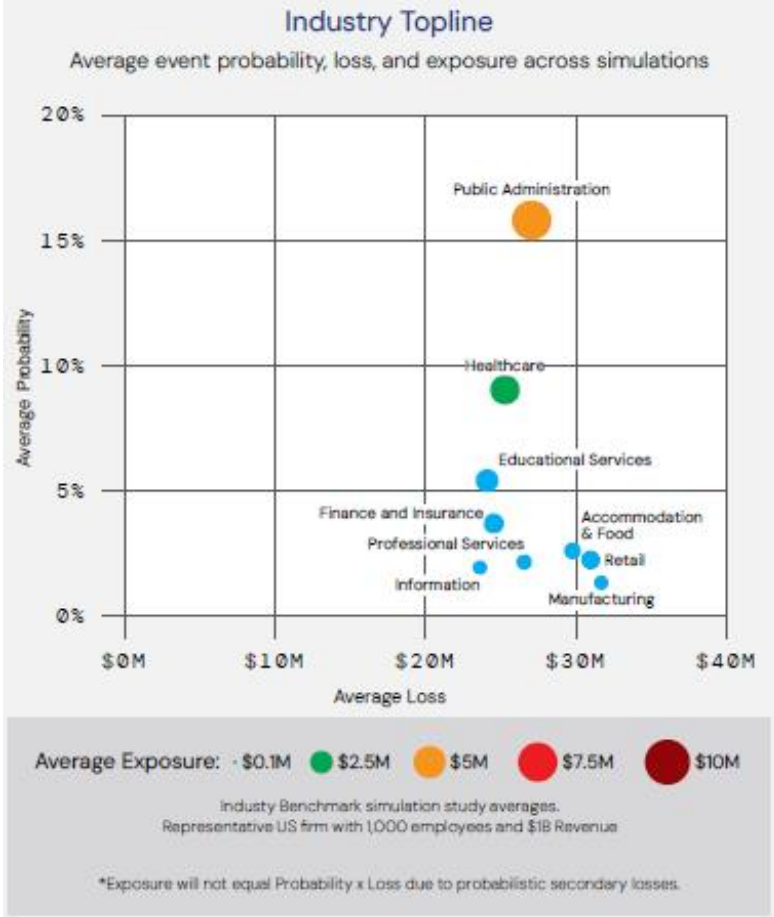
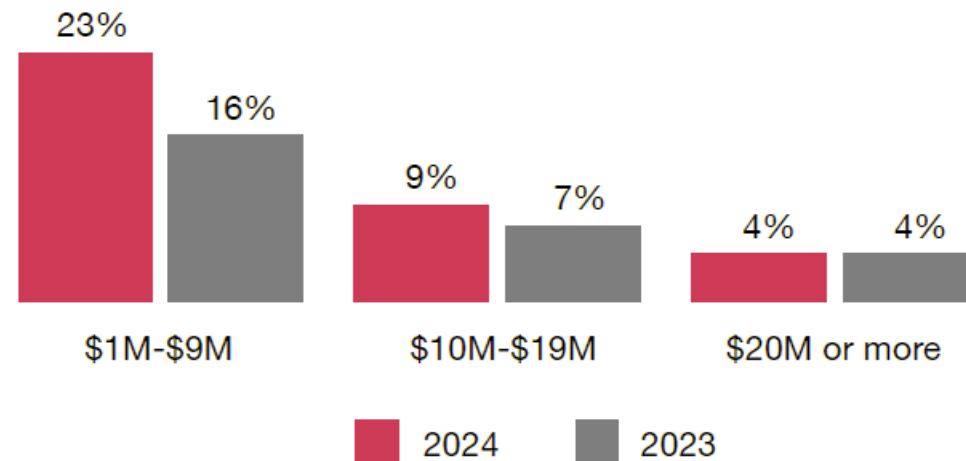


Image Source: Cybersecurity Risk Report 2024 by SAFE & EY

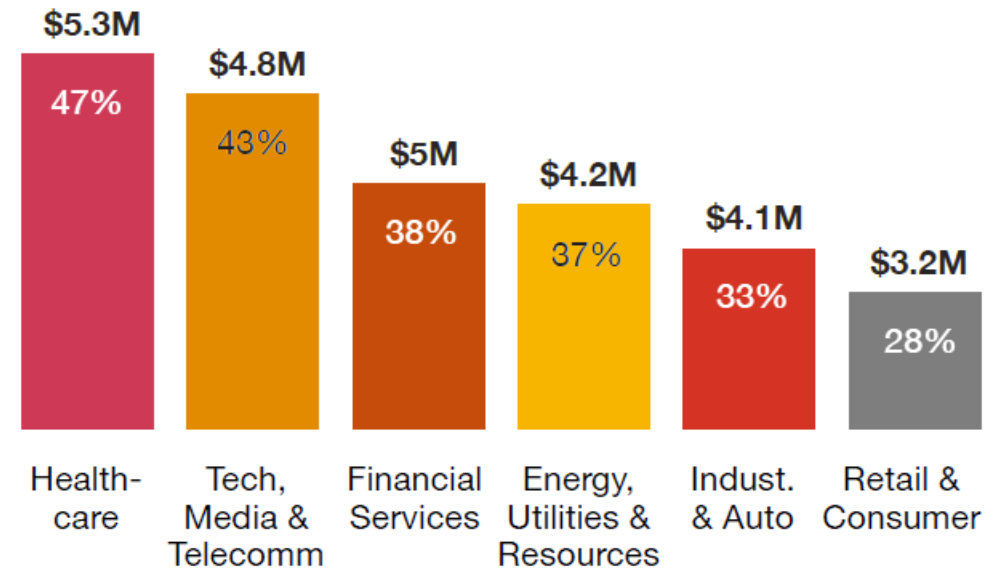
## Breaches are becoming more costly

### Estimated costs to organisations' most damaging data breach in the past three years

Percentage who say they had a \$1M+ breach:  
2024 total = 36%, 2023 total = 27%



### Average cost of breach in millions and percentage of most damaging breaches that cost \$1 million or more, by sector



Q5. Thinking about the most damaging data breach you experienced in the past three years, please provide an estimate of the cost to your organisation. Base: Security and IT and CFO respondents= 1651  
Source: PwC, 2024 Global Digital Trust Insights.

