SINGAPORE CYBER LANDSCAPE 2022

Singapore Cyber Landscape 2022

Designed by Urban Forest Design Pte Ltd

ISBN: 978-981-18-5413-2

The "Singapore Cyber Landscape 2022" publication reviews Singapore's cybersecurity situation in 2022 against the backdrop of global trends and events. CSA utilises multiple data sources to provide clarity on the common cyber threats observed in Singapore's cyberspace. CSA does not specifically endorse any third-party claim made in this material or related references, and the opinions expressed by third-parties are theirs alone. The enclosed facts, statistics and analyses are based on information available at the time of publication. The contents of this publication are provided on an "as is" basis without warranties of any kind. To the fullest extent permitted by law, CSA does not warrant and hereby disclaims any warranty as to the accuracy, correctness, reliability, timeliness, noninfringement, title, merchantability or fitness for any particular purpose of the contents of this publication. CSA shall also not be liable for any damage or loss of any kind caused as a result (direct or indirect) of the use of the publication, including but not limited to any damage or loss suffered as a result of reliance on the contents contained in the publication. CSA also reserves the right to refine its analyses as the threat situation evolves, and/or as further information is made available.

CONTENTS

Foreword 4

Chapter 1
GLOBAL TRENDS IN 2022 8

Cyber Threats Targeting OT Systems: Evolution of Carnage 10

Ransomware in 2022: Colossal Collective Challenge 13

Cybersecurity Implications of the Russia-Ukraine Conflict: A Year On 19

Chapter 2
WWW.TARGET.SG 22

Overview of Cyber Threats in 2022 24

State of Singapore's Cyberspace 26

Chapter 3
WHAT IS SINGAPORE DOING FOR A TRUSTED, RESILIENT AND SAFER CYBERSPACE? 34

Pillar 1: Build Resilient Infrastructure 36

- Critical Information Infrastructure Supply Chain Programme 39

Pillar 2: Enable a Safer Cyberspace 41

- Countering Ransomware Together 51

Pillar 3: Enhance International Cyber Cooperation 53

- UN-Singapore Cyber Fellowship 59

Foundational Enabler 1: Develop a Vibrant Cybersecurity Ecosystem 61

- From University Lab to the Global Stage 62

Foundational Enabler 2: Grow a Robust Cyber Talent Pipeline 63

What Singapore Government Partners are Doing for a Safer Cyberspace 65

- Ensuring a Safer and More Secure Digital Future 65
- Building a Safer Cyberspace with the Community 69
- Safeguarding Our Everyday Life – CIDeX and Our National Cyber Defence 71
- Minimise Data Breach Risks with Security 73
- The Fight Against Scams – The Singapore Approach 75
- Understanding the SocGholish Malware Compromise: Implications and Protective Measures for Organisations 78

Chapter 4
CRACKING THE CODE: LESSONS LEARNT FROM CYBER-ATTACKS 82

Decrypting the Lessons Learnt from a Ransomware Attack 84

Beyond the Inbox: A Business Email Compromise Lesson 87

Lessons Learned the Hard Way: Tales of Exploited Unpatched Vulnerabilities 89

Ask the Incident Responder: Wayne Lim, Head of Incident Response & Management, CSA 91

Chapter 5
TOMORROW'S DIGITAL SECURITY CHALLENGES 94

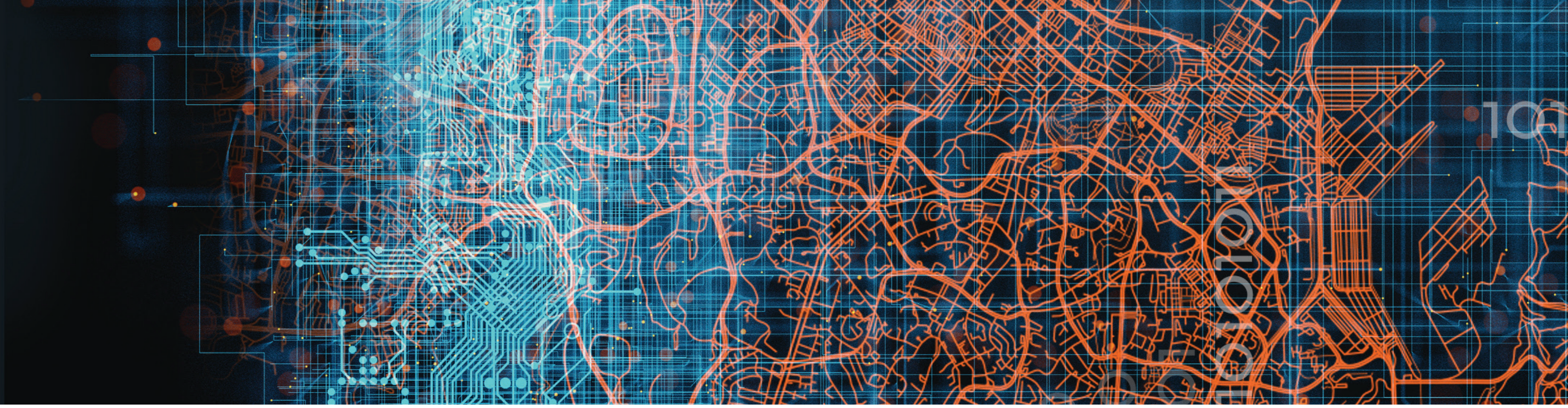
On the Horizon - Cybersecurity and Collective Efficacy 96

Over the Horizon - The Anticipated Emerging Cyber Threats in the Mid and Far-term 98

Glossary 104

Contact Details 107

FOREWORD



In the last Singapore Cyber Landscape (SCL), I wrote that we were encountering increasingly sophisticated threats and more brazen threat actors. Like in a long game of chess, threat actors are always seeking new ways to overcome defences, which means cybersecurity defenders around the world must constantly remain on our toes. True to form, the cyber threat landscape intensified in 2022. This was fuelled by the ongoing Russia-Ukraine conflict and the opportunistic exploits of cybercriminals as COVID-19 restrictions began to ease. Disconcerting developments over the past year included bespoke exploits aimed at industrial Operational Technology (OT) systems, ransomware groups targeting essential organisations, and global service disruptions caused by hacktivist groups, among others.

As Winston Churchill once said, however, "The pessimist sees the difficulty in every opportunity. The optimist sees the opportunity in every difficulty." While there were undoubtedly numerous persistent and emergent cyber threats that arose in the past year, there were also opportunities for Singapore to work with like-minded cyber organisations around the world to strengthen our collective digital resilience.

This duality is best typified by the ransomware threat. Ransomware groups hit a new milestone in 2021 in terms of cyber-physical impact. They caused widespread disruption, leading to supermarkets closing, petrol stations running out of fuel, and healthcare services being delayed, all as a result of compromised systems. In 2022, they outdid this by disrupting an entire government's services – the ransomware attacks on Costa Rica crippled around 30 critical services including utilities and healthcare systems. This resulted in the declaration of a state of emergency by the government. The audacity and severity of these attacks underscored the urgent need for coordinated efforts among governments to address the ransomware threat.

This is exemplified by the Counter-Ransomware Initiative (CRI), a global coalition aimed at collectively addressing the ransomware threat. Led by the US, the CRI aims to prevent cryptocurrency use in ransomware payments, share information, develop guidelines, and build cyber capacity. Singapore is fully involved in this initiative. We are co-leads of the countering illicit finance working group, committed to disrupting the financial flows, particularly in cryptocurrency, to ransomware operators. Given the cross-border nature of this menace, collaboration within the CRI represents a key means to deprive ransomware groups of their lifeblood, creating a more hostile environment for them, and breaking their business models.

This is also reflected in our local approach. While the country has been fortunate to avoid the worst of these attacks, we established the Counter-Ransomware Task Force (CRTF) in 2022, reflecting our determination to combat this growing menace. Chaired by the Cyber Security Agency (CSA), the CRTF brings together the expertise and resources of various government agencies, including the Government Technology Agency (GovTech), Infocomm Media Development Authority (IMDA), Ministry of Communications and Information (MCI), Ministry of Defence (MINDEF), Ministry of Home Affairs (MHA), Monetary Authority of Singapore (MAS), and Singapore Police Force (SPF), with support from the Attorney-General's Chambers (AGC).

