

Threat and Tech Trend in Cybersecurity

Abbas Kudrati
APAC Chief Cybersecurity Advisor
Abbas.Kudrati@microsoft.com
<https://aka.ms/abbas>



About me

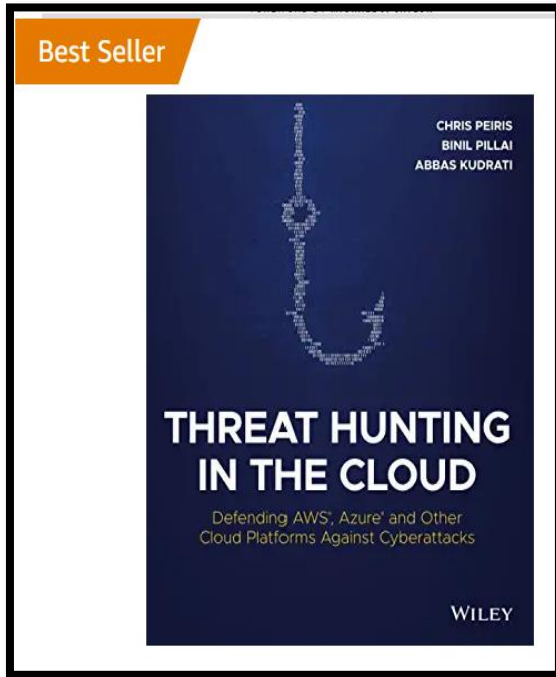
"You join Microsoft, not to be cool
but to make others cool"

Satya Nadella

- **Cybersecurity practitioner and CISO with 25 years of experience in Information / Cybersecurity.**
- **Part time Cybersecurity Professor with Deakin and LaTrobe University in Melbourne, Australia.**
- **Expertise in Zero Trust, Cybersecurity Strategy, Security Operations, Risk, Compliance, Cloud Security and Architecture.**

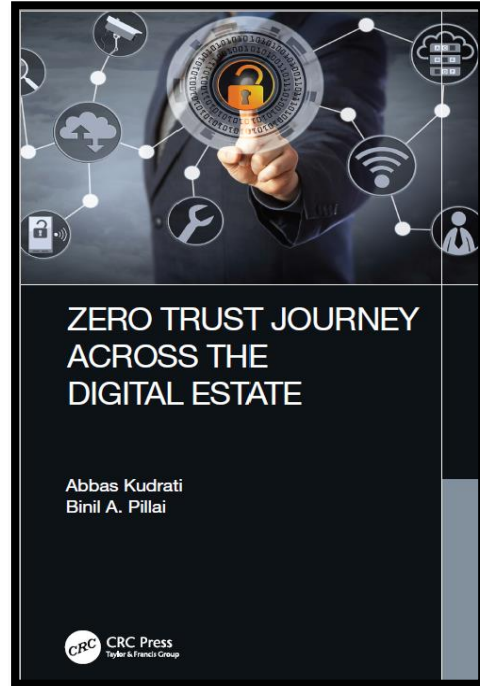


My Publications

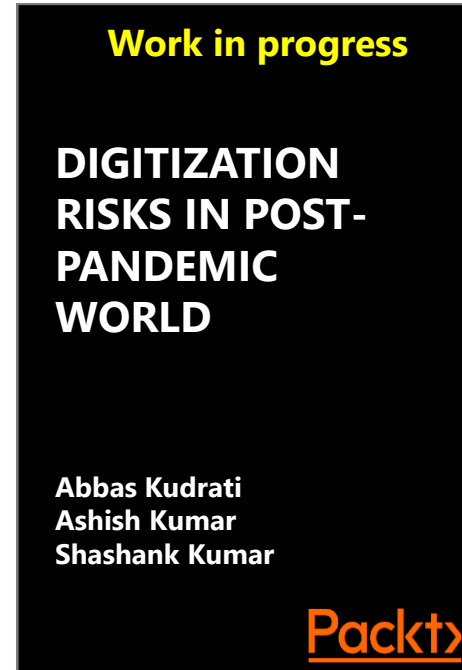


[Get it on Amazon](#)

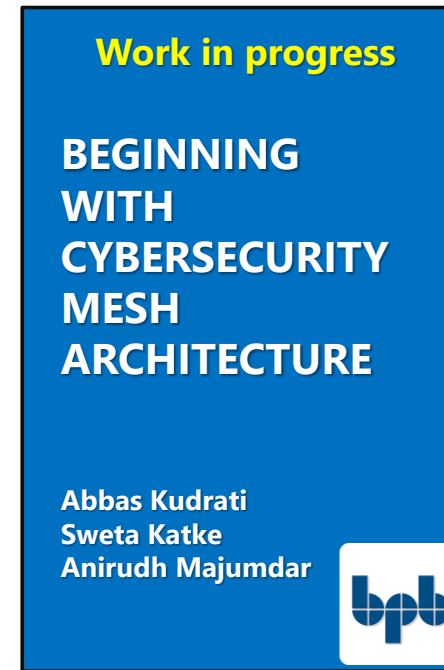
Or send me a request for a free
copy



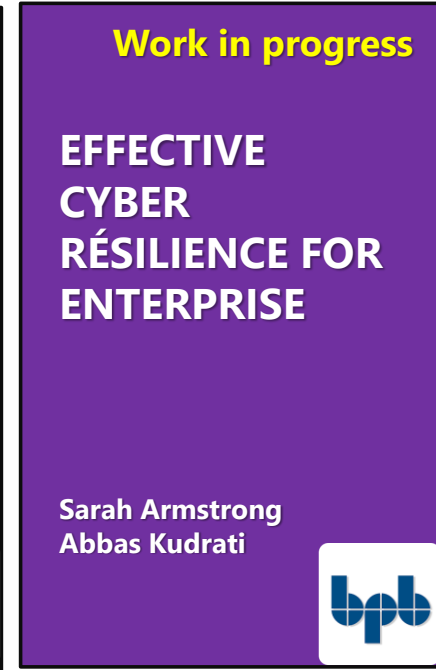
[Pre order on Amazon](#)



Releasing soon by Oct
2022



Releasing soon by Dec
2022



Releasing soon by Oct
2022

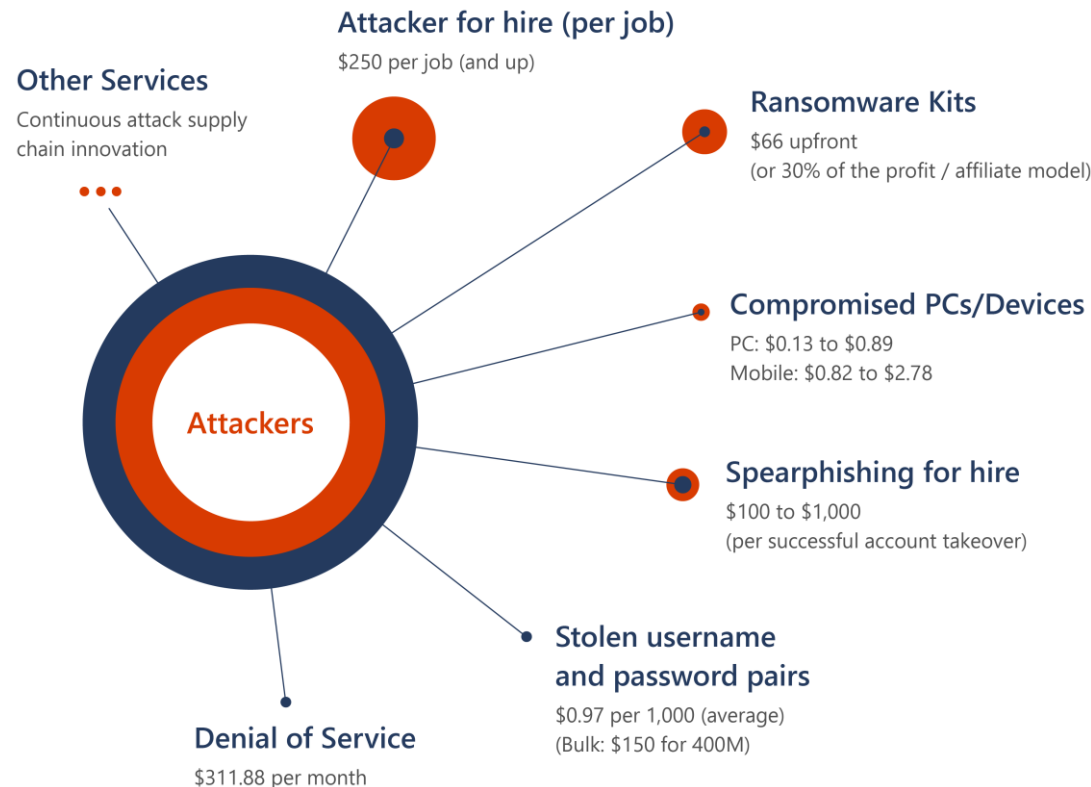
The growing threat of cybercrime

- A threat to national security
- Cybercriminals attacking all sectors
- Ransomware attacks increasingly successful
- Cybercrime supply chain continues to mature

POSITIVE TRENDS

- Transparency: governments and companies coming forward
- Priority: new laws, task forces, resources, partnerships

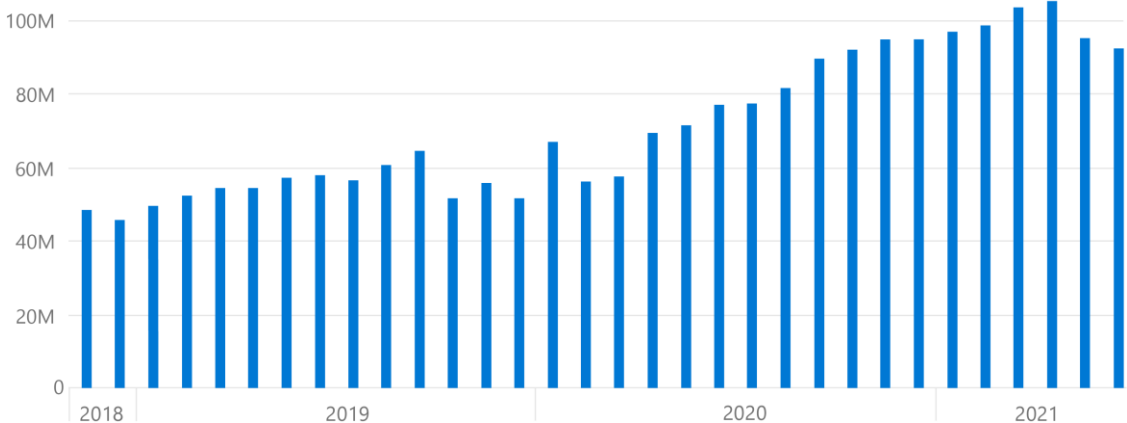
The cybercrime economy and services



WITH NO TECHNICAL KNOWLEDGE OF HOW TO CONDUCT A CYBERCRIME ATTACK, AN AMATEUR THREAT ACTOR CAN PURCHASE A RANGE OF SERVICES TO CONDUCT THEIR ATTACKS WITH ONE CLICK.