Image source: PWC

## Ransomware: Attackers get a payday

All but 4% of our respondents report suffering a ransomware attack, with 52% experiencing one that significantly impacted their business systems and operations.

While 96% is significant, prepare yourself — **83% of those who answered said they paid the ransom.** Of those who paid, 18% paid the ransom directly, 37% paid through cyber insurance and 28% paid through a third party.

And it's not cheap. The most significant number paid somewhere between \$25,000 to \$99,999 (44%), while more than half of respondents paid more than \$100,000, a stunning 9% of respondents (or one in 11) paid \$1 million or more. That's a lucrative business for ransomware gangs — and many desperate organizations gamble with their reputations in the hope of decrypting their data, recovering their systems and preventing the release of sensitive material.

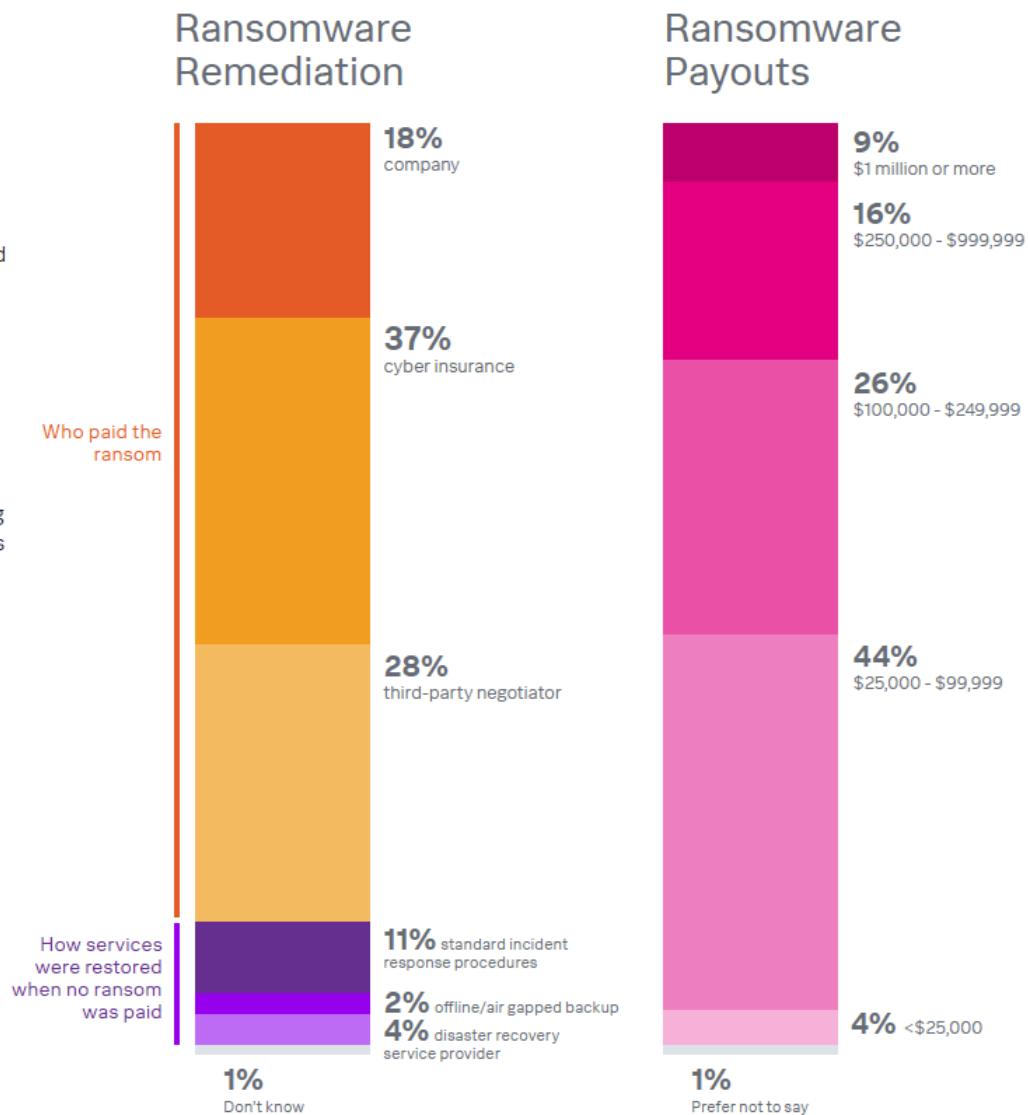


Image source: The CISO Report

# “How material is that hack?”

In **Dec 2023**, the Securities and Exchange Commission (SEC) issued new rules, mandating disclosure of material cyber incidents **within four days** from the moment that materiality was determined and disclosure of ongoing processes to manage cybersecurity risk. It was a powerful signal to public companies to improve their cyber risk reporting practices.

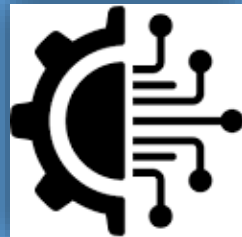
*“Sometimes it takes the forcing function of a regulation to help mature key business practices and help turn what was an ‘art’ into a ‘business science.’ This feels like one of those moments for cyber risk management. And one when the greater transparency and accountability will greatly help improve our cybersecurity posture as a nation.”*

Nicola (Nick) Sanna  
FAIR Institute Founder  
on the effects of the new SEC rule<sup>2</sup>