The Russia-Ukraine conflict serves as another striking example of local agencies banding together to confront cybersecurity risks resulting from an unstable geopolitical landscape. Now well past its 15th month, the conflict has greatly complicated the global cybersecurity environment, with a surge of hacktivist attacks on both sides and the discovery of highly destructive malware. One of the most worrying developments is the increase of malicious programs targeting industrial systems, posing a significant threat to vital services that sustain our daily lives and capable of causing unprecedented harm. These attacks have already caused significant disruption to Ukrainian systems. The potential of their spread beyond the conflict zone is a catastrophic possibility.

As a small state whose security and existence depends on the international rule of law, Singapore can be adversely affected by geopolitical instability and the potential for spill-over effects in cyberspace. The government worked closely with Critical

Information Infrastructure (CII) sector leads throughout 2022 to step up vigilance and monitoring. Cybersecurity exercises were conducted to test our response to scenarios such as ransomware, supply chain attacks and compromise of OT systems. Additionally, Singapore's Cyber Emergency Response Team (SingCERT) provided regular advisories to non-CIIs, alerting organisations of cybersecurity risks and recommended protective measures.

Away from geopolitical cybersecurity developments, scams continued to plague the local landscape. In 2022, Singaporeans and organisations lost a total of around S$661 million to scams, a 4.5% increase over 2021. Singapore is combatting the scam menace across multiple fronts. Under the leadership of the SPF's Anti-Scam Command (ASCom), over 16,700 bank accounts implicated in scams were successfully frozen, resulting in the recovery of approximately S$146 million for the victims. Additionally, the co-location of officers from six leading banks at ASCom has greatly improved the coordination of investigations. In order to bolster defences against scams, the IMDA has implemented solutions to flag out suspicious SMSes, while the MAS and the Association of Banks in Singapore introduced further measures to counter scams. These measures include the removal of clickable links in emails or SMS messages, as well as the implementation of an emergency self-service "kill-switch" for digital banking. The CSA has played a crucial role in supporting these collective endeavours. By investigating thousands of suspicious phishing URLs, the CSA has contributed to the detection and prevention of scams. In collaboration with the SPF, the CSA has also prioritised public awareness by regularly issuing alerts and advisories, educating the public about the latest scam campaigns and techniques.

The impact of cybercrimes such as scams is typically measured in financial loss, but the emotional toll it takes on individuals - such as anguish, confusion, and distress - is immeasurable. In this issue of SCL, we offer perspectives from individuals who have fallen victim to ransomware incidents and insights from an incident responder to provide first-hand experiences of the impact of cybercrime, prevention measures, and response strategies. I found these real accounts enlightening, and hope readers will find them helpful in your cybersecurity journey. To further align with this focus on the impact on individuals and organisations, the government has adjusted its reporting methods for key malicious cyber activities to emphasise their impact on Singaporeans and what measures are being taken to address them.

The old adage of 'prevention is often better than cure' still rings true for cybersecurity. With the rapid pace of digitalisation, it is more important than ever for the public and organisations to assess their cybersecurity posture and adopt good Internet security practices. Unfortunately, during the pandemic, cybersecurity can be overlooked in the rush to get services online. To address this issue, Senior Minister and Coordinating Minister for National Security Teo Chee Hean launched CSA's one-stop Internet Hygiene Portal (IHP) in October 2022. Since its launch, the IHP has been used by more than 60,000 websites and email domains to assess their security and hygiene levels. Encouragingly, about 2,300 of these have shown improvement in their Internet hygiene after following the recommendations provided. By encouraging more organisations to follow suit, we can improve the overall cyber resilience of our ecosystems and ultimately make Singapore cyberspace more secure.

In past issues of SCL, I usually conclude by looking forward to pressing cybersecurity issues for the coming year. Unsurprisingly, 2023 has been dominated by the game-changing race to launch Artificial Intelligence (AI) chatbots. With ChatGPT, Bard and other chatbots showcasing increasingly astounding capabilities, cybersecurity experts warn of their potential abuse to enable malicious cyber activities. Emerging technologies like these are double-edged, as with digitalisation. While we should be optimistic about the opportunities it brings, we have to carefully manage its accompanying risks to fully reap the benefits of our digital future.

Mr David Koh
Commissioner of Cybersecurity and
Chief Executive
Cyber Security Agency of Singapore

GLOBAL TRENDS IN 2022

2022 saw significant developments in the global cybersecurity landscape. In this chapter, we take a closer look at three trends that dominated headlines over the past year: cyber threats targeting Operational Technology (OT) systems, the continued evolution of the ransomware threat, and the cybersecurity implications of the Russia-Ukraine conflict.

Cyber Threats Targeting OT Systems: Evolution of Carnage

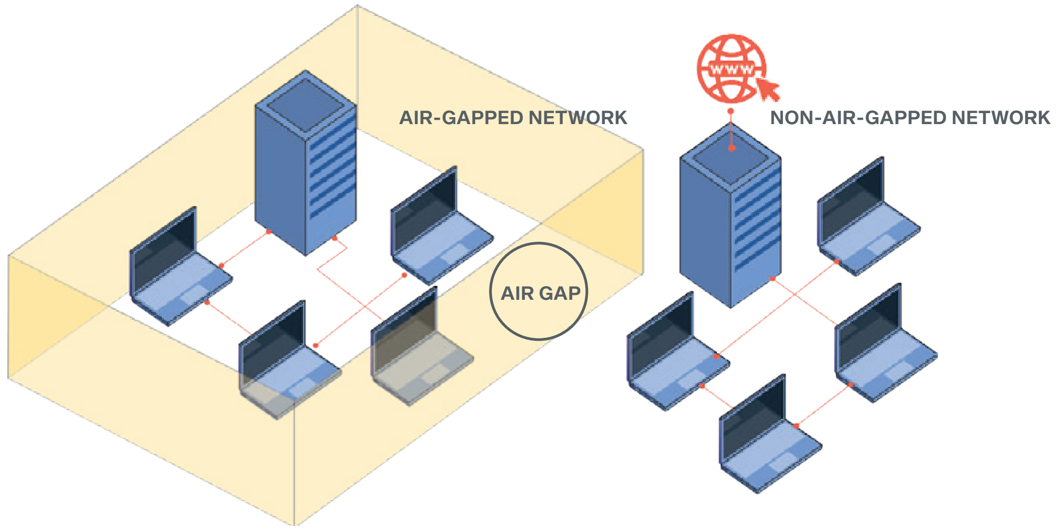


Figure 1: Graphical representation of an "air-gapped" system which is used in many OT environments. Such systems are not directly connected to the internet. Data can only be passed to it physically (e.g. via USB or removable media with another machine).[1]

Ever since the computer worm Stuxnet disabled Iran's Internet-disconnected Natanz nuclear facility in 2010, threat actors have been researching and refining similar methods to strike targets. Like Stuxnet, these focus on altering the behaviour of Operational Technology (OT) systems used to manage industrial operations, to effect complete or partial shutdown of important facilities and equipment. By doing so, the malware could have caused harm to human lives, physical damage, and financial loss. Given the high potential for disruption and destruction, they are widely regarded as national security concerns. As we shall see, such threats have come a long way in the 13 years since Stuxnet first crossed the theoretical barrier that divided our cyber and physical worlds.

Background: What are OT Systems?

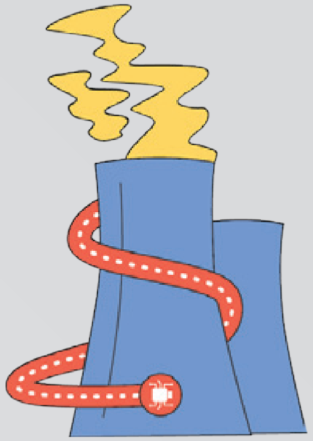
OT systems are designed to interact with machines and are found in a diverse array of automated and industrial applications, from factories to power plants, many of which are involved in the provision of essential services. For this reason, such systems are almost always found in protected environments, and managed and monitored separately from Internet-facing IT systems.

In addition, given the criticality of the infrastructure they control, OT systems are usually isolated or "air-gapped" from IT networks, running in separate and siloed environments away from the Internet (See Figure 1). In theory, while this made it extremely challenging for cyber-attacks to affect OT systems, threat actors have succeeded in crossing the "air gap" with highly customised and sophisticated malware.The attack surface is also expanding with the introduction of the Industrial Internet of Things (IIoT) revolution, which sees OT systems becoming increasingly connected to IT systems to allow their infrastructure to be controlled and monitored remotely.