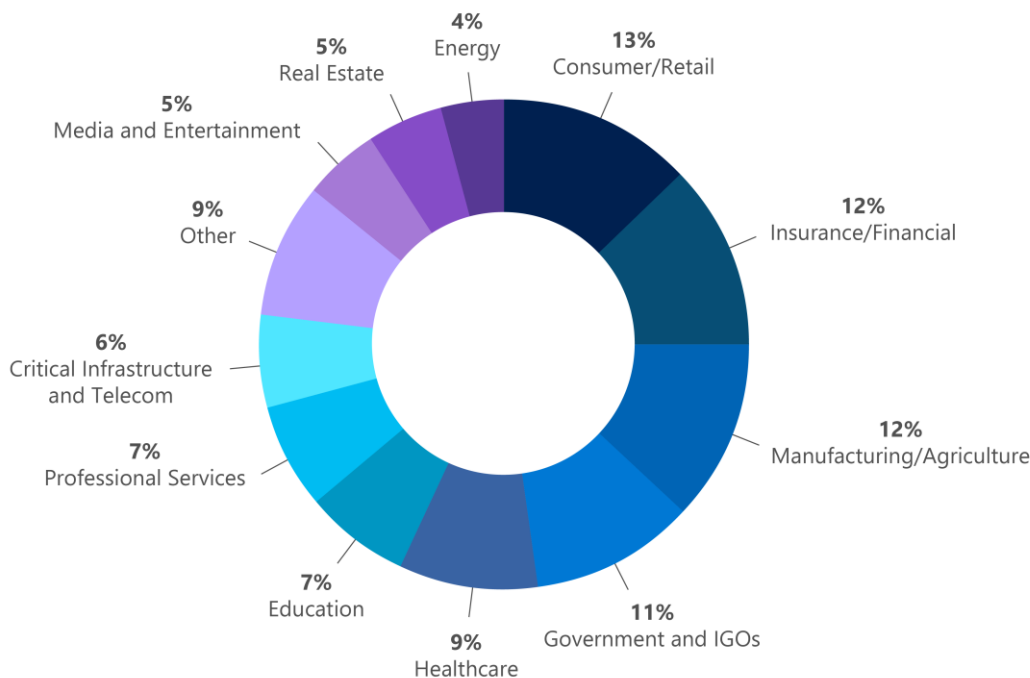
What we're seeing in ransomware data and signals

Ransomware encounter rate (machine count): Enterprise customers (Defender data)



Overall increase in ransomware encounters, with notable surge to consumer and commercial encounters in late 2019,6 when RaaS started to grow, and in early 2020 at the onset of the COVID-19 pandemic.

DART ransomware engagements by industry (July 2020-June 2021)



Deploy ransomware protection

- 1 Prepare a recovery plan**
Recover without paying
- 2 Limit the scope of damage**
Protect privileged roles
- 3 Make it harder to get in**
Incrementally remove risks

The stakes have changed. There is a massive growth trajectory for ransomware and extortion.

All types of businesses are being targeted

"Over 1700 Organizations...
attacked by #Ransomware groups."

twitter.com/darktracer_int

	Ransomware Group	Victim	Ransomware Group	Victim	Ransomware Group
4datanet.com	MAZE	Fresh Water Systems	MAZE	https://prakhinlaw.com/	NetWalker
4th Judicial Distr	MAZE	Fuel Transport	MAZE	https://www.redplanethotels.com/	NetWalker
Aban Offshore	MAZE	Furniture Row & Visser Precision	DoppelPaymer	Hustech Installations AG hustech.ch	Sodinokibi (REvil)
Action for a Better	DoppelPaymer	Fusion Connect, Inc.	MAZE	HYMAN GROUP COMPANIES	Sodinokibi (REvil)
Actuaries and As	MAZE	GAM - https://gamrentals.com	NetWalker	IBMC College	DoppelPaymer
Adam Kutner Ca	DoppelPaymer	GAR Equipment	Conti	ICM - International Commerce & Market	DoppelPaymer
Adams County M	MAZE	GCL System Integration Technology Co	MAZE	IHI-CSI.DE	CL0P
Adif (adif.es)	Pysa	Geidi.com	Sodinokibi (REvil)	Illinois Valley Community College	Pysa
Aebel	DoppelPaymer	Genesis Products Inc.	Sodinokibi (REvil)	Image one - https://i1ind.com/	Conti
Affordable Urgen	DoppelPaymer	Gestoria Auto Gestion	Conti	INDIABULLS.COM	CL0P
AFPA	MAZE	Ghantoo Group	MAZE	Indian River Transport Ltd.	MAZE
Agromart Group	MAZE	GILMER - Independent School District	AKO	Indocoo Remedies Ltd	Nefilim
Agrosuper	NetWalker	Global Union Canada	Suncrypt	Information Connectivity Solutions Lim	MAZE
Ahmed Almazrou	Sodinokibi (REvil)	Go West Tours	DoppelPaymer	Innotech-Execaire Aviation Group	MAZE
Aigües de Terras	Nefilim	GOODMANMINTZ	Sodinokibi (REvil)	Innovex	MAZE
Alaska General S	Sodinokibi (REvil)	Goodwill Industries of Kanawha Valley	DoppelPaymer	INRIX.COM	CL0P
ALFANAR - https	Sodinokibi (REvil)	greatnortherncorp.com	Sodinokibi (REvil)	insport.com.au	Sodinokibi (REvil)
Alliance Sonae	Conti	Greenville Technical College gvltec.edu	Avaddon	Instituto Costarricense de Acueductos y	MAZE
Allard	MAZE	Groupe Cactus	Sodinokibi (REvil)	Integrity	MAZE
Allfasteners	NetWalker	Groupe Igrec, igrec.fr	MAZE	Interstate Restoration	MAZE
Alliance Building Services	Pysa	Ragnar_Lodger	MAZE	J.W. Smith Customs Broker Ltd.	MAZE
Allison-Smith Company LLC	Sodinokibi (REvil)	EDP Group	Avaddon	Jacitara	MAZE
AMA Freight	MAZE	EFCO forms	Pysa	JAMESTAN - Engineering LTD	AKO
Amacon - https://www.amacon.com	NetWalker	Egypt Yellow Pages Online	MAZE	Jands - https://www.jands.com.au	NetWalker
American Osteopathic Association	MAZE	ehalc.com	Sodinokibi (REvil)	John Christner Trucking	MAZE
American Osteopathic Association	MAZE	Einhell Germany AG	MAZE	John Hardy	Pysa
Amicorp Group	Sodinokibi (REvil)	electric gas industries association inc	Conti	Johnbear	Conti
Amphastar Pharmaceuticals, Inc	DoppelPaymer	Electricaribe	MAZE	Johnson Air Products	MAZE
Andrew Cross & Co.	MAZE	Elsa LLC	Sodinokibi (REvil)	Joliet Park District	Conti
Ansen Corporation	MAZE	Empire Communities Corp.	DoppelPaymer	JX Enterprises, Inc	MAZE
Antonio Citterio Architetto	MAZE	Engineering Consultants Group	MAZE	Karmsund Maritime Offshore Supply AS	MAZE
Apollo Tyres Ltd	NetWalker	Entrust Energy - https://www.entrustener	NetWalker	Karmsund.no	Suncrypt
AppliChem GmbH	MAZE	eurecat.com	Sodinokibi (REvil)	KCG, Inc.	DoppelPaymer
Arabian Industries	MAZE	Exois Ltd	Sekhmet	Kenneth Cole Productions	Sodinokibi (REvil)
Argus Management Company, LLC	MAZE	EXECPHARM.COM	CL0P	Kent County Trading Ltd	DoppelPaymer
Armour & Associates	Sodinokibi (REvil)	Express Manufacturing, Inc.	MAZE	Ker Controls Limited	MAZE
Artech Information Systems LLC	MAZE	Faico	Pysa	Kimchuk Inc.	DoppelPaymer
Arteris SA	Nefilim	Fairfax County Public Schools	MAZE	KollerCraft	MAZE
ASCENT Network	Sodinokibi (REvil)	Famisanar	Pysa	Kristin Tarbet, Plastic Surgeon	MAZE
ASU Inc - ASU-NVG.COM	AKO	Faxon Machining, Inc.	MAZE	KUHNLE-TOURS GmbH	MAZE
Asunaro Aoki Construction Co.,Ltd.	DoppelPaymer	FERSPED Inc.	MAZE	L&F DISTRIBUTORS (LNF)	MAZE
athrone.com	Sodinokibi (REvil)	FGXI	Sodinokibi (REvil)	Laboratoires Expanscience	MAZE
Atlanta Computer Group, Inc.	MAZE	Filtration Group	Conti	Lakeland Community College	MAZE
Atlas Machinery	MAZE	Fincomex	Pysa	Lally Ford	MAZE
Austin College	NetWalker	Fisher & Paykel	Nefilim	Landmarkresort hotel beach	Conti
Australian company ARAFI	Sodinokibi (REvil)	Florida Chamber of Commerce	Conti	Lawyers network	MAZE
Automatic Handling International - http	NetWalker	Florsheim Homes	MAZE	Lectra	MAZE
aVINC	MAZE	FlorStar - https://www.florstar.com	NetWalker	Lee & Associates, LLC	MAZE
Axxess International Inc	Conti	Fondazione Arena di Verona	MAZE	Léon Grosse	MAZE
Bailey&Galyen Attorney	Ragnar_Lodger	FPI Management	Suncrypt		
Baker Wotring LLP	MAZE	Fraser Wheeler & Courtney LLP	Sodinokibi (REvil)		

Ransomware statistics and trends

Ransomware is one of the top threats in cybersecurity. With **878 cyberattacks in 2020**, **18%** of which **were ransomware**, according to the [Identity Theft Resource Center](#).

Organizations around the world are being held hostage by ransomware, with many paying up solely to avoid the cost and downtime of not paying the criminals.

In short, cybercriminals are making and demanding more money than ever.

- The **average ransom paid increased 171%** from 2019 to 2020 (\$115,123 to \$312,493), said the [2021 Unit 42 Ransomware Threat Report](#).
- The highest ransom paid **doubled from 2019 to 2020 from \$5 million to \$10 million**.