*Source: Cybersecurity Risk Report 2024 by SAFE & EY*

<https://howmaterialisthathack.org/>

# The Defensive Side



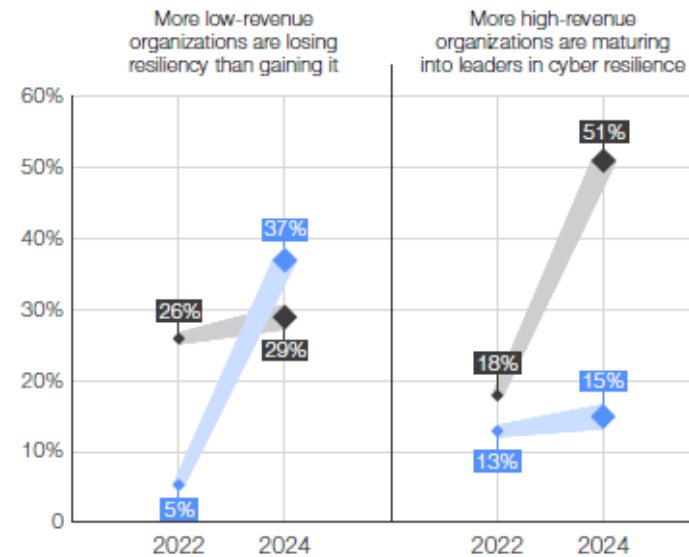
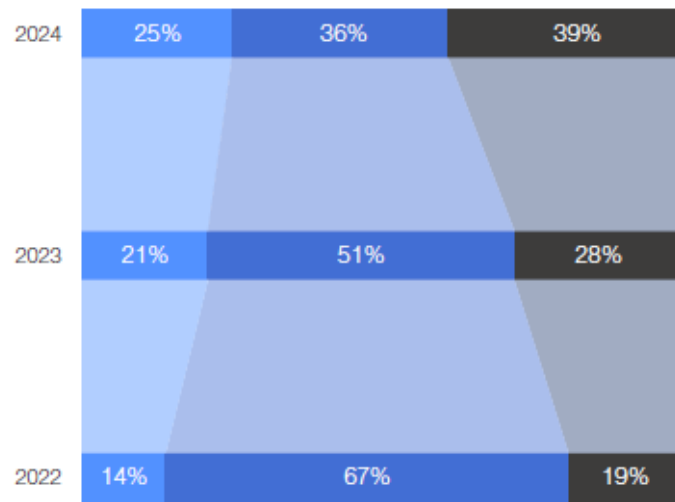
- ☐ Damage from Cyber Attacks
- ✓ Manage Cybersecurity
- ☐ Industry Best Practice



90% of cyber leaders who attended the Annual Meeting on Cybersecurity believe that inequity within the cybersecurity ecosystem requires urgent action.

There is growing cyber inequity between organizations that are cyber resilient and those that are not

What is the state of your organization's cyber resilience this year?

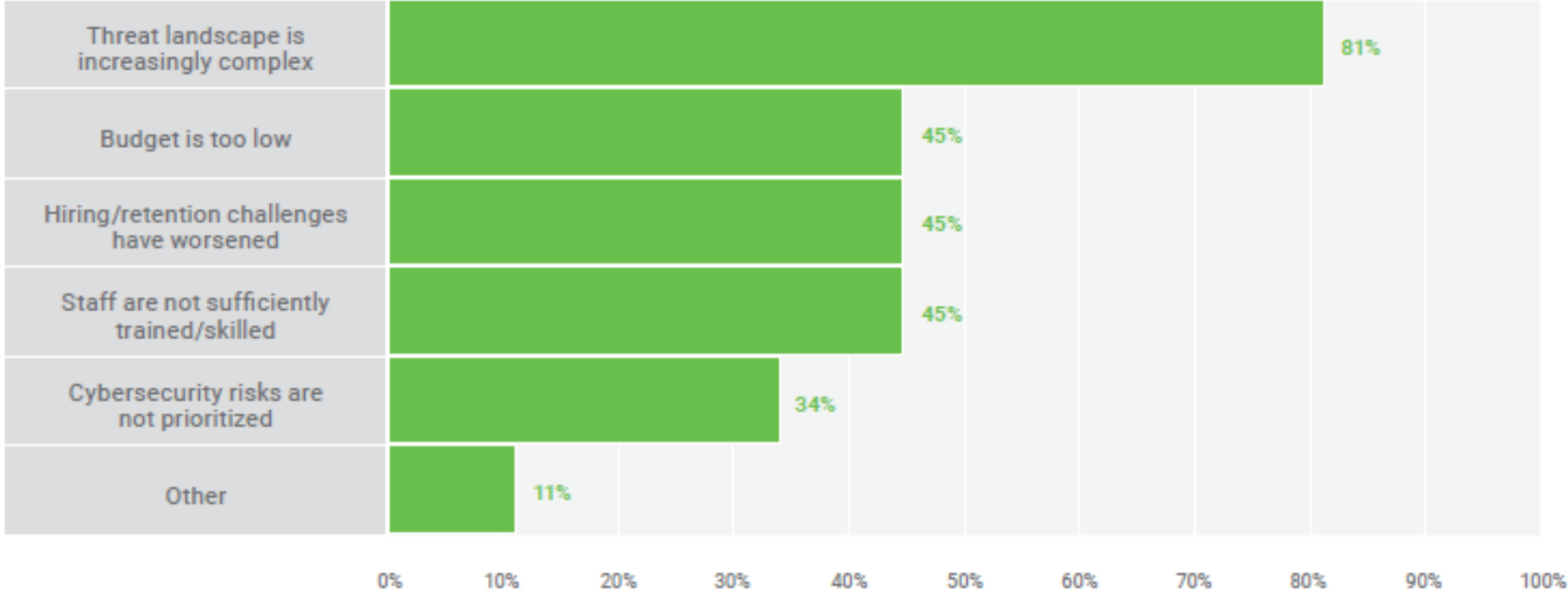


● Our cyber resilience is **insufficient**
● Our cyber resilience meets **minimum requirements**
● Our cyber resilience **exceeds** our requirements