[1] "Air Gapping for Enterprise Cybersecurity – What, Why, How - The K7 Security Blog," 7 October 2020, https://blog.k7computing.com/air-gapping-for-enterprise-cybersecurity-what-why-how/

KEY INCIDENTS

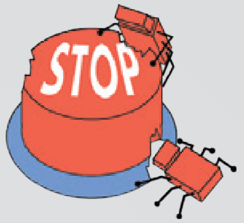
Major cyber-attacks against OT systems over the past 13 years include:



Stuxnet

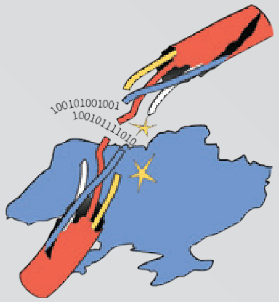
A multi-stage computer worm specifically designed to cross the gap to target programmable OT systems by several manufacturers and cause them to malfunction, while providing a false picture of normalcy to system monitors. Stuxnet was used to target Iran's Natanz nuclear-enrichment facility in 2010, causing affected centrifuges to behave erratically, resulting ultimately in equipment failure and shutdown.

Triton



Triton is regarded as the first malware known to target Safety Instrumented Systems (SIS). These systems are responsible for the operational safety of equipment and ensuring the emergency stoppages of systems when necessary. Once deployed on a safety engineering workstation, the malware can exploit a zero-day vulnerability that enables attackers to execute codes on safety controllers, which are usually the last lines of defence preventing dangerous industrial accidents. Triton was used against a Saudi Arabian petrochemical facility in 2017, with the likely intention of causing a major accident.[2]

Industroyer



A malware deployed in the 2016 attacks on Ukraine's electrical grid. This malware targeted several OT systems to orchestrate a massive outage across the country, disabling protective relay devices that cut off power to ignition systems. Prior to the Russian invasion of Ukraine in February 2022, a Ukrainian energy provider was targeted by a modified and enhanced version of the Industroyer malware, which tried to disable its electrical substations. Ukraine Computer Emergency Response Team (CERT) reported that the cyber-attack was unsuccessful.

Incontroller or Pipedream

A malware package (or attack toolkit) of custom-made tools targeting OT systems and Supervisory Control and Data Acquisition (SCADA) devices that can scan, compromise and control affected devices once they have established initial access to the OT environment. It was discovered by researchers in April 2022, as it was being readied for use against US Critical Infrastructure (CI). Incontroller was specifically developed by threat actors to disrupt industrial processes and has been described by researchers as a "Swiss Army knife" for cyber-attacks against OT systems. It incorporates an expansive array of modules that can disrupt or prevent operators from accessing devices, permanently disable them, or leverage them to access other parts of the network. Such malware may also include wiper capabilities as just one among many functionalities within their arsenal. What sets Incontroller apart from other OT systems malware is its adaptability and multi-functionality, which could pose a threat to almost all types of industrial systems around the world. Fortunately, the malware was discovered before it could be used, and mitigation measures were quickly implemented to protect vulnerable systems.

[2] The malware was extremely stealthy and was uncovered because the hackers made a mistake and triggered the safety system leading to a shutdown of the plant. This prevented the release of toxic gases or explosions, which could have put lives at the plant and its surrounding areas at risk.

How OT-targeting Malware Works

As in all cyber-attacks, the malware carries out reconnaissance in the first stage, allowing attackers to survey the targeted network environment. This allows the attacker to understand the target's security posture, including how the OT and IT networks interface with each other, and to identify the "air gaps". By properly researching the target, attackers can identify potential points of entry into those networks.

In the second stage, threat actors 'engage' with their target to achieve intrusion into the latter's network. In the case of an OT environment, threat actors can accomplish this via removable media and devices (e.g. USB sticks, cables), through unsecured links between an organisation's IT-OT systems, or through an IIoT interface.

Thereafter, in the third stage, threat actors can employ different tactics to accomplish their objectives:

- In the case of systems that can be controlled remotely – such as SCADA systems – this might mean gaining control of a management workstation, which can then be used to make changes on the target system, and/or hide valid alerts.
- Alternatively, malware can directly target individual components to cause malfunction. One instance would be to change the state of control system hardware – such as Programmable Logic Controllers (PLCs) – and making them operate beyond safe parameters with the intention of causing an accident.
- Some malware also target adjacent IT systems to cause disruption as well. One example of this would be ransomware, which rarely have the capability to affect OT-controlled infrastructure. However, it can still cause operations to fail when deployed on workstations intended to run OT systems.

Defending Against OT Systems Attacks

Threat actors have, and will, deploy OT-targeting malware against weak links in such systems. However, the emergence of Pipedream is an indication of the increasing sophistication and capability of threat actors in manipulating and disrupting industrial systems and processes. Pipedream is particularly troubling given the breadth of its functionality which expanded its capabilities, thus setting it apart from other OT-targeting malware (e.g. Stuxnet, Triton, which were purpose-built to target one particular network, with specific equipment and controllers from a particular vendor). The growing nexus between IIoT applications and OT, which sees the latter become increasingly connected to IT systems to allow their infrastructure to be controlled and monitored remotely, will also expand the attack surface further.

IMPLICATIONS

While it is very difficult to completely prevent a highly motivated and technically sophisticated threat actor from accessing critical networks, strong cyber hygiene across business, IT and OT networks can make lower-level or accidental intrusion much less likely and make purposeful intrusion significantly more expensive and less attractive. Fast and effective recovery is also crucial. This means it is essential to conduct secure, offline backups of OT critical systems and device configurations, test critical system resilience, and practice recovery on a routine basis.

Ransomware in 2022: Colossal Collective Challenge

Ransomware was a near-universal cyber threat in 2022, posing a severe threat to almost every industry and government in the form of significant disruptions to business operations, essential services, and by extension, people's way of life. Organisations within 14 of the United States' (US) 16 CI sectors were victims of ransomware attacks last year, as highlighted in the US Federal Bureau of Investigation's (FBI) Internet Crime Report 2022. Disruptions to these essential firms can often manifest real-world impact across all levels of society. This was evidenced in April 2022, when a series of crippling ransomware attacks by the Conti ransomware group targeting around 30 Costa Rican government institutions brought the country to a virtual standstill, with the public cut off from online services and a state of emergency declared.

The government sector and healthcare sector were prime targets for ransomware attacks (See Figure 2). There appeared to be an increase in ransomware attacks on the education sector, e.g. Knox College in the US and Queensland University of Technology in Australia in December 2022.

Figure 2: Top three sectors targeted by ransomware attacks in 2022 as reported by cybersecurity organisations

BlackFog[3]	Cybereason[4]	Emisoft[5]	FBI's Internet Complaint Center[6]	Trend Micro[7]
Education	Legal	Local Governments	Healthcare and Public Health	Government
Government	Financial Services	Education	Critical Manufacturing	Manufacturing
Healthcare	Manufacturing	Hospitals (Healthcare)	Government Facilities	Healthcare

[3] https://www.blackfog.com/the-state-of-ransomware-in-2022/
[4] https://www.cybereason.com/ransomware-the-true-cost-to-business-2022
[5] https://www.emsisoft.com/en/blog/43258/the-state-of-ransomware-in-the-us-report-and-statistics-2022/
[6] https://www.bankinfosecurity.com/healthcare-most-hit-by-ransomware-last-year-fbi-finds-a-21315
[7] https://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup/rethinking-tactics-annual-cybersecurity-roundup-2022

In Singapore, ransomware incidents reported to Singapore Cyber Emergency Response Team (SingCERT) remained high at 132 cases in 2022, a slight 4% dip from the 137 cases reported in 2021. Organisations most affected comprised Small and Medium Enterprises (SMEs) in the manufacturing and retail sectors. These figures, however, are not likely to represent the full extent of the ransomware threat as not every victim will report an attack. For instance, only 20% of US ransomware victims reached out to law enforcement for help, according to the FBI's estimates.

The continued proliferation of Ransomware-as-a-Service (RaaS) affiliate models means that anyone with the resources to buy such a service can launch a sophisticated ransomware attack, thereby substantially amplifying the ransomware threat.

In addition to their increasing audaciousness, ransomware groups exhibited more commercial and professional-like behaviour in 2022, diversifying their portfolios to target Cloud environments and Linux systems, and adopting malware-free attacks. Their negotiation tactics became more aggressive, amidst falling ransomware revenue and concerted, coordinated global efforts to counter their nefarious operations. We take a closer look at several of these traits.