Double Extortion Dashboard

Date	Victim	Actor	Sector	Country
22/03/2022	APEC Group	LockBit	Financial Services	Australia
13/01/2022	FDC Construction & Fitout	Cuba	Constructions	Australia
6/12/2021	MST LAWYERS	Conti	Legal	Australia
1/12/2021	SICAME AUSTRALIA PTY LTD	Grief	Industrial Goods & Services	Australia
21/11/2021	ASPECT STUDIOS ASIA PTY LTD	BlackByte	Constructions	Australia
21/11/2021	Law Society of South Australia	Haron	Legal	Australia
19/11/2021	PKF	LockBit	Financial Services	Australia
12/11/2021	Reds Rugby (Rugby Australia)	LVBlog	Entertainment	Australia
11/11/2021	Greymouse VA PTY Ltd	Conti	Business Training & Employment Age	Australia
10/11/2021	Evolve Development	LockBit	Real Estate	Australia
7/11/2021	TRINA SOLAR	Conti	Energy	Australia
5/11/2021	CTI Group	LockBit	Consumer Services	Australia
5/11/2021	Sports Entertainment Network	LVBlog	Broadcasting & Entertainment	Australia
1/11/2021	Finite Recruitment	Conti	Business Training & Employment Age	Australia
29/10/2021	Folio Mortgage & Finance	LVBlog	Financial Services	Australia
19/10/2021	Watson Mangioni Lawyers Pty	LockBit	Legal	Australia
15/10/2021	PJ SAS Trading	LVBlog	Financial Services	Australia
13/10/2021	Matic Transport	BlackByte	Transportation & Logistics	Australia
13/10/2021	JADECORP	Conti	Constructions	Australia
11/10/2021	Ferretti International	Spook	Constructions	Australia
8/10/2021	Macquarie Health Corporation	Hive	Health Care	Australia
28/09/2021	Minjar Gold	Conti	Mining	Australia
25/09/2021	Jaylon	LockBit	Materials	Australia
21/09/2021	Noone	LockBit	Apparel & Textile	Australia

\$ 3.6M

Average
organizational
cost of a data
breach in ASEAN
in 2019*

96 percent of Singaporean businesses reported suffering a data breach between September 2018 and September 2019.*

Singapore, January 2019: second health data breach in six months*

Philippines, January 2019: Cebuana's marketing server breached*

"More than 900,000 clients of Philippine-based pawnshop Cebuana were affected by a data breach"

Thailand and Vietnam, March 2019: Toyota suffers a chain of data breaches*

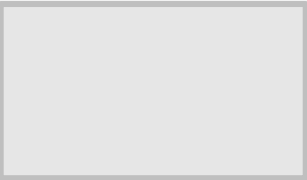
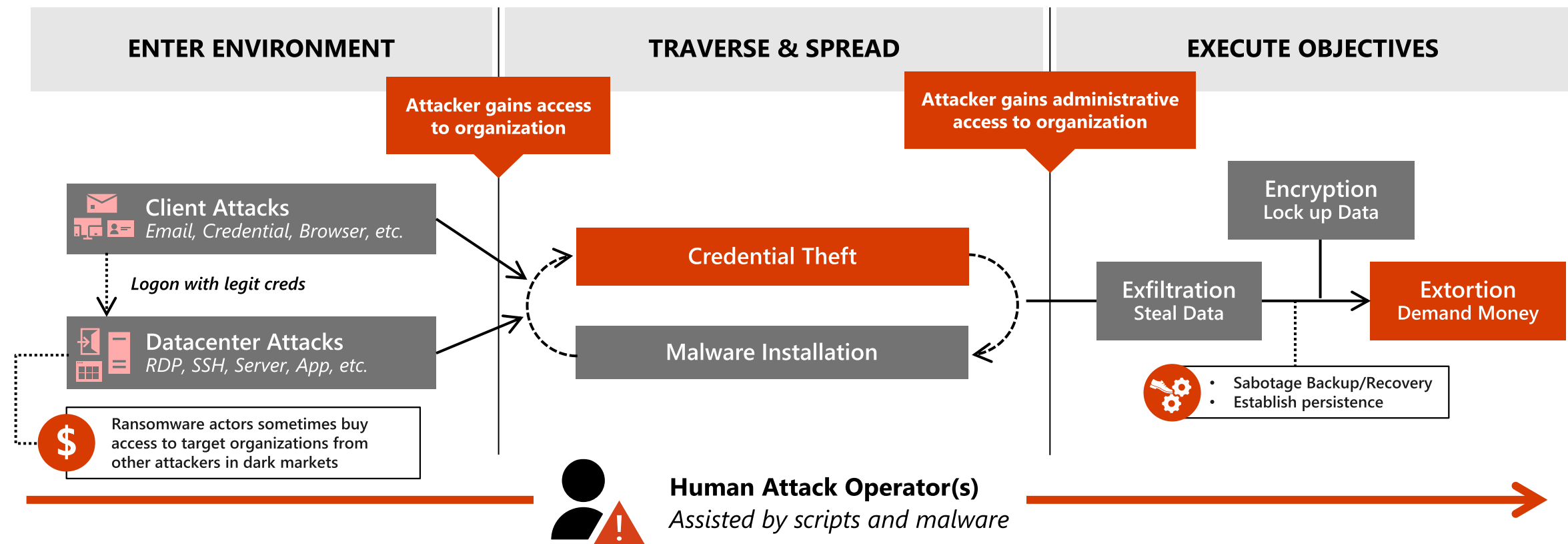
Singapore, July 2018: the city-state suffers its largest data breach*

"largest data breach in its history with 1.5 million patients affected by it, including Prime Minister Lee Hsien Loong"

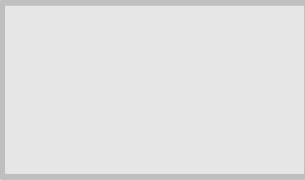
Philippines, May 2018: Wendy's and Jollibee asked to take preventive measures against data breaches*

* <https://www.csoonline.com/article/3532816/the-biggest-data-breaches-in-southeast-asia.html>

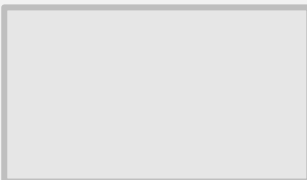
Pattern – Human Operated Ransomware



Ryuk
example (Email)



Wadhrama
example (RDP)



Comparison to
traditional ransomware

Introduction to Cybersecurity

- According to Gartner, cybersecurity is the combination of people, policies, processes and technologies employed by an enterprise to protect its cyber assets. Cybersecurity is optimized to levels that business leaders define, balancing the resources required with usability/manageability and the amount of risk offset.
- Subsets of cybersecurity include IT security, IoT security, Information security and Operational Technology (OT) security.

Cybercrime has increased every year as people try to benefit from vulnerable business systems. Often, attackers are looking for ransom: 53% of cyber attacks resulted in damages of \$500,000 or more.

Types of Cybersecurity Threats

Phishing	Phishing is the practice of sending fraudulent emails that resemble emails from reputable sources. The aim is to steal sensitive data like credit card numbers and login information.
Ransomware	Ransomware is a type of malicious software. It is designed to extort money by blocking access to files or the computer system until the ransom is paid.
Malware	Malware is a type of software designed to gain unauthorized access or to cause damage to a computer.
Social engineering	Social engineering is a tactic that adversaries use to trick you into revealing sensitive information. They can solicit a monetary payment or gain access to your confidential data.

Cybersecurity Trends

In October 2021, Checkpoint Software reported that India ranked second for ransomware threats in the world, and Sri Lanka ranked third. However, a study by US-based Temple University found only 28 reported cyber-attacks in Asia, suggesting a large degree of underreporting.

Acceleration in the adoption of Zero Trust

- Zero Trust (ZT) is an architectural model that intelligently and strategically upscales an organization's security posture. It increases data security through obfuscation, limits the risks associated with excessive user privileges, and uses analytics and automation to dramatically improve security detection and response.

Spending on fraud prevention technology

- According to GBG firm's report, the financial institutions in Australia have an average estimated budget of AU\$104.3 Mn to purchase new fraud prevention technology in 2020-2021.
- The average across APAC was AU\$114.1 Mn, with the highest average estimated fraud budgets being in Thailand at AU\$130.7 Mn, China at AU\$125.2 Mn and Indonesia at AU\$121.8 Mn.

Ransomware attacks as the primary form of threat

- Indian organizations were worst hit by ransomware attacks among all Asia Pacific (APAC) nations during the COVID-19 pandemic, and globally, India stood second when it came to ransom.
- According to CrowdStrike's global survey, 74% organizations in India suffered a ransomware attack in 2020 compared to 67% of Australia's companies 52% in Japan, and 46% in Singapore.

COVID-19's Impact on Cybersecurity

As the COVID-19 pandemic has forced organizations around the globe to shift to remote work, cyber-attackers have taken advantage of vulnerabilities in the new IT environment to launch ransomware and phishing campaigns. In the APAC region, the healthcare sector is lacking in cybersecurity, making global cybersecurity collaboration even more important.

Inadequate protection in remote work locations

- The sudden shift to remote work has forced many businesses and organizations to adopt a new IT environment, sometimes without incorporating adequate cybersecurity safeguards.
- According to CrowdStrike's 2020 Work Security Index, 54% of employees believe their orgs are more likely to experience a serious cyberattack during the pandemic than before the outbreak

Need for new solutions

- The traditional cybersecurity solutions are not sufficient and cannot detect or tackle new sophisticated attacks such as the advanced persistent threat (APT) and so investment is needed to acquire new cybersecurity technologies. However, the budget issue is a critical area that needs the attention of the Association of South East Asian Nations (ASEAN) countries.

Attacks on the Healthcare Sector

- Although ransomware attacks on the Asia-Pacific healthcare sector have been rarely reported since the start of the coronavirus outbreak, the sector is not immune to these threats.
- The Indian government had acknowledged that their healthcare and educational sectors have been targeted by COVID-19-themed phishing attacks and malware, including ransomware. Other Asia-Pacific governments have issued alerts.

Cybersecurity Drivers

With the onset of COVID-19, there has been a rise in cyberattacks, data fraud, and security breaches which have forced many businesses and organizations to adopt new IT environments. Governments are also driving the adoption of new cybersecurity technologies by enforcing stricter rules and guidelines to mitigate cyber risk.

Rise in cyberattacks and data fraud

- Rise in cyber attacks and ransomware is one of the key factors driving the APAC cybersecurity market. Organizations are spending huge amount on new technologies and solutions to cope up with the attacks.
- CrowdStrike has observed an increase of over 330% in eCrime activity since the start of 2020 compared to 2019.

OS vulnerabilities leading to security breach

- Security attacks continue to rise at an accelerated pace in Singapore with more than 80% of businesses having suffered a breach within 12 months.
- Representing an average of 1.67 breaches per organization, new VMware findings highlight a 43% spike in attack volumes across the city-state within the space of a year, with 67% being "more sophisticated" in nature.

Government initiatives to strengthen Cybersecurity

- Governments across APAC have started to enforce strict laws and finer to ensure that organizations and institutions, handling public data, have taken necessary steps to mitigate cyber-risk and safeguard data.
- As a result, companies who would may not have voluntarily strengthened their IT infrastructure are now forced to adhere to standards prescribed by their government.

Market Overview

APAC's cybersecurity market was valued at \$30.45 Bn in 2019, and it is expected to register a CAGR of 18.3%, during 2020-2025.

- According to Allianz Risk Barometer 2020, the average organizational cost of a data breach in the Association of Southeast Asian Nations (ASEAN) accounted for \$2.62 Mn. The average number of records per breach is 22,500.
- Many emerging countries in the region, such as India, China, Singapore, and Japan, are facing increasing cybersecurity issues. India has experienced a rapid increase in cybercrime, according to Gemalto, India accounts for 37% of the global breaches in terms of records compromised or stolen.
- Many governmental and regulatory bodies in the region are identifying the need to balance technological innovation with risk management and user protection. Thus, they are incorporating strong regulatory and legislative framework for cybersecurity measures such that the digital economy can prosper without any hindrance.
- The increasing realization among companies about the importance of saving money and resources by moving their data to the cloud, rather than building and maintaining new data storage, along with the COVID-19 induced shift to remote work environment have skyrocketed the demand for cloud-based solutions, which in turn is increasing the adoption of on-demand security services.
- According to Microsoft, 19 Mn ransomware and phishing attacks were noticed in the Asia, from February to May 2020. Of those, 9,100 encounters were related to COVID-19 in India.

Cybersecurity Spending

According to Deloitte's report, Cyber Smart: Enabling APAC Businesses, cyber spending in APAC is expected to grow faster than the global average with an additional \$31 Bn spent by 2026.