Image Source: World Economic Forum

**FIGURE 7: Sources of Stress**

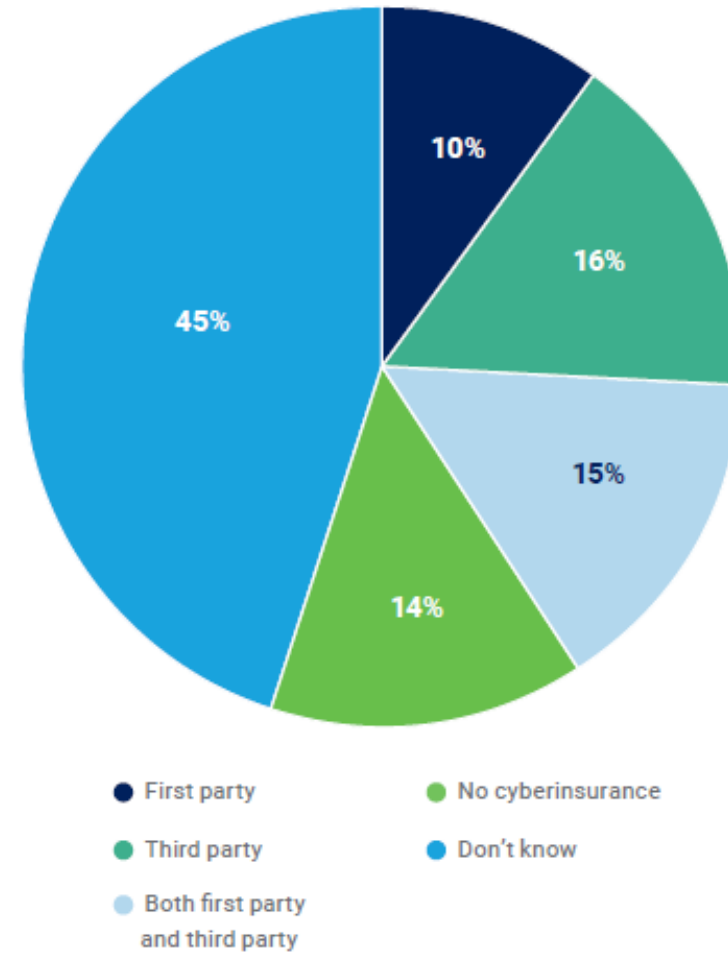
Please tell us why your role is more stressful today than it was 5 years ago.



*Image source: ISACA*

**FIGURE 38:** Cyberinsurance Type

What kind of cyberinsurance, if any, does your organization carry?



*Image source: ISACA*



We found that on average, overall respondents are spending between US\$147 million and US\$266 million annually on IT. Of that, 19% (US\$39 million) is allocated for cybersecurity related activities, and respondents expect to increase that by 3% in the next 12-24 months.



Image source: Deloitte

Ninety-three percent of organizations actually expect to increase cybersecurity spending, either significantly or somewhat, over the next year. This is great news for security teams, as 85% percent of CISOs say a reduction in spending would hamper their ability to respond to threats, and 80% say they have noticed that their organization has faced a growing number of threats coinciding with the declining economy.

Yet 83% of CISOs see the cuts in other parts of their organization, and 85% say that they're worried about the macroeconomic uncertainty and its potential impact on their team.

Almost a third (31%) say that projects have been delayed or eliminated due to a lack of funding. While 87% say they've demonstrated a business case for increased budget year-over-year, only 35% say that their boards allocate adequate

cybersecurity budgets. With security budgets expected to rise, there's reason to be optimistic. However, despite increased investment, the additional funding is still not enough for many CISOs wrangling their technical debt.

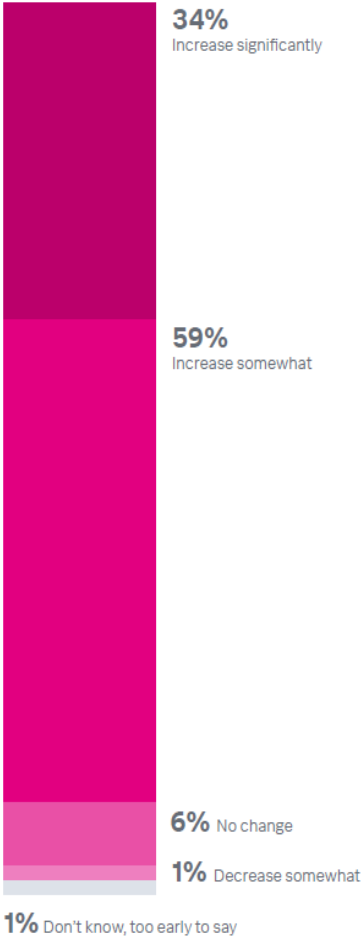
We saw CISOs are justifying ROI for security investments to the board, and some of them have a focus on tool sprawl. The vast majority (88%) say they see a need to rein in security analytics and operations tools with solutions like SOAR, SIEM and threat intelligence, to address issues of tool sprawl and complexity, with only 2% disagreeing that they need to consolidate their tools. This is a message that always lands well with a CFO — and helps to justify ROI.



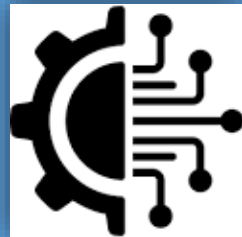
“My CFO has said my budget will always be sufficient ... as long as I can justify funding, then I will get it.”

— CISO, banking industry

### 2024 Cybersecurity Spending



# The Defensive Side



- ☐ Damage from Cyber Attacks
- ☐ Manage Cybersecurity
- ✓ Industry Best Practice

# For Organizations: Cybersecurity used to be an afterthought...

60%

organizations do not have a head of cybersecurity who sits on the board or at executive management level.

59%

of organizations say that the relationship between cybersecurity and the lines of business is at best neutral, to mistrustful or non-existent.

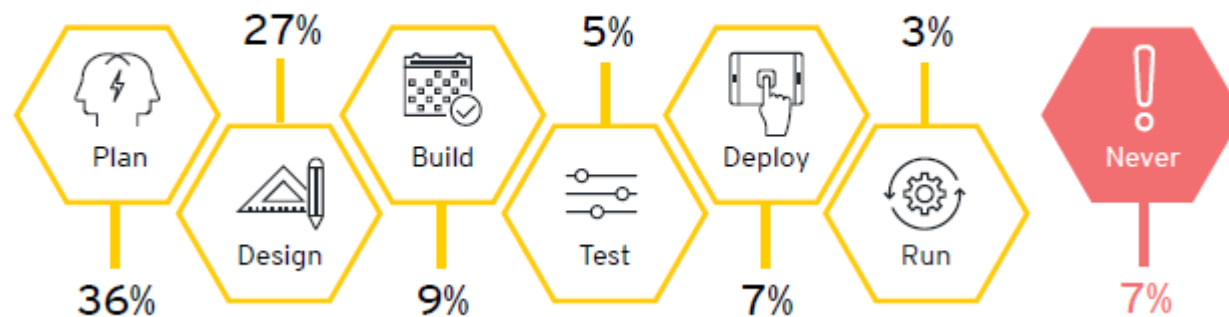
Only  
36%

of organizations say cybersecurity is involved right from the planning stage of a new business initiative.