Corporate Branding and Customer-centricity

Ransomware groups have evolved to become even more commercial and professional-like in 2022. They are now branding their ransomware and ransom notes with a distinctive logo and style as a form of brand identity. This could be an attempt by ransomware groups to cultivate a public profile, in order to reassure victims that they will regain access to their data once the ransoms are paid. Many groups now provide "customer support" functions to help victims through the ransom payment and file decryption processes, making their own remuneration process smoother and closer to a legitimate business transaction. Most offer the option of a small fee to extend the payment deadline and impose a penalty for missing the ransom payment deadline, not unlike how credit card companies offer the option of paying a minimum sum on your bill to avoid the late payment penalty on the full sum.

A March 2022 report by Check Point Research revealed the inner workings of the now defunct-Conti ransomware group, outlining a setup akin to a tech startup, with a structured hiring process, salaries, and bonuses. The image-conscious Conti subsequently shut down and rebranded itself as several smaller ransomware groups in mid-2022 following negative reactions arising from its conspicuous affiliation with Russia amidst the ongoing Russia-Ukraine conflict. Former Conti members purportedly now operate the splinter Black Basta, BlackByte, Karakurt and Royal ransomware groups.

Such groups will continue to evolve in tandem with myriad geopolitical and economic developments. With ransomware revenue falling to US$456.8 million in 2022 from US$765.6 million the year before[8], ransomware groups are now looking to seek out "new markets" just like what legitimate businesses would do.

Cloud We Go and They Follow (and Linux Next?)

Increasingly, ransomware groups are turning their attention to cloud services and infrastructure as more organisations move their assets and data to the cloud. Check Point Research's examination of the cloud-based networks landscape found that there was a significant 48% growth in cloud-based network attacks in 2022, particularly in Asia, which saw a 60% year-on-year growth. CrowdStrike's 2023 Global Threat Report paints a starker picture: Observed cloud exploitation cases grew by 95% over the course of 2022, and cases involving cloud-conscious actors nearly tripled from 2021, albeit not all are ransomware groups.

Cloud services are interconnected, which means compromising one system could enable the ransomware to spread rapidly to the many connected systems and organisations. Managed service providers for the cloud are thus prime targets for ransomware attacks because a single breach can impact many downstream customers. As cloud security is a shared responsibility between the vendors and customers, cloud-oriented ransomware attacks may sometimes occur due to misconfiguration or unpatched vulnerabilities on the customers' end, because of confusion over each party's cybersecurity obligations. For instance, the series of VMWare ESXi ransomware attacks in February 2023 which impacted over 3,800 servers had exploited a two-year-old vulnerability. This meant that the impacted customers were likely running out-of-date or unpatched versions of the VMWare ESXi software.

The increase in cloud-oriented ransomware attacks is just one manifestation of ransomware groups diversifying their portfolios in tandem with the evolving business environment. Trend Micro also observed ransomware groups such as BlackCat, Hive and RansomExx develop versions of their malware in the cross-platform language Rust, enabling them to customise their malware for both the Windows and Linux operating systems (OS) according to what their targets use. Rust is purportedly more difficult to analyse and has a lower detection rate by antivirus software, making it more appealing to ransomware groups. Specifically, Trend Micro's findings highlighted a significant increase in Linux OS being targeted from 3,790 instances in 2021 to 27,602 instances in 2022.

[8] The 2023 Crypto Crime Report, Chainalysis, February 2023

This diversification in portfolios ties in with some ransomware groups adapting their tactics and techniques, including employing more aggressive techniques to effectively coerce victims into paying up.

Coercion by Any Mode or Means

There was continued growth in malware-free ransomware attacks in 2022 as evidenced in various cybersecurity vendor reports. For instance, CrowdStrike highlighted that such attacks accounted for 71% of its detection, as compared to 62% the year before. These attacks do not involve infecting the victim's system with malware to encrypt their data to hold it hostage, but instead focus on directly exfiltrating their data (particularly those of a sensitive nature) to coerce victims into paying for fear of it being leaked publicly. Such extortion-only tactics are sometimes referred to as "data-kidnapping". Notable examples of ransomware groups adopting extortion-only tactics are Lapsus$ which claimed multiple high-profile attacks against tech companies such as Nvidia and Samsung, and Karakurt which targeted Methodist McKinney Hospital and other healthcare institutions in the US.

This growth in the malware-free mode of ransomware attacks might have been sparked by several reasons:

(i) the absence of a malware payload and a protracted encryption process makes such ransomware attacks harder to detect and stealthier,

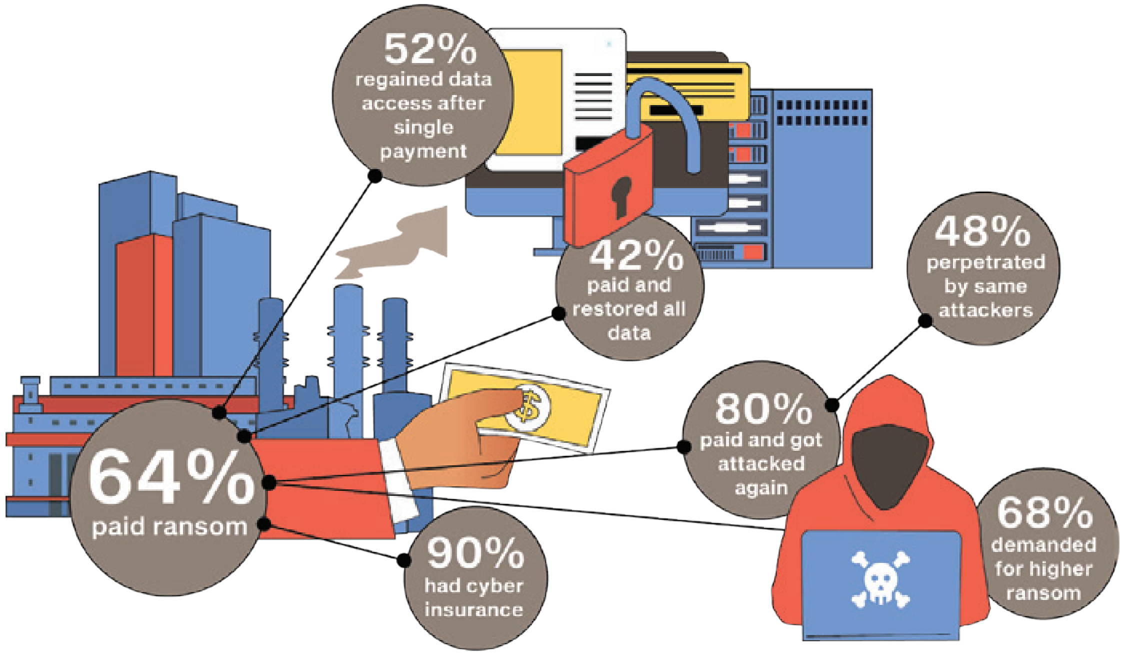
(ii) they abuse valid credentials and legitimate tools in the victim's environment (e.g. PowerShell), which is perceived by attackers to be more reliable, and

(iii) it allows ransomware groups to focus on expanding their attacks towards maximising profits, without worrying about upkeeping their encryption malware.

Ransomware groups are also resorting to increasingly aggressive tactics to coerce victims to pay up in "data-kidnapping" incidents, akin to physical kidnapping cases where the perpetrators coerce the victims' families to pay up by threatening bodily harm. For instance, in February 2023, the BlackCat ransomware group leaked several personally intrusive photos of cancer patients receiving radiation treatment at the Leigh Valley Health Network, when the latter refused to pay its US$1.5 million ransom. In February 2023, the Medusa ransomware group likewise released a 51-minute-long video showcasing sensitive data stolen from Minneapolis Public Schools, when the school district refused to pay its US$1 million ransom. The video purportedly included student sexual violence allegations, student discipline records, civil rights investigations, student maltreatment cases, and sex offender notifications.

Both Leigh Valley Health Network and Minneapolis Public Schools refused to pay the ransom. However, many organisations did so in other ransomware attacks, often with an unexpected negative outcome.