- According to the Global Data forecast, the rising threat of data breaches among enterprises has raised the issue of securing enterprise networks and as a result, the network security revenue in the APAC region will reach \$1.4 Bn in 2024.
- The overall network security spending in the region is expected to grow at a CAGR of 1.3% during 2019-2024.
- Global Data forecasted that the managed security services revenue in the Asia Pacific region will reach \$17.0 Bn in 2024, as a surge in cyber attacks sees enterprises ramp up investment in solutions to combat rising threats.
- According to Global Market Insights, the global cybersecurity market is set to exceed \$400 Bn by 2026 and the APAC cybersecurity market is set to attain over 20% revenue share by 2026.
- The government authorities of China, India, and Singapore are making significant efforts and introducing security guidelines. These supportive initiatives are enabling enterprises from multiple industry verticals to adopt network connectivity and infrastructure protection devices. This helps in mitigating potential threats and track vulnerabilities to enterprise network connectivity.

Cybersecurity Challenges

According to CrowdStrike, the top cybersecurity challenges in the region are remote workforce, new regulation, cost of compliance, limited budgets, and additional training.

Other key cybersecurity challenges include:

Vulnerabilities in remote work

- Barracuda report revealed that 46% of organizations in the region do not have an up-to-date security strategy or solution covering all the vulnerabilities posed by remote working, while 54% admitted that security has taken a back seat in the shift to this mode of working.

Lack of cybersecurity workforce

- According to Statista, APAC witnessed the largest cybersecurity workforce gap in 2020, as around 2 Mn IT security professionals were still needed at that time.
- The global pandemic has sent 92% of organizations scurrying to adopt new technologies in order to facilitate remote work, but businesses in Asia-Pacific often come up short on cloud expertise and endpoint controls, leaving companies vulnerable to cyberattacks.

Low maturity level of the APAC healthcare sector

- According to NTT's 2020 Global Threat Intelligence Report, The cybersecurity maturity level of the healthcare sector is lower than that of technology and financial sectors. Asia-Pacific healthcare sector's level is the lowest of the healthcare sector in any region.
- The medical institutions in APAC are less interested in cybersecurity than those in other regions, making it challenging for them to adequately prevent, detect, or respond to cyber threats.

Future Outlook

Governments and organizations will continue to adopt new cybersecurity technologies, principles, and partnerships.

Asia Pacific finally catches up on Zero Trust adoption

According to Forrester, Zero Trust adoption in APAC has lagged its global peers, but the acceleration of cloud adoption and an explosion in remote work, as well as changing regulations and consumer behaviours, make it ripe for change. Besides, according to Forrester, at least one of the APAC country governments will be embracing the Zero Trust Cybersecurity framework, as early as 2021.

Chief Information Officers will embrace cloud-first and platform strategies for speed and adaptiveness

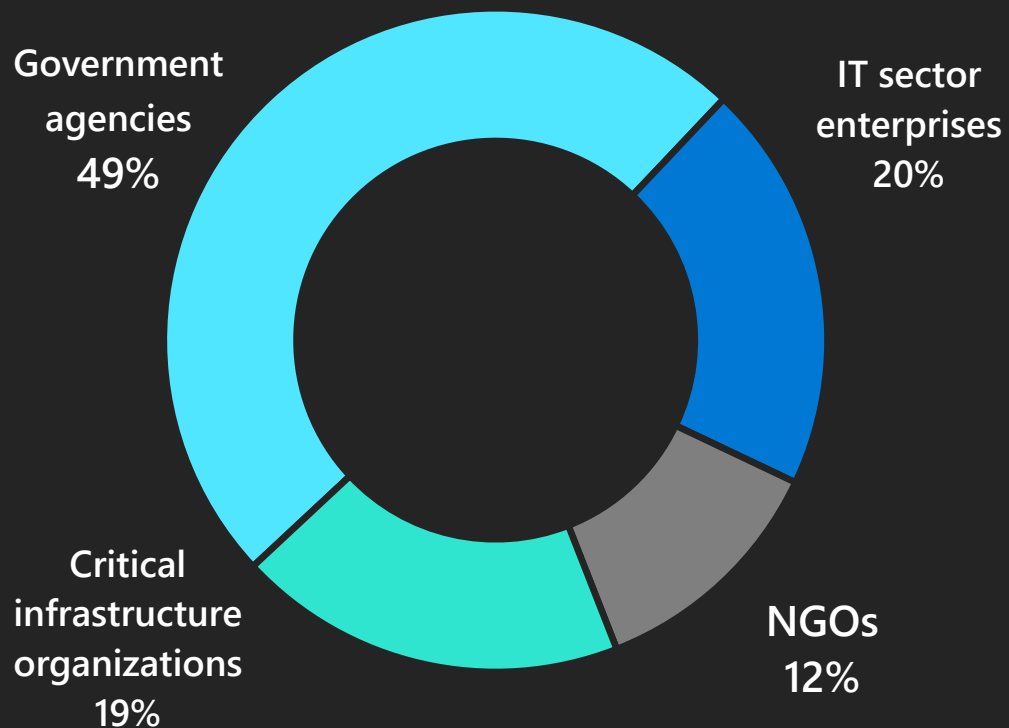
In 2021, 30% of firms will continue to accelerate their spend on cloud, security and risk, networks, and mobility, including struggling firms looking to leapfrog the competition and gain advantage as pandemic transitions take place.

Lessons from Ukraine's Hybrid War

Cyber espionage

Recent Russian network penetration and cyber espionage operations outside Ukraine

Russian network intrusion targets



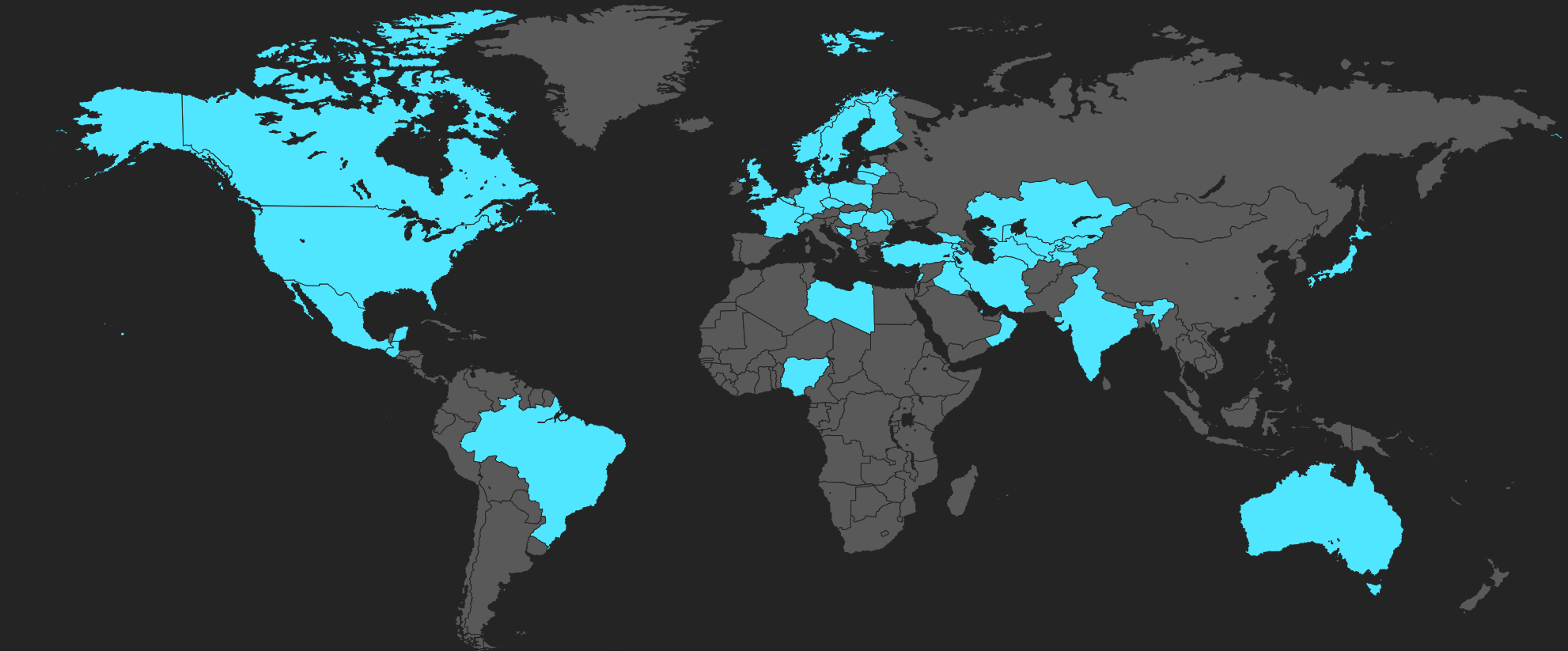
128 Russian network intrusions

42 Countries

29% Success rate

In most instances the victims were operating on premises, not in the cloud

Countries outside Ukraine targeted by Russian cyber espionage since the start of the war in Ukraine



Russian malware families used for destructive attacks

- WhisperGate / WhisperKill
- FoxBlade, aka HermeticWiper
- SonicVote, aka HermeticRansom
- CaddyWiper
- DesertBlade
- Industroyer2
- Lasainraw, aka IssacWiper
- FiberLake, aka DoubleZero

WhisperGate, FoxBlade, DesertBlade, and CaddyWiper are all malware families that overwrite data and render machines unbootable. FiberLake is a .NET capability being used for data deletion. SonicVote is a file encryptor sometimes used together with FoxBlade. Industroyer2 specifically targets operational technology to achieve physical effects in industrial production and processes.

Key learnings

Russia:

Multiple Russian threat actors converged on Ukrainian entities, while NOBELIUM continued to pursue compromises among IT services providers globally. STRONTIUM targeted the unpatched Exchange on-premises and cloud environments of defense and government sector organizations worldwide. Threat actors worked in part to gain intelligence relevant to ongoing geopolitical tensions.

China:

DEV-0322 remained focused on targeting individuals and entities that support the United States defense industrial base. China exploited a previously unidentified Exchange vulnerability that was weaponized shortly after being discovered during the Tianfu Cup, a domestic hacking competition.

Iran:

Began more brazen cyber operations. Conducted ransomware attacks at an increased pace and expanded those attacks to US and EU targets. Likely set itself up for attacks on infrastructure in the US and Israel in the future if it decides it needs to increase pressure.

North Korea:

Targeted journalists and construction/architectural entities in South Korea to obtain geopolitical intelligence. They also attempted to bolster their struggling economy by compromising many cryptocurrency companies.

15,740

Nation State Notifications

Microsoft issued 15,289 NSNs for enterprise accounts across 466 organizations, along with 451 for consumer accounts. While this was a drop in NSNs from an all-time high the previous quarter, it was still a very large number, historically speaking.

6%

Compromise rate

The compromise rate of 6% was a slight uptick from the previous quarter, but it remains lower than the 11% compromise rate we saw prior to mid-2021.

37%

Critical infrastructure

The percentage of attacks targeting critical infrastructure was down from the record high of 45% the quarter before, but was still very high, historically speaking.