Only  
7%

of organizations would describe cybersecurity as enabling innovation; most choose terms such as "compliance-driven" and "risk averse."

When are cybersecurity teams joining new business initiatives?



EY Global Information Security Survey 2020

65%

of businesses only consider cybersecurity after it's already too late – reveal 1,300 cybersecurity leaders.

# For Organizations: Things are changing...

## Security by design

“We’re actually investing in what we call ‘secure by design’ to make sure that security is one of the many elements of our value proposition. We are investing in policies, tooling, and controls across the software and product lifecycles to ensure we are creating great—and secure—technology. Our customers expect it.”

—Allan Cockriel, Group CIO/CISO, Shell

---

# 400%

Building customer trust affects partners and improves market capitalization, with trusted companies ultimately outperforming their peers.

“

The big shift for us is by bringing in the security discussion **before, not after**, building the solution. We really want to move into ‘**security by design**’ as opposed to what often happens—‘**security during assessment**’—which requires security to be more of **a strategic part of the overall business.**”

—Director General, Cyber and IT Security,  
Government and Public Services Agency

“

For our group, which operates globally, strengthening security is a crucial activity that is essential for promoting **digital transformation**. We have established an internal structure called the **JFE-Security Integration and Response Team**, allocating resources such as budget and personnel, and implementing necessary measures in terms of human, technological, and physical aspects. We aim to **enhance cybersecurity measures in various business activities**, including the development, design, manufacturing, and provision of products, systems, and services. As a result, we contribute to strengthening cybersecurity throughout the **supply chain** and, ultimately, to the overall cybersecurity enhancement of society on a global scale.”

—Akira Nitta, Chief Information Security Officer, JFE Steel

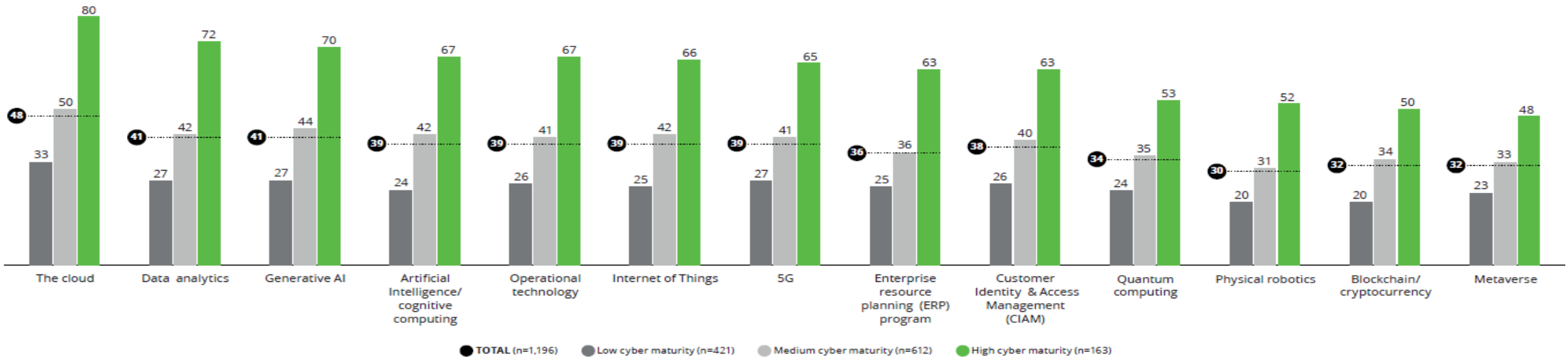
*Image Source: Deloitte 2023, 2024*

Respondents in high-cyber-maturity organizations anticipate almost **two times** the positive business outcomes compared with their peers.

- The C-suite and board have higher ability to navigate cybersecurity
- More adept at leveraging cybersecurity to secure investment for technology capabilities
- CISOs more likely to be brought into strategy conversations about technology capabilities

#### GREATER MATURITY MEANS A GREATER ROLE FOR CYBERSECURITY IN TECH-DRIVEN CAPABILITIES

(FIGURE 19)



## 9 degrees of separation: Top performers vs the rest

### Top 5% are:



**6x more likely** to have already implemented **transformative cybersecurity initiatives** from which they are **realising benefits**.



**5x more likely** to be very satisfied with their current cyber technology capabilities.



**4x more likely** to be **continually updating their risk management plan** to mitigate cloud risks.



**9x more likely** to be mature in their **cyber resilience practices**.

Source: PwC, 2024 Global Digital Trust Insights.

### Top 5% are more likely to:



**Invest more into cyber budget**, with **85% increasing their cyber budget in 2024** (vs 79% overall), of which 19% are increasing cyber budget in 2024 by 15% or more, compared to 10% overall.



Say their **most damaging cyber breach** in the last three years cost them less than \$100k (28% vs 19% overall).



Strongly agree their **organisation will develop new lines of business using generative AI (GenAI)** (49% vs 33% overall).



**Plan to deploy GenAI tools** for cyber defence (44% vs 27%).



**Disagree** that 'GenAI will lead to a catastrophic cyber attack' (33% vs 22% overall).

Image Source: PWC 2024

# Example

- For example, heightened security risks led **one retail giant** to pursue a cyber reform initiative that **enhanced value** beyond **reduced vulnerability**. This included:
  - More efficient technology spending
  - Removal of obsolete and redundant tools
  - Optimized manpower and refined roles and responsibilities
  - More efficient collaboration
  - Strengthened **trust** in its over **one-billion-strong customer base**

*Image Source: The EY 2023 Global Cybersecurity Leadership Insights Study*



# Job Demand





# Digital Technology

Office of the Government Chief Information Officer (OGCIO)

## Cyber Security – Challenges

# New MSc. In Information and Cyber Security

- Increasing reliance on technology & rise in cyber security incidents

➤ Need for well-trained cyber security professionals

Only 1.4% of IT employees in Hong Kong (i.e. 1,587) specialised in IT security in 2022