Key statistics on ransom payment, as reported by cybersecurity vendors


52% regained data access after single payment
42% paid and restored all data
48% perpetrated by same attackers
80% paid and got attacked again
64% paid ransom
90% had cyber insurance
68% demanded for higher ransom

Paying Up Does Not Pay

Research by cybersecurity vendor Proofpoint highlighted that up to 64% of organisations impacted by ransomware ended up paying the ransom. This could be because 90% had cyber insurance, and their insurers were generally willing (82%) to pay up. Worryingly, only half (52%) of these victims regained access to their data after making a single ransomware payment. Nearly as many were hit with further ransom demands. Such findings were echoed in Cybereason's research, which underscored that only 42% of organisations that paid the ransom managed to restore all their systems and data. 54% still encountered system errors and corrupted data after decryption using keys provided by the attackers. Nearly 80% of organisations that paid the ransom were hit by a second ransomware attack, 48% of which was perpetrated by the same attackers, and 68% demanding a higher ransom. In addition, nearly 60% of organisations were unable to recover all their systems and data even after paying up, meaning there are no guarantees that organisations will regain full access to their data. Worse, it sets a dangerous precedent that they are willing to pay, making them a target for future attacks. It creates a vicious cycle that emboldens ransomware groups, making them more likely to increase the scale and extent of ransoms demanded in future attacks on others.

Increasingly prevalent and larger-scale ransomware attacks can pose a threat to economic prosperity, public safety, and even national security, thus presenting a colossal collective challenge. As such, coordinated international efforts have been made to crackdown on the global ransomware scourge.

Fighting Back: Coordinated International Ransomware Crackdown Efforts

Officials from 36 countries and the European Union (EU) met in the US in October 2022 to address the global threat of ransomware at the second international Counter-Ransomware Initiative (CRI) Summit. Alongside private sector partners, the international community discussed and developed concrete, cooperative actions to stem the extent and impact of ransomware globally. The CRI will further its work in 2023 through three pillars:

(i) the Policy Pillar led by Singapore and the United Kingdom (UK),
(ii) the Diplomacy and Capacity Building Pillar led by Germany and Nigeria, and
(iii) the International Counter-Ransomware Task Force, coordinated by Australia.

One notable success story of similar global efforts was the FBI's January 2023 announcement of a months-long US-led international campaign to disrupt the Hive ransomware group responsible for targeting over 1,500 victims in more than 80 countries for over US$100 million in ransoms. Such high-profile operations have the potential to significantly undermine the RaaS economy by visibly hampering one of the most prolific groups.

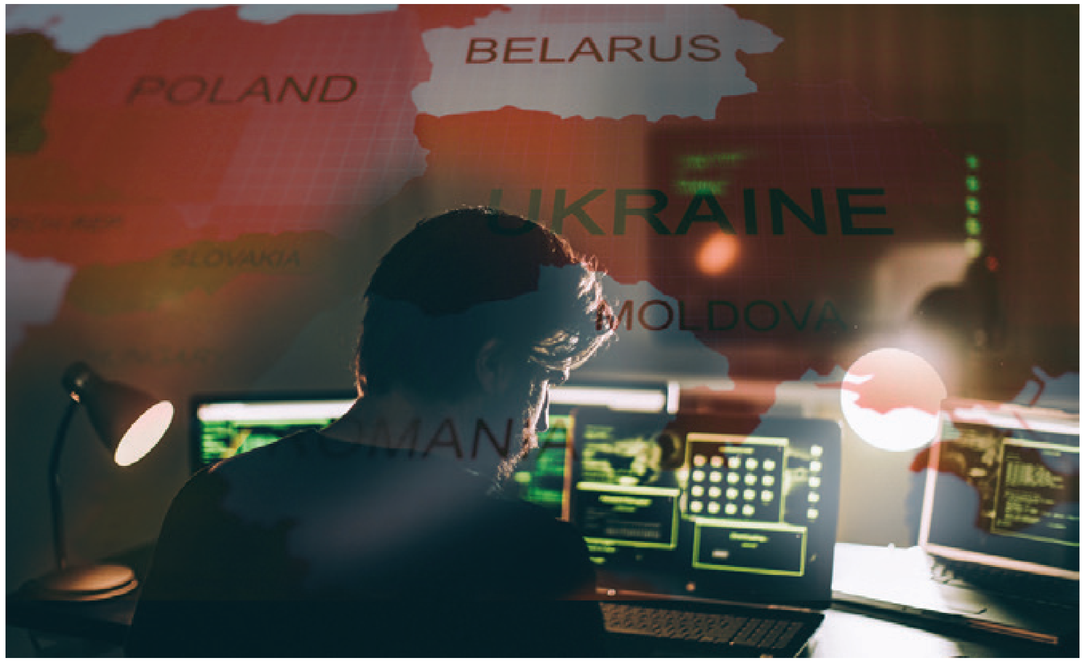
The local parallel to the CRI is Singapore's CRTF established in 2022 to bring together government agencies across relevant domains to strengthen our national counter-ransomware efforts. More information on the CRTF's upcoming initiatives can be found in Chapter 3.

IMPLICATIONS

Ransomware continues to be a borderless threat that shows no sign of letting up in 2023. BlackFog's tracking indicates that there have been 73 publicly disclosed ransomware attacks globally by end-February 2023, with potentially up to 543% more attacks (i.e. 396) going unreported. Ransomware attacks are a clear demonstration of how cyber incidents can have significant real-world consequences. The January 2023 ransomware attack on the Royal Mail in the UK, for example, disrupted the overseas delivery of parcels and letters for two weeks. In March 2023, a ransomware attack on the Hospital Clinic de Barcelona in Spain shut down the facility's emergency rooms, laboratories and pharmacy at three centres and several external clinics, resulting in the cancellation of up to 3,000 patient check-ups and 150 non-urgent operations.

CSA is closely monitoring local developments in ransomware attacks and working with our international counterparts on collective efforts to counter the global ransomware threat. We have issued several advisories on steps that organisations and individuals can take to protect themselves, many of which relate to basic cyber hygiene practices. Organisations with a robust cybersecurity posture will invariably fare better against ransomware as illustrated by a case study in Chapter 4 that outlines how a Singapore-based precision engineering company managed to regain access to its systems and data without paying the ransom.

Cybersecurity Implications of the Russia-Ukraine Conflict: A Year On



More than a year has passed since Russia invaded Ukraine in late February 2022. What has the past year taught us about the role of cyber in a modern conflict?

Since the onset, Ukraine and other countries such as the US, UK and Australia have accused Russia of carrying out disruptive wiper malware attacks and influence operations. The attacks primarily targeted Ukraine, but some – such as the attack on satellite communications provider Viasat in February 2022 – also affected countries and entities not directly involved in the conflict.

Researchers are not surprised by the use of cyber by state-linked actors to support the military invasion. What was surprising was the extent of involvement that non-state actors have had in the cyber conflict. This article discusses the rise of two particularly prolific groups of non-state actors – namely, hacktivists and Big Tech companies – and examines how their involvement has shaped the conflict and the global cybersecurity landscape.

Rise of Hacktivism

Two days after Russia's invasion of Ukraine, Ukraine's Vice Prime Minister and Minister for Digital Transformation, Mykhailo Fedorov, announced the creation of the government-sanctioned volunteer army, "IT Army of Ukraine". He called for volunteers in Ukraine's hacker underground to provide cyber defence for Ukraine's critical infrastructure and to carry out offensive cyber operations against Russia-linked entities.

The formation of the "IT Army of Ukraine" is unprecedented. It quickly led to a call to arms by various groups, including the Anonymous collective and self-declared hacktivist group AgainstTheWest (previously known for leaking data obtained from the Chinese Communist Party) and hundreds of thousands of netizens to take up digital arms in support of Ukraine.

Since then, other hacker groups have also taken sides. Pro-Russia hacktivist groups, such as Killnet, rallied against countries they felt were acting in an "unfriendly" manner towards Russia – including but not limited to the US, Germany, UK, Italy, Spain, Norway and Japan.

Over the past year, reports of hacktivist activities have continued at a brisk pace. In their attempts to shape the global narrative and discourse about the war, hacktivists have engaged in a series of disruptive Distributed Denial-of-Service (DDoS) attacks and hack-and-leak campaigns targeting both public and private organisations from military entities and government ministries, to energy, banking, and even healthcare institutions.

But this rise of hacktivism is not without risks. As non-state actors, hacktivists often lack the coordination and discipline to prevent collateral damage or unintended effects on uninvolved parties. For example, in March 2023, hacker group Anonymous claimed credit for an attack on the servers of Russian radio stations and TV channels to broadcast fake air raid warnings in at least 10 cities, inducing panic among Russian civilians.