IT

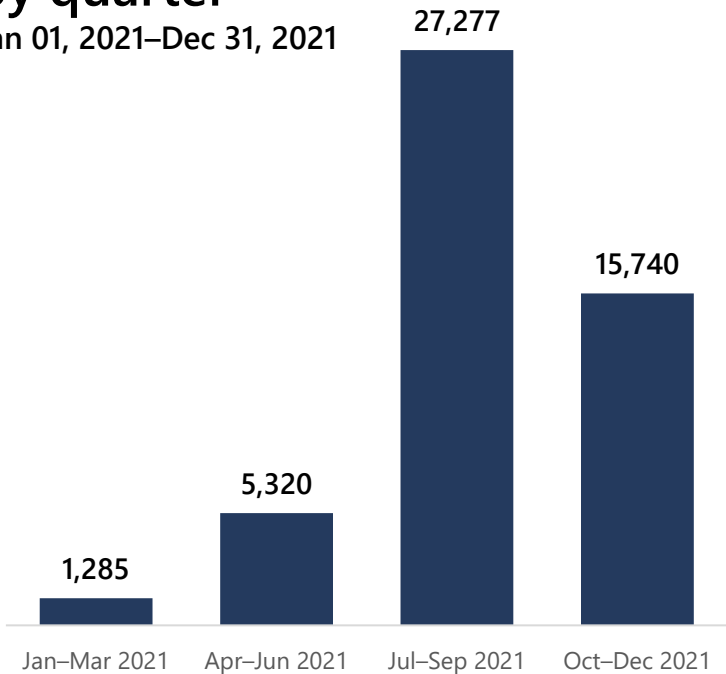
Most targeted sector

IT remained the most targeted sector, with 36% of NSNs issued to IT companies, continuing an ongoing spike from last quarter in nation state targeting of this space.

Oct–Dec 2021: By the numbers worldwide

Past year NSNs quarter by quarter

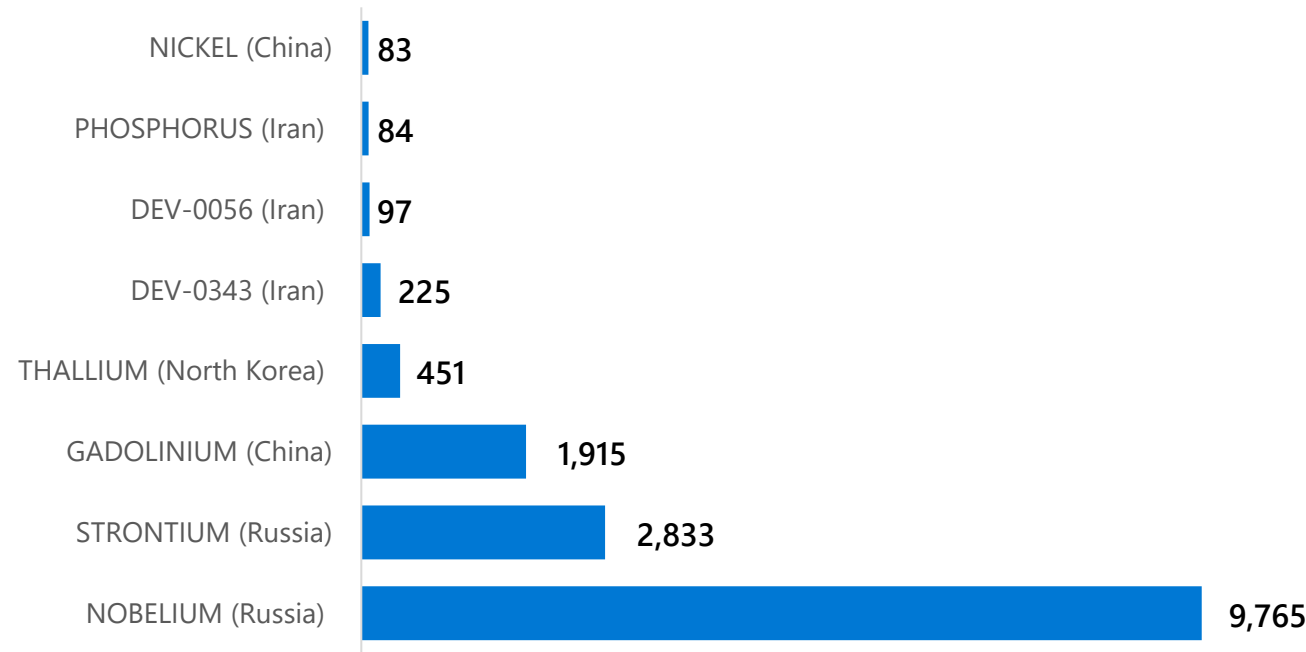
Jan 01, 2021–Dec 31, 2021



NSNs remained elevated, albeit with a decline from the previous quarter’s all-time high.

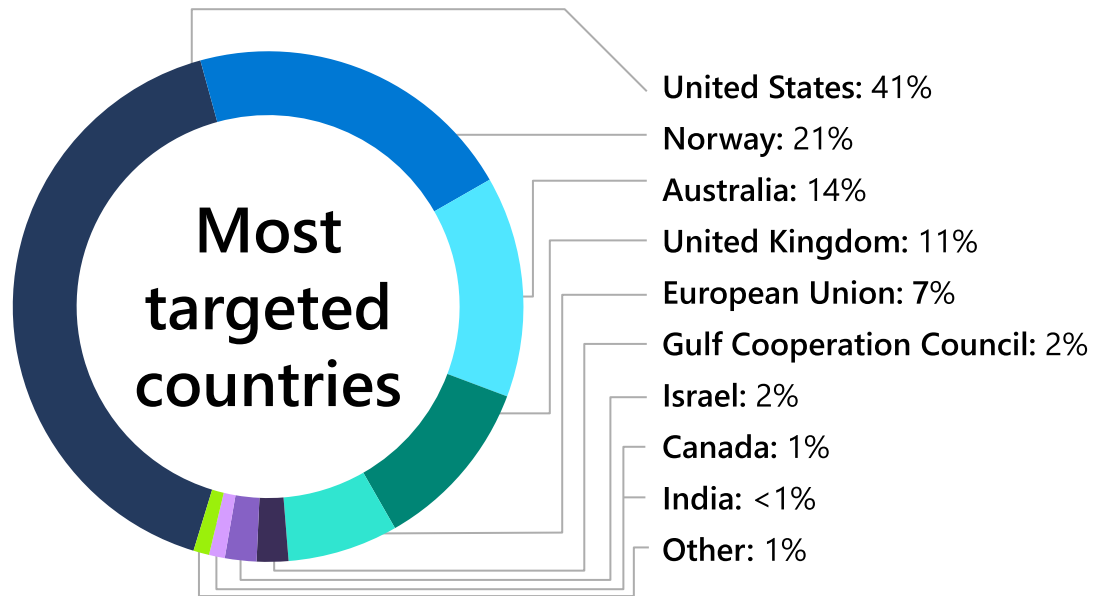
Most active actors

October–December 2021

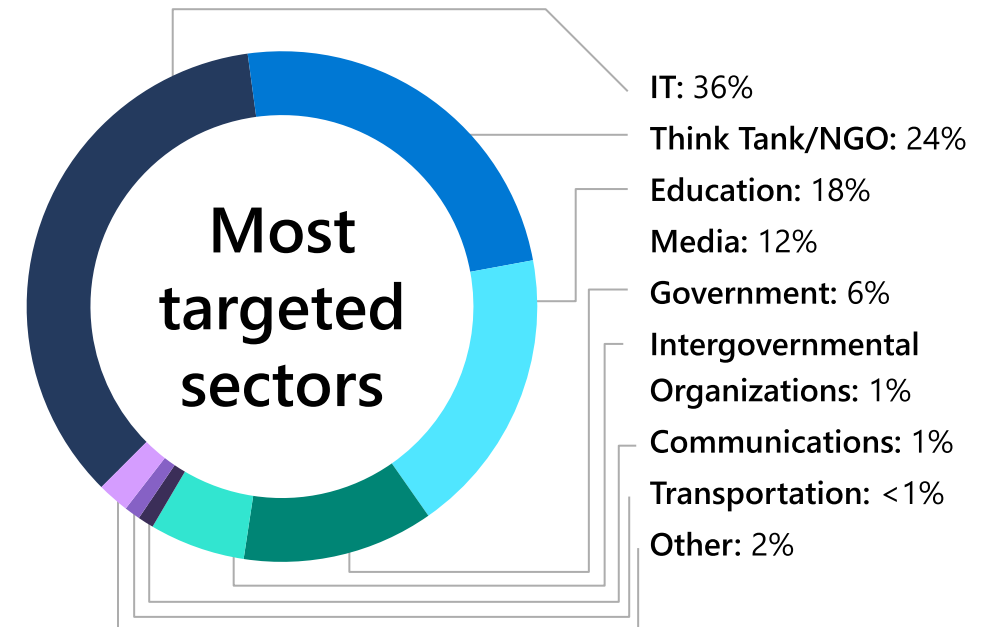


NOBELIUM remained by far the most active actor by NSN count, while STRONTIUM and GADOLINIUM had a surge of activity due to their targeting of an educational institution in Norway and a media entity in Australia, respectively.

Oct–Dec 2021: By the numbers worldwide



US and UK remained a focus but targeting spanned the globe. The targeting of Norwegian and Australian enterprises surged this quarter because of cyber operations by Russia and China, respectively. Enterprises in NATO countries accounted for four out of every five NSNs.

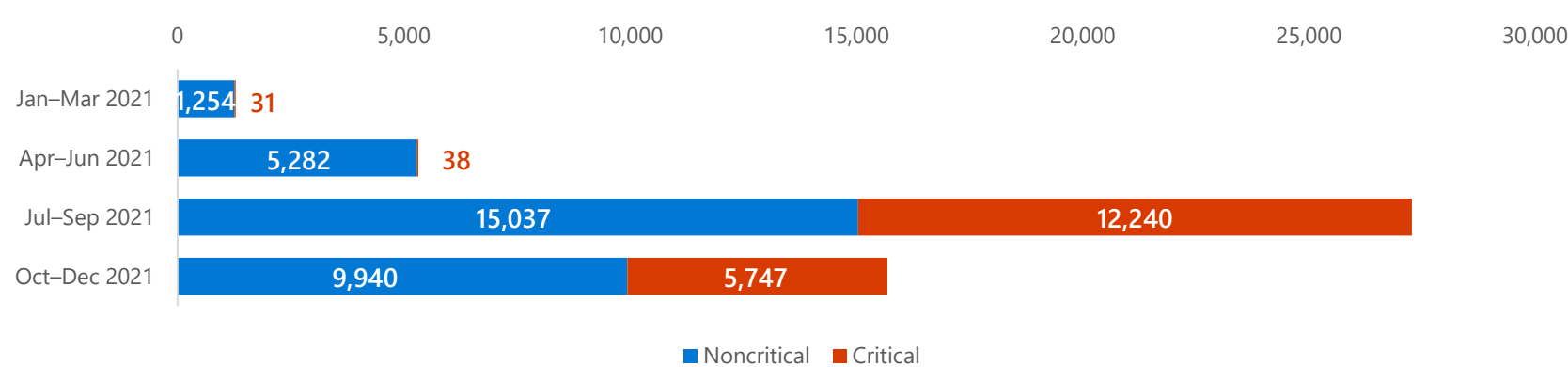


IT sector targeting remained elevated. Nation state actors continued their focus on the IT and higher education sectors this quarter, while targeting of media and think tanks/NGOs increased compared to the last quarter and last year.