➤ With 4.9% full-time vacancies

- Shortage of cyber security professionals - a global issue

(2023 ISC2 Cybersecurity Workforce Study)

➤ Estimated global cyber security workforce at ~5.5 million

➤ With ~4 million global cyber security workforce gap

- For Hong Kong to meet its cyber security challenges

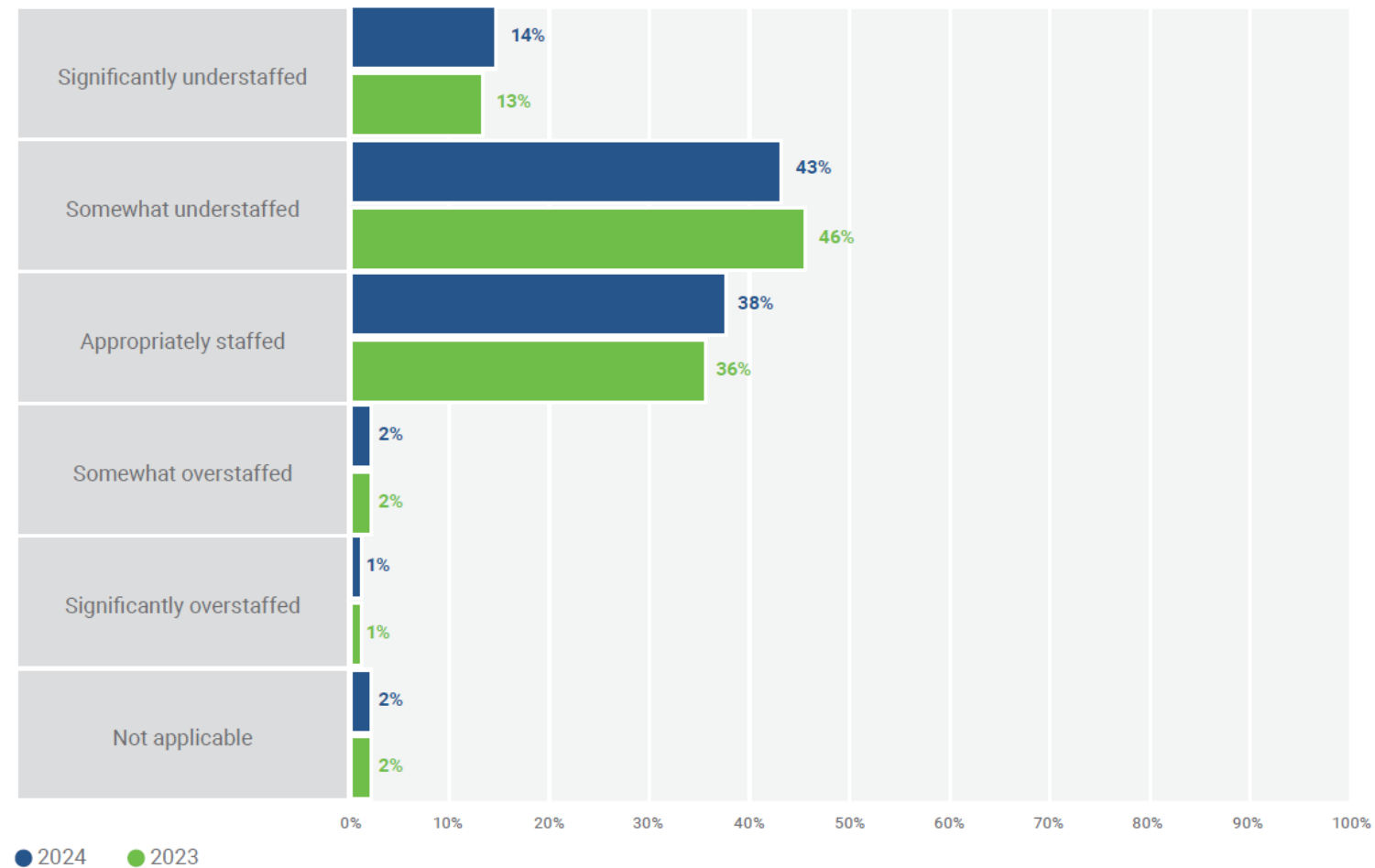
➤ Nurture home-grown talent through education

➤ Promote digital skills

# Cybersecurity Talent Shortage

**FIGURE 4:** Cybersecurity Staffing

How would you describe the current staffing of your organization's cybersecurity team?