Some researchers have also observed hacktivist activities taking a more dangerous turn over the course of the war. Beyond DDoS attacks and data leaks, some hacktivists are employing ransomware and destructive malware on critical infrastructure to disrupt essential services. For instance, pro-Ukraine hacktivist group NB65 claims to have used Conti's leaked ransomware in a series of attacks to disrupt the operations of Russian entities. However, other researchers have noted that that the impact of hacktivist activities still pales in comparison to military campaigns and is unlikely to significantly shift the course of the war.

IMPLICATIONS

Regardless of their direct impact, the involvement of hacktivists has increased the level of unpredictability and instability of the cyber landscape amidst the Russia-Ukraine conflict. Any serious cyber incident triggered by the hacktivists may inadvertently escalate the conflict – or be used as a pretext by either side for escalation. Globally, the resurgence of hacktivism poses an increased risk of collateral damage and unintended effects on uninvolved countries. As the conflict enters its second year, organisations are reminded to remain vigilant, and take the necessary actions to review their security preparedness and strengthen their cybersecurity posture.

Role of Big Tech

The conflict has also been characterised by the unprecedented involvement of "Big Tech" companies.

The impact of Big Tech is highly visible in our everyday lives. They supply technology and platforms used daily by billions of individuals and organisations around the world. However, in the arena of geopolitics – traditionally the domain of nation states – Big Tech has often opted to remain in the background, avoiding the need to pick sides to minimise losses to its bottom line.

This was not the case in the Russia-Ukraine conflict. Over the past year, many Big Tech companies have publicly and actively taken sides, demonstrating their support for Ukraine in various ways. Many, including Google, IBM and Microsoft, announced the suspension of some or all of their business activities in Russia at the start of the conflict. Social media platforms blocked access to Russian state media from their sites. Facebook and Instagram removed Russian state media from their platforms in Europe, whereas Google dropped Kremlin content from Google News.

Some Big Tech companies went a step further, providing tactical support to Ukraine on the physical and cyber battlefields. In the early days of the conflict, Microsoft reportedly worked with the Ukrainian government to transfer important digital operations and data to the cloud within 10 weeks. They also provided cybersecurity services to protect Ukrainian critical infrastructure from cyber-attacks. Google supported Ukraine's efforts to protect civilians on the ground when they disabled some live features on their Maps applications in Ukraine to protect the safety of local communities, and introduced a rapid Air Raid Alerts system for Android phones in Ukraine, at the request of, and with the help of the Ukrainian government.

The impact of these moves has not been insignificant. In response to Meta's move to restrict access to Russian media on their platforms, both Facebook and Instagram have been banned by Russia. According to reports, this could have cost Meta close to US$2 billion in revenue. Despite these potential revenue losses, Big Tech companies continue to play a key role in the Russia-Ukraine conflict, demonstrating an unprecedented willingness to support a geopolitical cause – even if it comes at a short-term cost to their bottom line.

IMPLICATIONS

By deciding what capabilities to supply and to whom, Big Tech has demonstrated that they too can have an independent voice on the international stage, and can play a part in shaping geopolitical and wartime developments. However, this raises the question of who in these Big Tech companies makes these decisions – whether it is the CEO, the shareholders, or even the employees. As the size of Big Tech companies continue to grow, so too will their influence and impact on future cyber conflicts and the global cyber landscape.

WWW.TARGET.SG

This chapter presents the key trends and statistics of malicious cyber activities observed in Singapore's cyber landscape in 2022. Ransomware and phishing remained persistent threats locally, with more than one ransomware case reported every three days, and phishing attempts more than doubling over the past year. In contrast, there was a decrease in web defacements and infected infrastructure, marking a general improvement in local cyber hygiene levels amidst the heightened threat landscape.

Starting with this issue, CSA has revised our reporting method for malicious cyber activities, to provide better understanding of their impact on Singapore entities:

- **Instead of reporting phishing URLs which measure potential threat activity, we will publish the number of phishing attempts reported, which measure actual threat levels.**
- **To provide a better sense of the level of local cyber hygiene, the previously separate categories of command and control (C&C) servers and botnet drones will be combined into a single category known as infected infrastructure.**

All statistics in this issue have been generated using this new methodology.

OVERVIEW OF CYBER THREATS OBSERVED IN SINGAPORE IN 2022

Phishing Attempts: 8,500 cases

KEY TRENDS

- **Around 8,500 phishing attempts** handled by SingCERT in 2022, **more than double** the 3,100 cases handled in 2021, mirroring global trends[1].
- Most spoofed: **Banking & Financial Services, Government, and Logistics.**

WHAT DOES THIS MEAN?

- As a result of CSA's consistent outreach and engagement efforts, public awareness of phishing threats is growing. More members of the public are actively reporting phishing cases to SingCERT.
- Nonetheless, the continued rise in phishing cases, both in Singapore and worldwide, highlights the need for individuals and organisations to remain vigilant.

WHAT CAN WE DO?

- SingCERT **investigates reported cases** and reports malicious URLs to relevant parties for takedown and/or blocking, and will publish an alert/advisory if a mass phishing campaign targeting Singapore is detected.
- In 2022, SingCERT facilitated the takedown of 2,918 malicious phishing sites, and published 98 alerts and advisories.
- Individuals and organisations can do your part to keep our cyberspace safe by **reporting suspicious emails or websites via SingCERT's incident reporting form.**

Ransomware Incidents: 132 cases

KEY TRENDS

- **Number of reported ransomware cases remains high**, with 132 cases in 2022 (a 4% drop from 137 cases in 2021), amidst a continued growth in ransomware cases observed globally.
- Top targets: SMEs in **Manufacturing** and **Retail**.

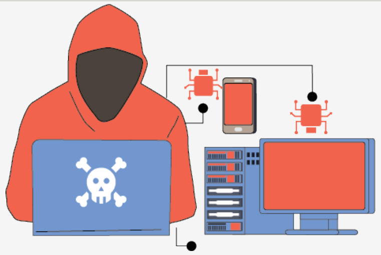
WHAT DOES THIS MEAN?

- **Ransomware remains a major issue both in Singapore and globally**, with cybersecurity vendors reporting a 13% increase in ransomware incidents worldwide in 2022.

WHAT CAN WE DO?

- The Government convened an inter-agency CRTF to develop recommendations that will serve as a blueprint for Singapore to counter ransomware effectively (see pages 49 to 51 for more info).
- **Prevention is key to avoid falling victim to ransomware.** Organisations should take steps to secure their systems and backup critical data regularly.

[1] For comparison, based on the old reporting method, around 42,000 phishing URLs were observed in Singapore in 2022 – a 24% drop from the 55,000 phishing URLs in 2021.



Infected Infrastructure: 81,500 systems

KEY TRENDS

- 13% **decrease** in infected infrastructure in Singapore, from 94,000 in 2021 to 81,500 in 2022, despite a sharp growth of infected infrastructure observed worldwide.
- **Singapore's global share of infected infrastructure fell** from 0.84% in 2021 to 0.34% in 2022.

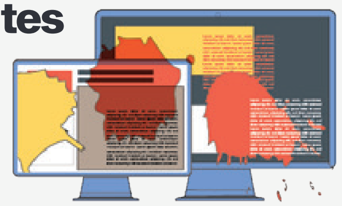
WHAT DOES THIS MEAN?

- Marks an improvement in cyber hygiene levels. However, the absolute number of infected infrastructure in Singapore remains high. This is partly because Singapore is a data and digital cyber hub.
- The attack surface will continue to grow, as users continue to connect more smart devices to the Internet. The average number of connected devices in Singapore households grew from 6.5 in 2020 to 7.0 in 2021[2].

WHAT CAN WE DO?

- As a responsible member of the global community, Singapore strives to prevent the abuse of our digital infrastructure. CSA regularly **informs hosting providers and Internet service providers** of reported botnet and C&C servers for their assistance with remediation.
- Individuals and organisations are reminded to **practise good cyber hygiene** to prevent their devices from being compromised and used by threat actors for malicious purposes.

Website Defacements: 340 websites



KEY TRENDS

- **Drop in the number of website defacements**, with 340 defacements observed in 2022 (a 19% decrease from 419 in 2021), mirroring global trends.

WHAT DOES THIS MEAN?