Oct–Dec 2021: NSNs by the numbers worldwide

Noncritical vs. critical infrastructure

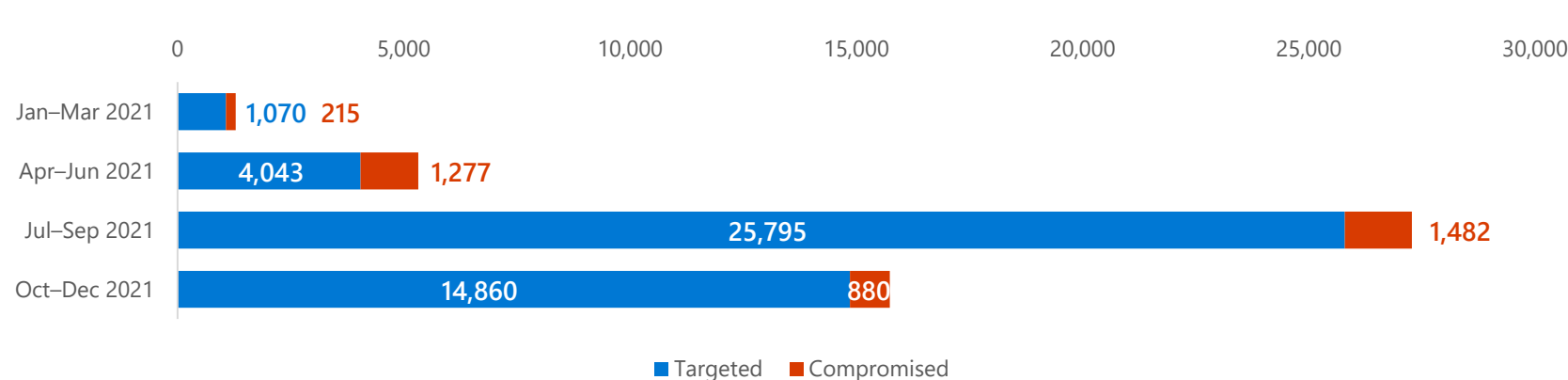
Jan 01, 2021–Dec 31, 2021



Critical infrastructure targeting remained well above historical norms, particularly by Russia and Iran.

All notifications, targeted vs. compromised*

Jan 01, 2021–Dec 31, 2021

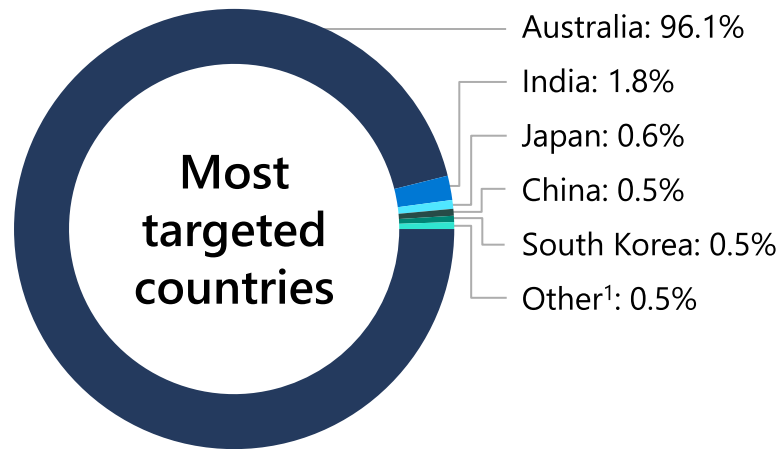


Compromise rate remained steady despite a decline in massive brute force attacks, which yield high target counts with low success rates.

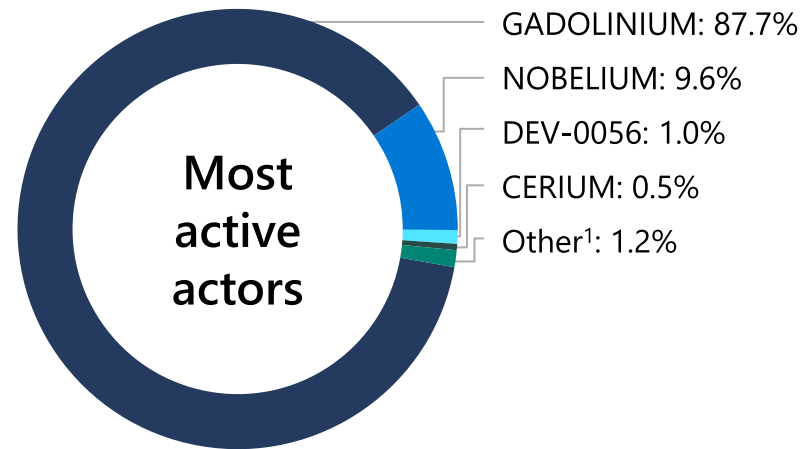
*Targeted accounts include failed login attempts and phishing emails, for which we could not confirm compromise.

Asia-Pacific

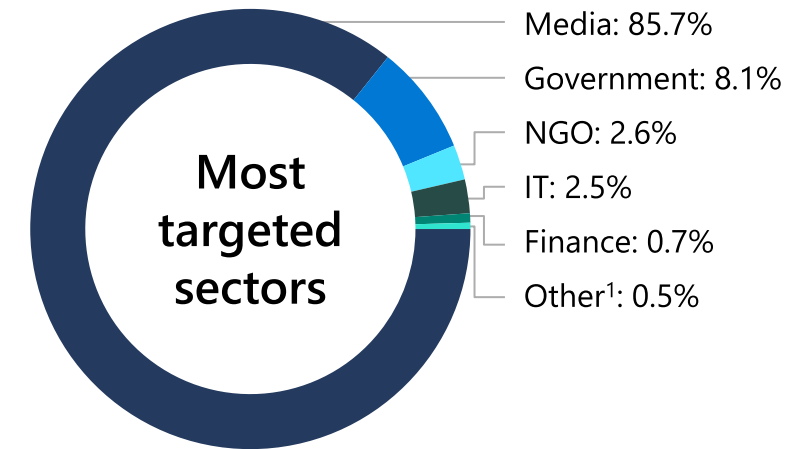
Oct 01, 2021–Dec 31, 2021



A password spray from Chinese actor GADOLINIUM drove up Australian targeting.



GADOLINIUM's password sprays drove its numbers up, including against an Australian media network.



GADOLINIUM's attack on the Australian network involved so many accounts, it alone is responsible for the prevalence of media among sectors targeted from the quarter.

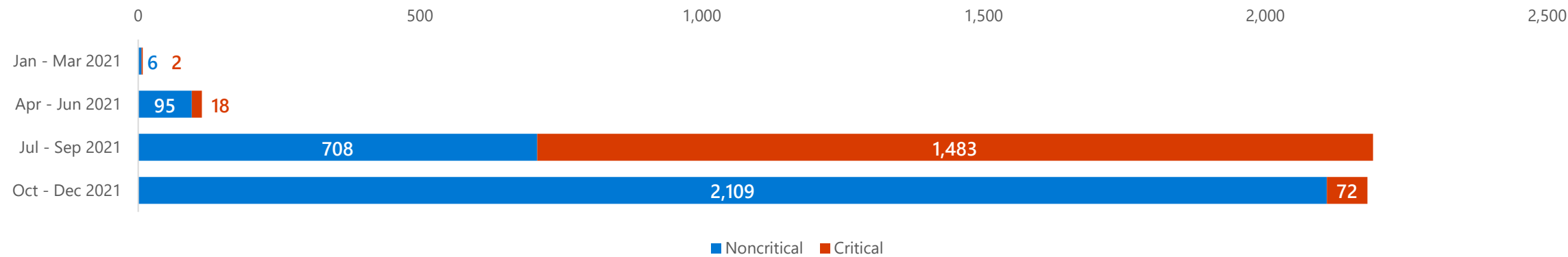
Note: 1. Other is inclusive of all other categories excluding those previously named.

Asia-Pacific

Jan 01, 2021–Dec 31, 2021

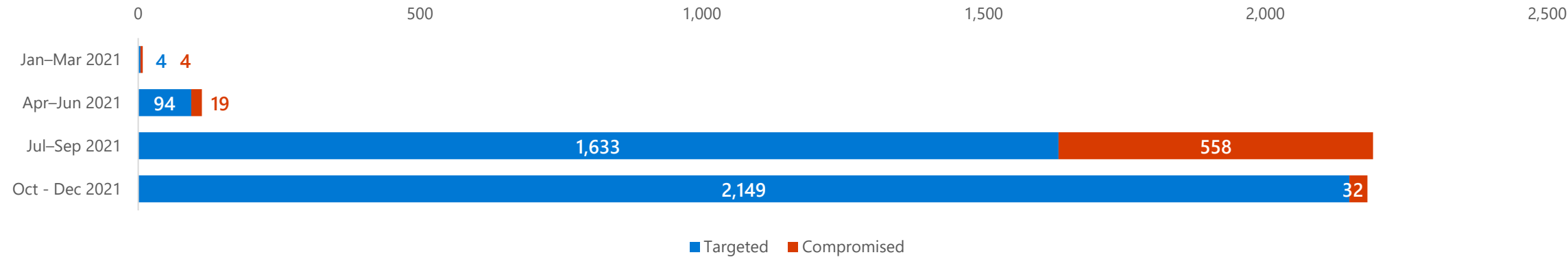
Noncritical vs. critical infrastructure

Jan 01, 2021–Dec 31, 2021



Targeted vs. compromised

Jan 01, 2021–Dec 31, 2021

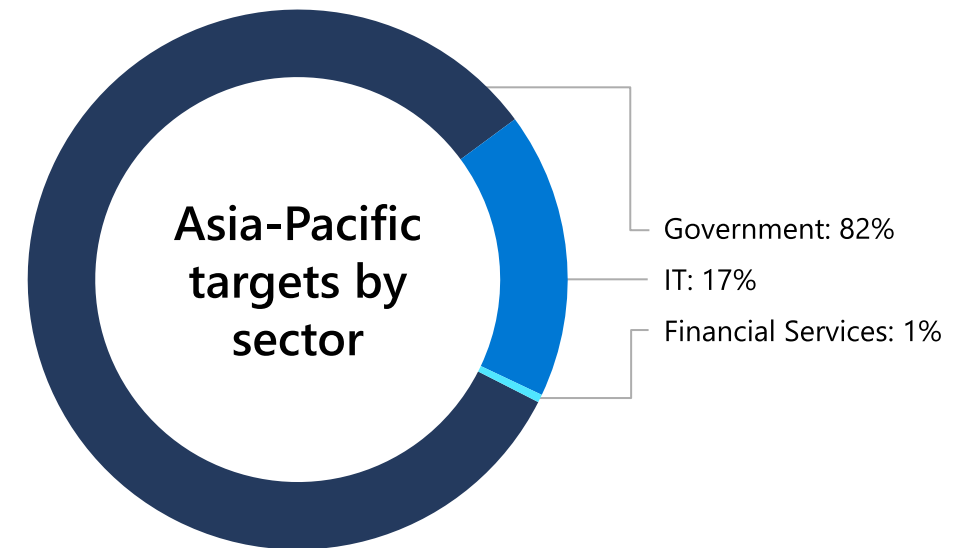


Asia-Pacific

NOBELIUM, the only Russian threat actor to target the Asia-Pacific region this period, focused primarily on government foreign and national security policy organizations in Australia.