*Image source: ISACA*

# Cybersecurity Talent Shortage

The cyber skills and talent shortage continues to widen at an alarming rate

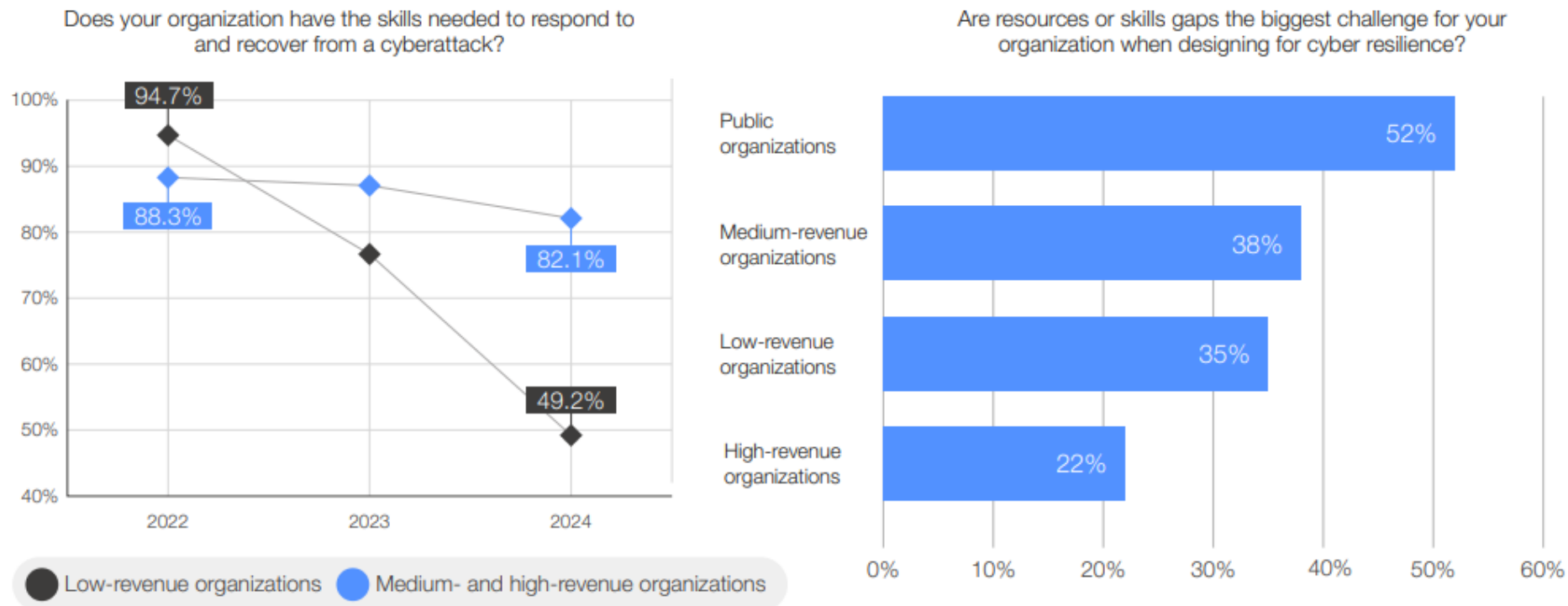


Image Source: Global Cybersecurity Outlook 2024 by WEF

# Talents That Organizations Look for

FIGURE 23: Top Five Security Skills

Please choose the top five most important security skills needed in your organization today.

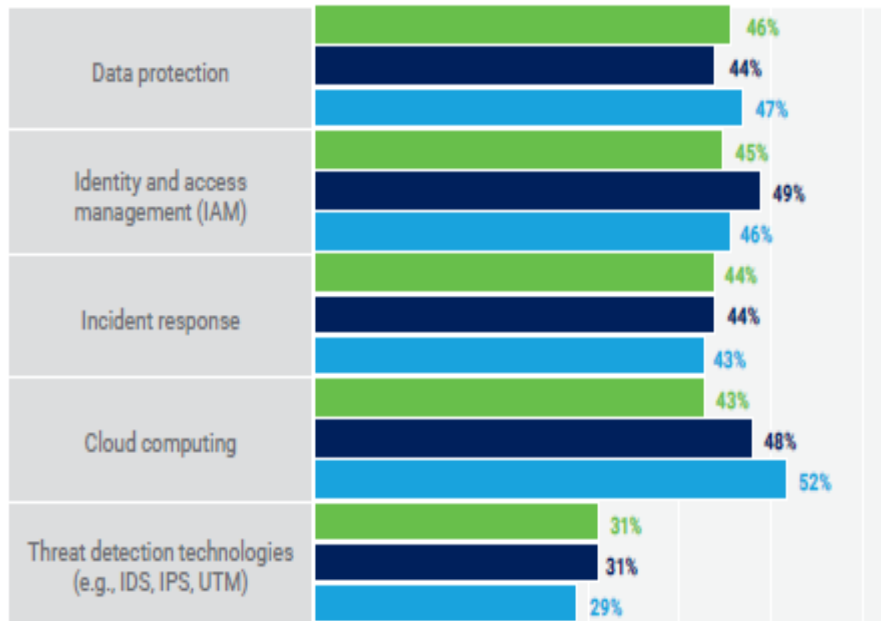


FIGURE 24: Top Five Soft Skills

Please choose the top five most important soft skills needed by security professionals in your organization today.

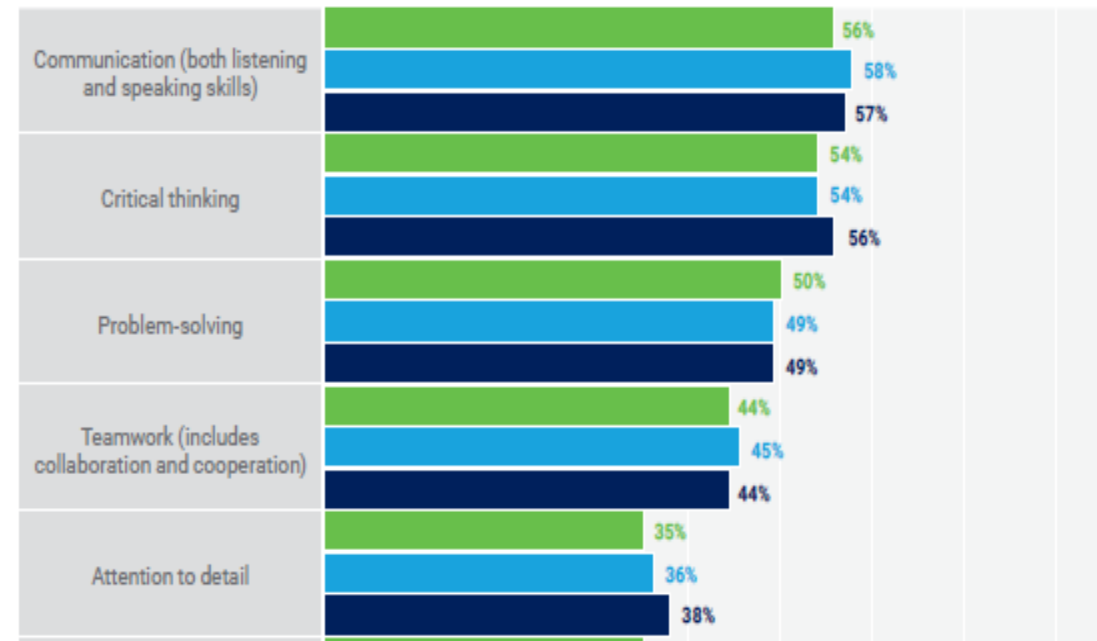


Image source: ISACA

# Popular Certificates

- Entry-Level
  - Certified Information Systems Auditor (CISA) – ISACA/HK Chapter
- Advanced-Level
  - Certified Information Security Manager (CISM) – ISACA/HK Chapter
  - Certified Information Systems Security Professional (CISSP) – ISO/US/UK
  - National Institute of Standards and Technology (NIST) - US/Federal
- Technical
  - Certified Ethical Hacker – EC-Council
  - Council of Registered Security Testers (CREST) - UK