- Continued downward trend in website defacements since 2019, as hacktivist activities continue to move to other platforms with wider reach (e.g. social media).
- Nevertheless, organisations are reminded to ensure their websites are properly configured and updated to minimise the risk of website defacements as they can lead to significant reputational and brand damage.

WHAT CAN WE DO?

- **Organisations may use CSA's Internet Hygiene Portal (IHP) to perform a free check on the cyber health of their websites.**
- Since its launch in October 2022, **the IHP has been used by both local and overseas entities to conduct more than 60,000 (12,000 unique) website and email scans, with more than 2,300 scanned domains showing an improvement** in their Internet hygiene (see page 47 for more info).

[2] Based on Infocomm Media Development Authority's (IMDA) Annual Survey on Infocomm Usage by Individuals.

State of Singapore's Cyberspace

8,500 cases

174% ↑ from 2021

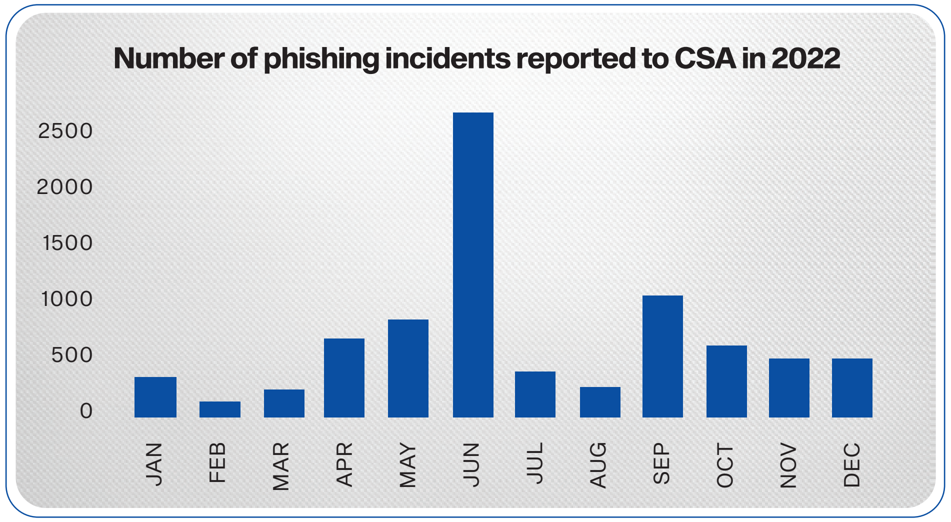
Phishing Attempts

A form of social engineering attack, and a common avenue for scams. According to data released by the Singapore Police Force (SPF), phishing scams remains the top scam type in Singapore, with more than 7,000 reported cases in 2022 (a 41% increase from 2021).

- Close to 8.500 phishing attempts were reported to CSA in 2022. This is more than double the 3,100 cases reported in 2021, mirroring global trends. This substantial increase highlights the need for individuals and organisations to remain vigilant to guard against phishing attempts.
- **Vector:** More than 50 percent of phishing attempts involved links with the ".xyz" domain. This is likely because .xyz domain registrations are relatively cheap (as little as US$1 compared to US$3 for .com domains), and can be purchased by malicious actors in bulk for use as part of the same phishing campaign.
- **Format:** The average length of reported phishing links was observed to have decreased by almost half, from 44 characters in 2021 to 26 characters in 2022. This could indicate that threat actors are using URL shortener services (such as bit.ly) to mask their intent and track the "performance" of their phishing campaigns.
- **Top Spoofed Sectors:**

I. The top spoofed sector was Banking and Financial Services, which made up more than 80% of all phishing attempts on organisations.

- Since 2016, it has consistently been in the top three sectors with the highest number of phishing attempts.
- They are often targeted by phishing attacks as they are trusted institutions which hold sensitive and valuable information (such as personal details and login credentials). Such information potentially allows threat actors to commit identity theft and other forms of fraud. Moreover, increasing digitalisation has expanded attack surfaces. Largely precipitated by the COVID-19 pandemic, customers have been moving to online banking in considerably larger numbers, leading to an uptick of malicious cyber activities, targeting organisations and individuals.
- June and September 2022 saw the highest number of phishing attempts from the sector. More than half of these attempts saw China-based banks spoofed. Interestingly, several of these banks — Agricultural Bank of China, Zhongyuan Bank, and China Minsheng Bank — have little to no presence in the Singapore retail banking scene and are unknown to most retail banking customers in Singapore. The threat actors were likely mass-targeting victims utilising the 'spray and pray' tactic, which capitalises on anxieties and concerns over developments in China's banking sector. A sharp spike in reported phishing attempts involving China-based banks was observed, coinciding with China's rural bank scandal[3] in June 2022. These attempts represented nearly 50% of all banking-related phishing attempts within 2022.

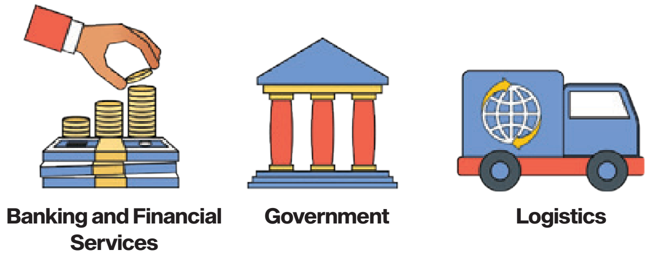

Number of phishing incidents reported to CSA in 2022

II. The second most spoofed sector was Government. The three most spoofed Singapore government-related organisations/services were the Land Transport Authority (LTA), Singpass, and Inland Revenue Authority of Singapore (IRAS). Many of these cases involved phishing emails or SMS messages exploiting the victims' trust in and tendency to comply with the authorities. The relevant government organisations have since issued advisories through various channels to warn the public of such phishing attempts.

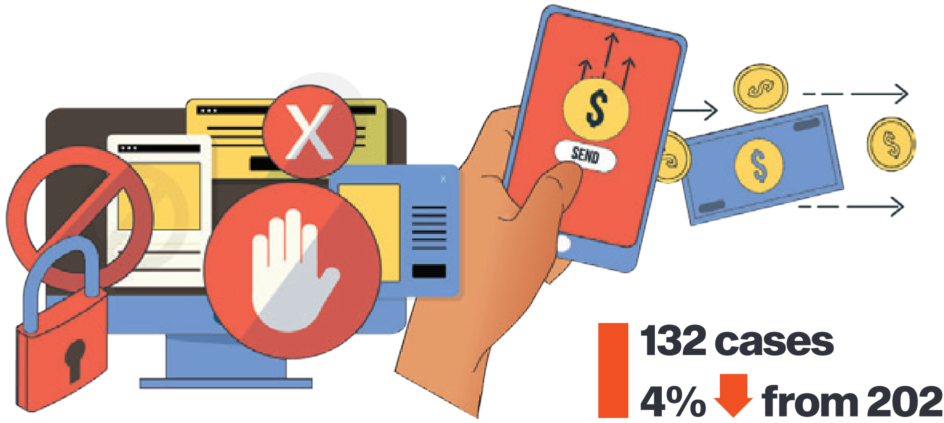
- There was a rising trend of phishing attempts targeting LTA from October to December 2022. These attempts used lures such as vehicle-related bills or fines, which proved compelling as a larger number of people returned to work following easing pandemic restrictions.

III. The third most spoofed sector was Logistics, with SingPost accounting for more than 80% of logistics-related phishing attempts via fake websites or SMS alerts. These phishing scams could be designed to target the online shopping habits of customers, with emails serving as fake notifications relating to incoming delivery, shipment issues, missing packages, etc.

Most spoofed industries



[3] China's rural bank scandal saw several banks in Henan province defaulting on their depositors.



132 cases

4% ↓ from 2021

Ransomware Incidents

A form of malware that encrypts files on a victim's device, rendering them unusable until a ransom is paid.

- Amidst a continued growth in ransomware cases observed globally, the number of reported local ransomware cases remained high at 132 cases in 2022, comparable to the 137 cases reported in 2021.

- **Top Affected.** In line with global observations, most victims were SMEs in the Manufacturing and Retail sectors. They are commonly targeted by hackers as: (i) they may hold valuable data as well as Intellectual Property (IP), which cybercriminals often seek to extort and monetise for financial gain; and (ii) they often lack dedicated resources to counter cyber threats.

- **Prevalent Strains.** RaaS ransomware strains observed in Singapore's cyber threat landscape continue to reflect global trends, and include LockBit, DeadBolt and MedusaLocker.