- Australian organizations represent 88% of Russia's targets in the Asia-Pacific region.
- In addition to Australian government entities, the actor also sought access to foreign policy-related agencies in Thailand and Japan.

Outside of the government sector, NOBELIUM attempted to compromise IT sector organizations in Australia and India, likely to facilitate access to those firms' customers.



Asia-Pacific

GADOLINIUM conducted a password spray against a media entity in Australia.

- In addition to the media entity, GADOLINIUM also targeted an Australian based non-government organization.

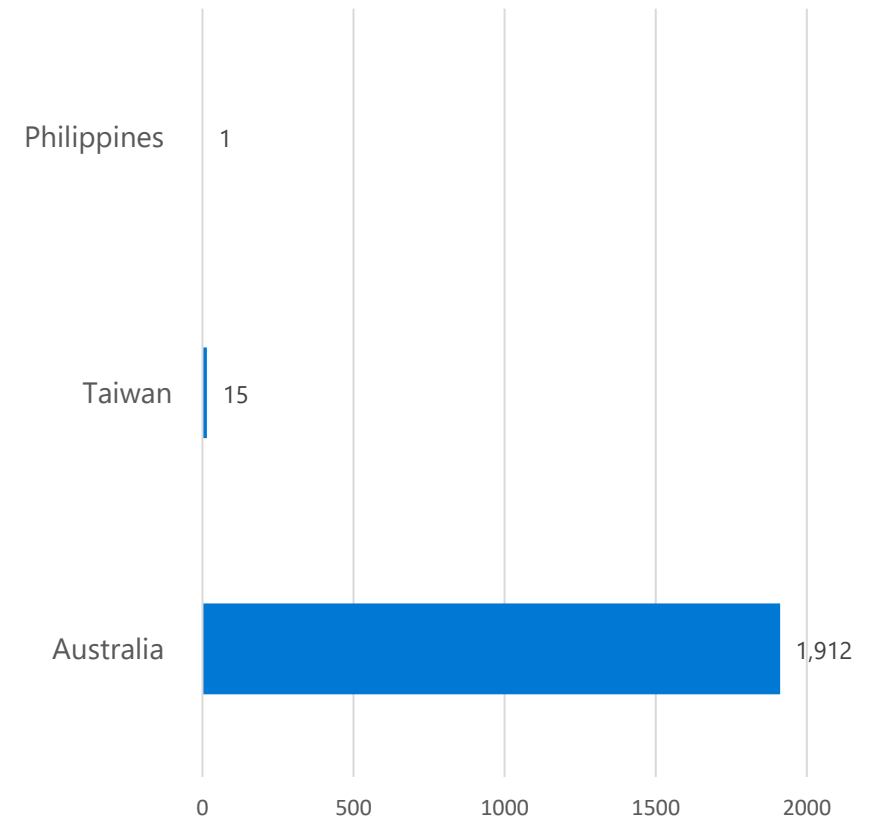
CHROMIUM continued to target Taiwan.

- CHROMIUM showed continued interest in targeting the higher education sector in Taiwan, a trend observed since Spring 2021.

HAFNIUM displays an interest in the Philippines.

- HAFNIUM successfully compromised a single online service account at a government entity in the Philippines.

NSNS issued for Asia



Asia-Pacific

North Korea's two concerns in the region are South Korea and Japan.

- Much of this is seen in spear phishing of individual accounts used by government, think tank, academic, and university entities.
- Sophisticated targeting is also used, especially in South Korea. Example: exploiting weaknesses in VPNs of government organizations.

North Korea also targets entities in China, its strongest ally.

- North Korea has successfully compromised cryptocurrency companies in Hong Kong, as well as a few on mainland China.



Empower your security teams to protect employees and resources

How CISOs are navigating the challenges of COVID-19

82%

feel pressured to lower costs.

67%

identified pandemic-themed phishing attacks.

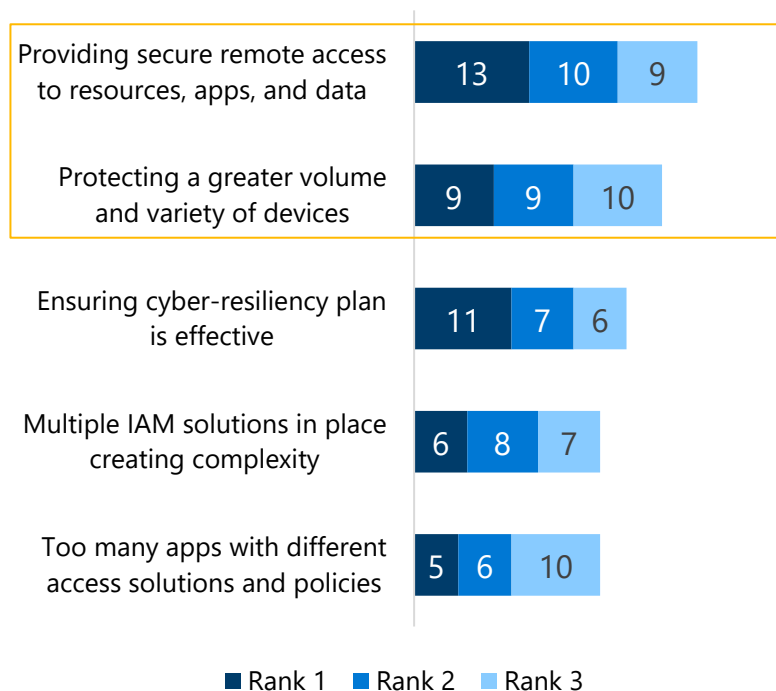
#1

priority to reduce cost is improved threat protection.

Remote work is dominating cybersecurity and compliance efforts

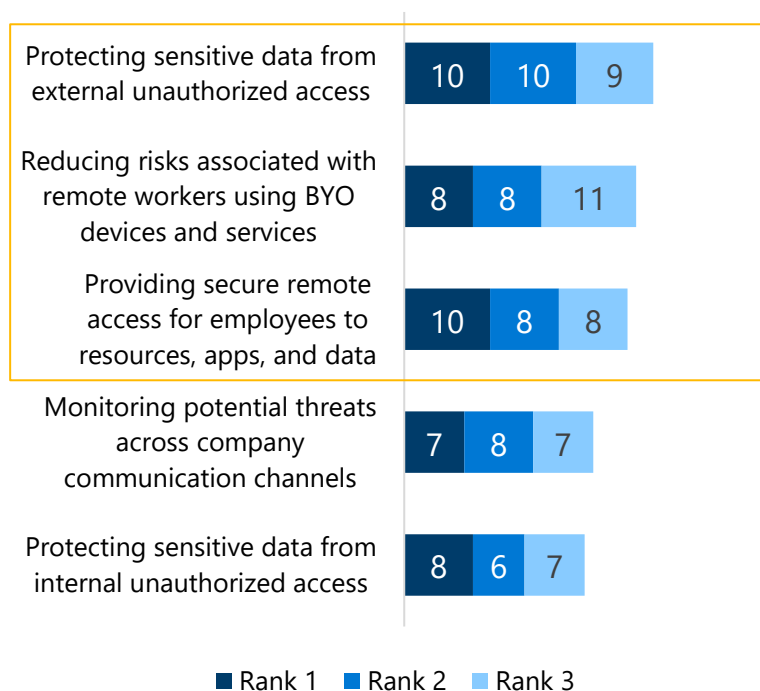
Supporting remote work through secure access and **protecting more devices** are the biggest challenges Security DMs face

Top 5 Cybersecurity Challenges Through Calendar Year
n524; Shown as %



Protecting sensitive data, reducing BYOD risks, and **providing secure remote access** are the top priorities for Compliance DMs

Top 5 Compliance Priorities Through Calendar Year
n570; Shown as %

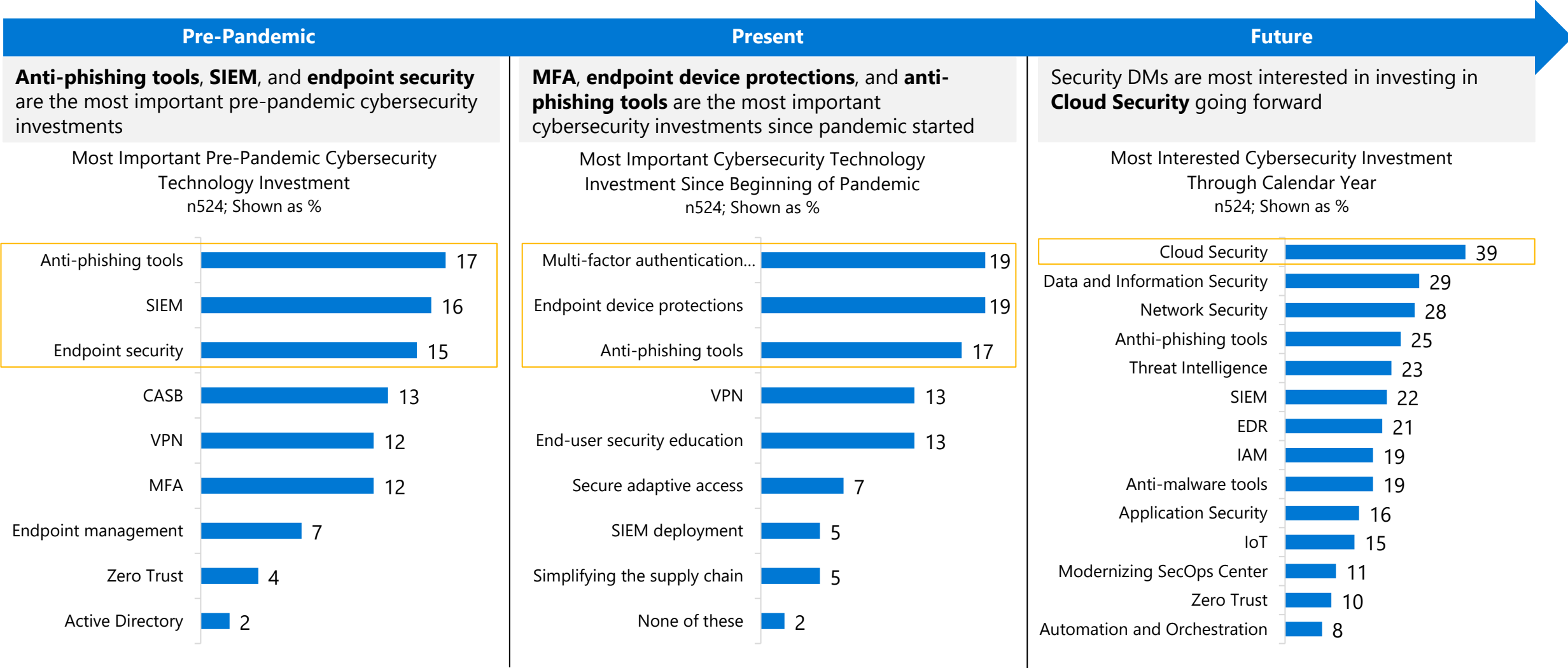


Investments in **Data Protection** is helping organizations address compliance priorities

Top 5 Most Helpful Pre-Pandemic Compliance Investments
n570; Shown as %



The importance of anti-phishing tools, MFA, and endpoint security is well-established; Security DMs are now prioritizing investments in Cloud Security