# Food for thought 1:

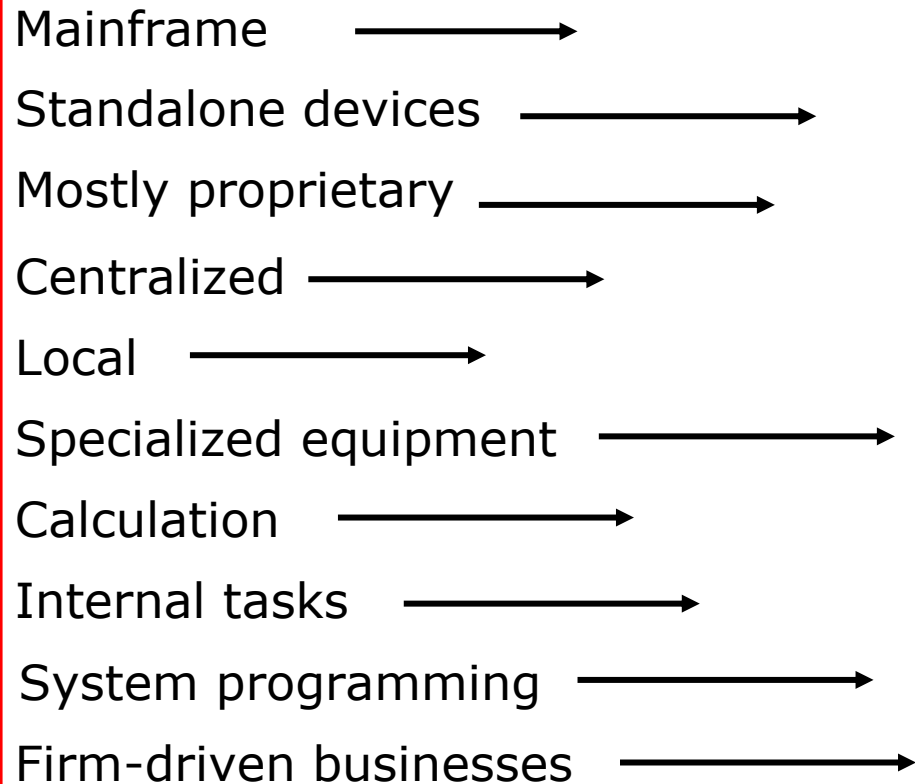
- With the fast-growing technologies from both the offensive and the defensive side, do you think there will be more security breaches or less? And why?
- - Like to be more as more is at stake.



# Food for thought 2:

- How do trends in the computing Industry impact the cybersecurity horizon?
  - Refer to handout

# Trends in the Computing Industry

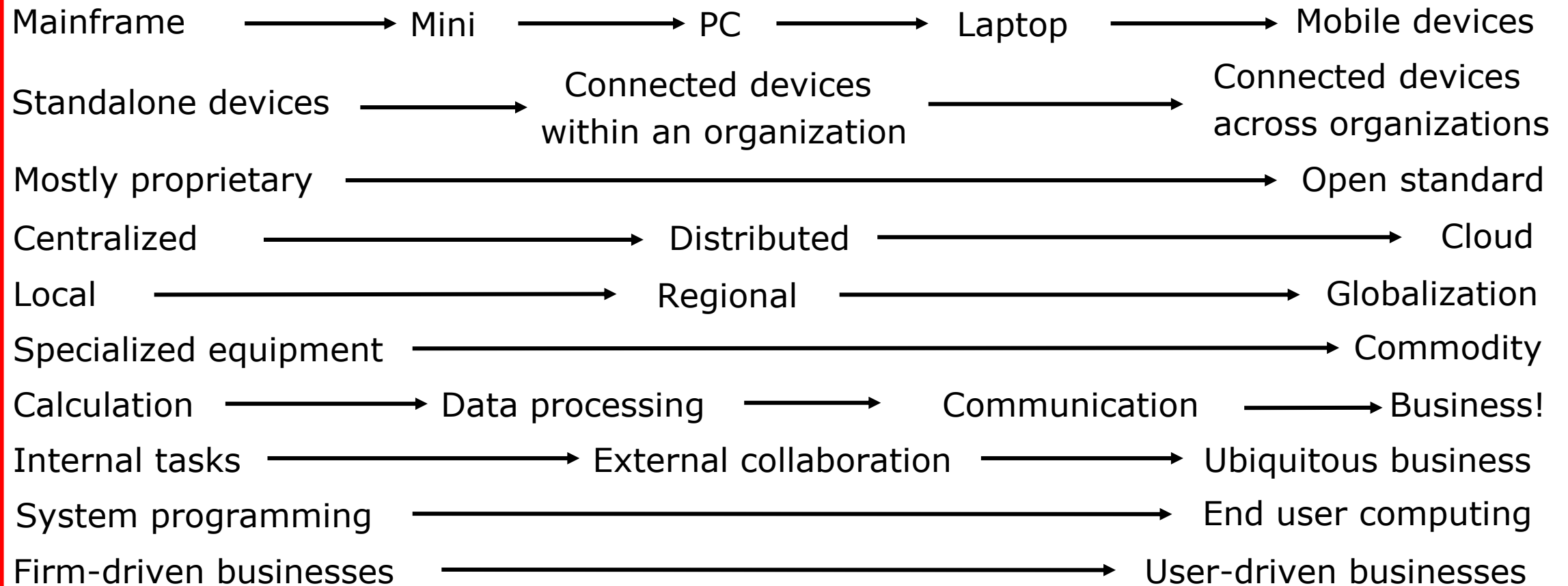


Mainframe →  
Standalone devices →  
Mostly proprietary →  
Centralized →  
Local →  
Specialized equipment →  
Calculation →  
Internal tasks →  
System programming →  
Firm-driven businesses →

How are they related to computer and Internet security?



# Trends in the Computing Industry



## Food for thought 3:

- Is cybersecurity more of a technical issue or a business decision?
- - As a business decision first, then technical decisions.