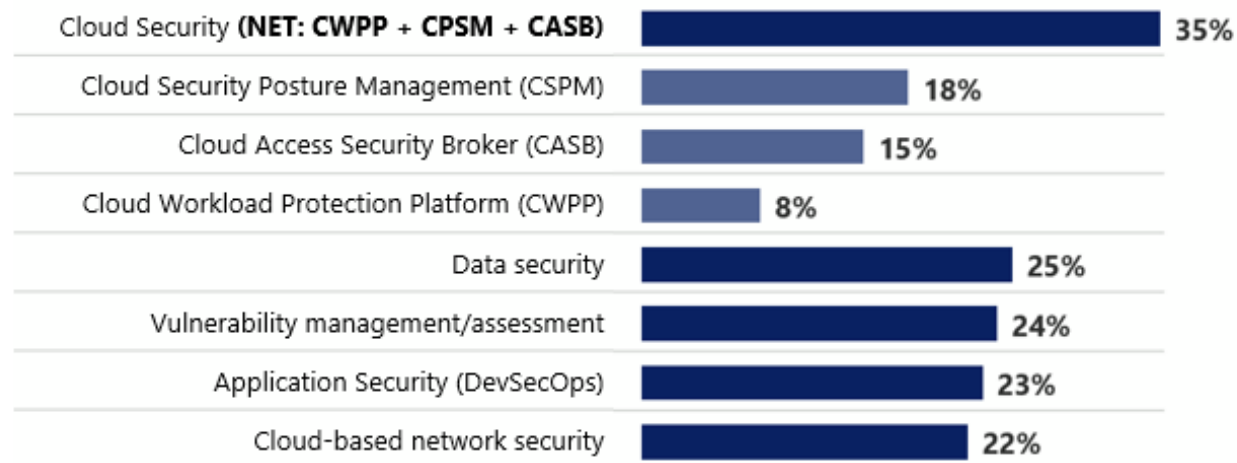


Answer choices have been truncated

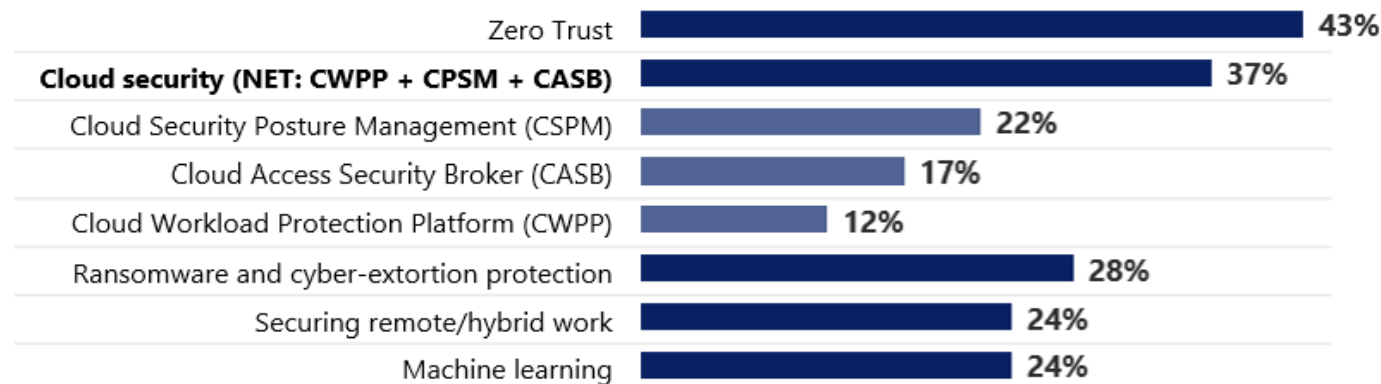
Top 5 cybersecurity challenges



Most Interested in Investing in Next 12 Months



Security Topics of Interest



[How CISOs are preparing to tackle 2022 - Microsoft Security Blog](#)

More Than 70% of SOC Analysts Experiencing Burnout

Nearly 65% of security operations center (SOC) analysts are likely to change jobs in the next year, survey shows.



Dark Reading Staff

Dark Reading

March 05, 2022

Stress and frustration continue to plague the security operations center (SOC):

nearly 70% report understaffed teams, and 60% say their workloads have spiked over the past year.

Some 64% of SOC analysts say manual work eats up more than half of their time, and reporting and monitoring are their least favorite parts of the job.

More than 65% say half of their security tasks could be automated, leaving them time to do deeper security work.

And 64% are considering leaving the organization for a new position somewhere else.









Gartner Cybersecurity Prediction 2021-2022

1. By the end of 2023, modern privacy laws will cover the personal information of 75% of the world's population – strong need to automate Privacy Mgt
2. By 2024, 30% of enterprises will adopt cloud-delivered Secure Web Gateway (SWG), Cloud Access Security Brokers (CASB), Zero Trust Network Access (ZTNA) and Firewall As A Service (FWaaS) capabilities **from the same vendor**. – tools consolidation
3. By 2025, 60% of organizations will use cybersecurity risk as a primary determinant in conducting third-party transactions and business engagements. – Cyber readiness becoming a KPI

[The Top 8 Cybersecurity Predictions for 2021-2022 \(gartner.com\)](https://www.gartner.com)

[Gartner Top Security and Risk Trends for 2021](#)

Top Security and Risk Trends for 2021

01 Cybersecurity mesh		02 Cyber-savvy boards	
03 Vendor consolidation		04 Identity-first security	
05 Managing machine identities becoming a critical security capability			
06 “Remote work” now just “work”		07 Breach and attack simulation	
08 Privacy-enhancing computation techniques			

gartner.com

© 2021 Gartner, Inc. All rights reserved. CTMKT_1187855

Gartner

EXHIBIT 3. HYBRID WORKPLACE INTENT

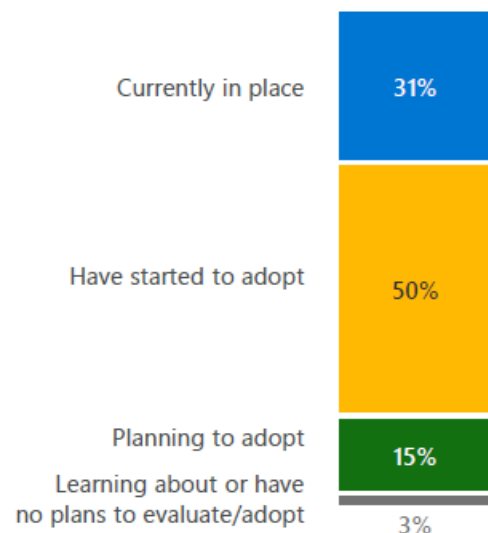


EXHIBIT 4. HYBRID WORKPLACE CONCERNS

Employees downloading unsafe apps	37%
An increase to IT workload	37%
Ransomware attacks	36%
Phishing attacks	35%
Improper use of personal devices	34%
Unauthorized access to data	31%
Inability to manage all devices	30%
Use of personal email accounts	30%
Non-compliance with data regulations	24%

Zero Trust Adaption report 2020 /21

EXHIBIT 1. ZERO TRUST IS CRITICAL

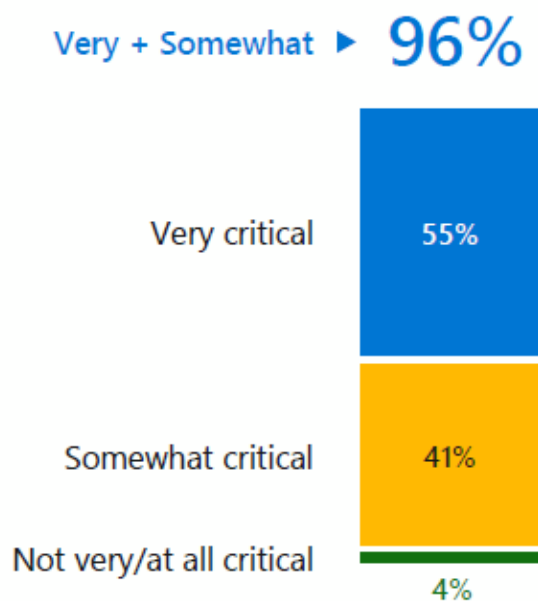






EXHIBIT 2. ZERO TRUST MOTIVATORS

Top Motivators

Improve overall security posture	47%
Improve end user experience and productivity	44%
Transform the way security teams work together	38%
Simplify security stack	35%
Reduce security costs	35%

People

Role	Challenges	How modernizing security operations can help		
 CISO	"The buck stops with me." Escalating threats, high pressure and expectations, job insecurity.	Improved security Better protect organization by proactively blocking threats and responding faster to incidents.	Increased efficiency Leverage automation to more effectively allocate capital and staff resources.	Operational excellence Respond efficiently across environments for better recovery, resiliency, and continuity.
 Infra Manager	"How do I keep my staff?" Increasing threat volume, employee staffing challenges, high stress.	Proactive risk mitigation Identify trends in real time with layered analytics.	End-to-end visibility Insights and analytics support continuous improvement.	Analyst productivity Reduce analyst fatigue and retain staff.
 Dev SecOps	"How can I keep up?" Alert overload, inability to focus on proactive measures, constant stress.	Clear insights Gain greater clarity with role- and objective-specific views.	Improved detection Identify external and insider threats more quickly.	Increased efficiency Focus on addressing and eliminating real threats.
 Security Architect	"Where do I even begin?" Alert fatigue, inability to prioritize threats, risk of burnout.	Improved focus Spend less time chasing false negatives.	Lower "real" threat risk Identify threats faster and cut through the noise.	Better Prioritization Manage alert overload with automated system support.

Reduce cyber risk with integrated, best-in-class protection

Integrated threat protection powered by AI and automation

- Detect and respond faster and more accurately to attacks.
- Increase SecOps efficiency.
- Reduce the number and cost of breaches.



Q & A

- **Security Audits, Vendors, and Tools and Pricing patterns?**
- **How can we provide SSH access in case of Cloud Infra[inside Private Subnet], and Maintain that access in case of On-boarding and Off-boarding new users?**
- **How to Present Security Posture of the Org to non-Security Persons like CEO**
- **How to build a Security Roadmap for eCommerce Unicorn startups in the growth phase.**

Board communication tips from Microsoft's CISO

- Updates and Discussion, have discussion as and when needed and updates 2 or 3 times a year.
- 5 questions CISOs need to ask themselves before presenting to the board
 1. Can you demonstrate a good governance process ?
 2. Do you have the right talent in place ?
 3. What are you doing to ensure a culture of cybersecurity ?
 4. How are you dealing with Technical Debt
 5. How are you and what are you doing to Future Proofing the company?

<https://www.microsoft.com/en-us/videooplayer/embed/RE30ldv?autoplay=true>

Resources

- [Microsoft Cloud Adoption Framework for Azure - Cloud Adoption Framework | Microsoft Docs](#)
- [Understanding just-in-time virtual machine access in Microsoft Defender for Cloud | Microsoft Docs](#)
- [Microsoft Security Best Practices | Microsoft Docs](#)
- [Cyberthreats, viruses, and malware - Microsoft Security Intelligence](#)
- [Cybersecurity + Threat Intelligence | Microsoft Security Insider](#)



Thank you!