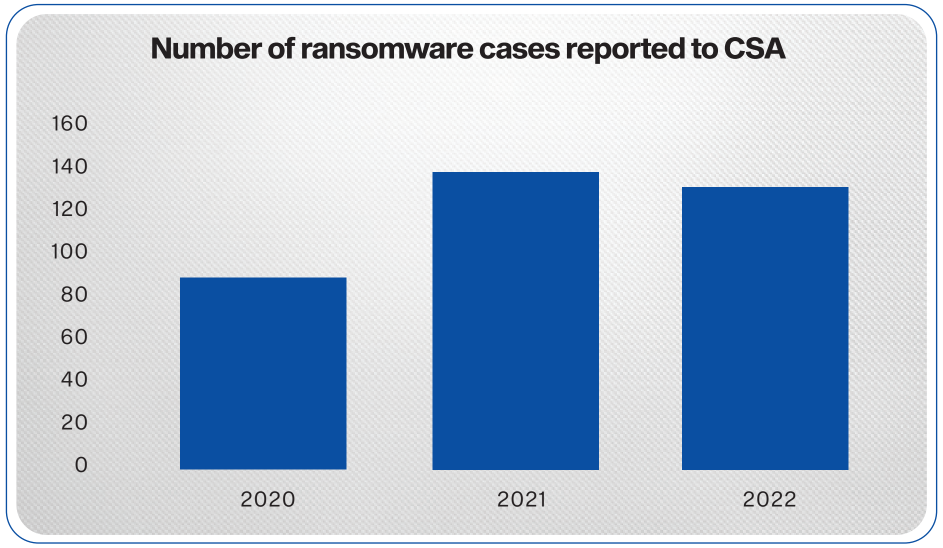
  - The majority of DeadBolt's Singapore-based SME victims saw their network-attached storage (NAS) systems (which allow network users data access) encrypted by the ransomware. While the actual intrusion vector remains unclear, global observations suggest that DeadBolt operators are widely targeting Internet-facing unprotected NAS systems. Organisations are encouraged to patch and update their Internet-exposed NAS systems regularly to prevent any security vulnerability from being exploited for ransomware attacks.

- **Global trends.** The ransomware ecosystem has become more complex and fluid, largely precipitated by government actions that force threat actors to find new ways to operate.

  - **Capability Integration.** This has seen groups reusing, borrowing or stealing capabilities from other cybercriminals e.g. LockBit ransomware gang's latest malware, LockBit 3.0, seems to have co-opted several capabilities from another RaaS strain, BlackMatter. These new capabilities have allowed LockBit 3.0 to self-propagate or spread on its own. After the threat actor manually infects a single host, the infection spreads through the victim network entirely without human intervention.

  - **Cross-operability.** Ransomware has also evolved to work across multiple operating systems, which makes executing attacks easier. This allows threat actors to be more efficient as they only need to write the malware code once and use it across multiple targets using Windows, Linux and Mac operating systems. Additionally, cross-platform ransomware both hampers analysis and allows threat actors to customise the attacks to specific environments, such as only attacking certain kinds of virtual machines. DeadBolt is an example of a prevalent ransomware strain written in a cross-platform language (i.e. Golang).

  - While MedusaLocker has remained largely unchanged since its inception in 2019, it was significant enough that a joint cybersecurity advisory was issued by the US FBI, the Cybersecurity and Infrastructure Security Agency (CISA), and Financial Crimes Enforcement Network (FinCEN) in 2022.[4] MedusaLocker generally exploits unpatched Remote Desktop Protocol vulnerabilities to give attackers access into victim workstations.



Ransomware strains observed
include LockBit, Deadbolt and MedusaLocker
that adopt the Ransomware-as-a-Service (RaaS) model

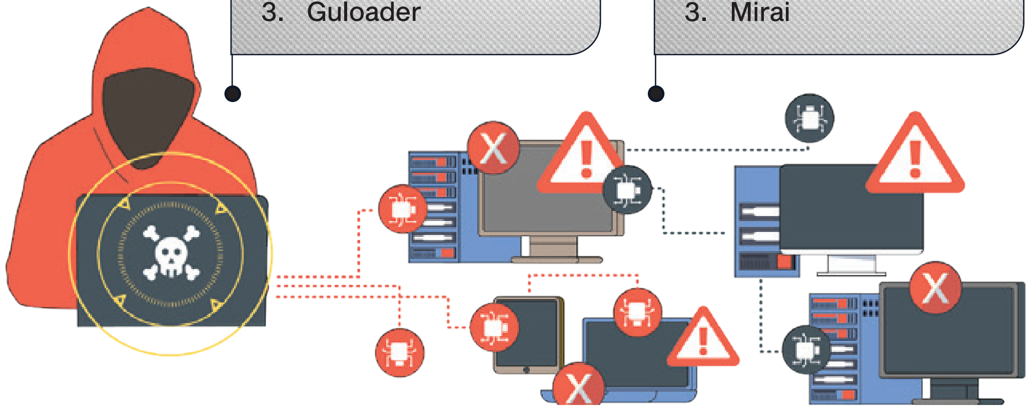
[4] #StopRansomware: MedusaLocker," CISA, 11 August 2023, https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-181a

Top three malware in infected C&C servers

1. Cobalt Strike
2. Emotet
3. Guloader

Top three malware in infected botnet drones:

1. Gamarue
2. Nymaim
3. Mirai



81,500 systems

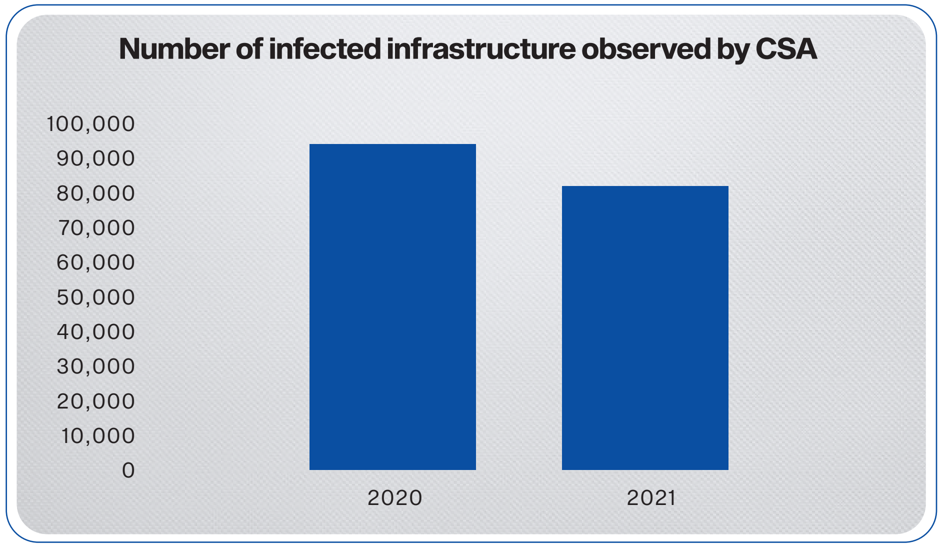
13% ↓ from 2021

Infected Infrastructure

[*Formerly known as Command & Control (C&C) Servers and Botnet Drones*]

Compromised devices abused by attackers for malicious purposes, such as conducting DDoS attacks or distributing malware and spam. Comprising "zombified" user devices (botnet drones) and the threat actors' C&C servers, this category provides an approximate gauge of the cyber hygiene level within the local digital landscape (since infections usually occur through unpatched vulnerabilities and weak passwords). As a responsible member of the global community, Singapore strives to prevent the abuse of our digital infrastructure for malicious purposes, whether locally or abroad.

- There was a slight decrease in the number of infected systems observed in Singapore, from 94,000 in 2021 to 81,500 in 2022 (a 13% decrease), despite a sharp growth of infected infrastructure observed worldwide.
- Singapore's global share of infected infrastructure fell from 0.84% in 2021 to 0.34 % in 2022. While this decrease points to an improvement in cyber hygiene levels, the absolute number of infected systems in Singapore remains high. This is partially because of Singapore's status as a data and digital infrastructure hub. Maintaining good cyber hygiene is crucial as users continue to connect more smart devices to the Internet. According to IMDA's Annual Survey on Infocomm Usage by Individuals, the average number of connected devices in Singapore households grew from 6.5 in 2020 to 7.0 in 2021[5].



Number of infected infrastructure observed by CSA

- Top three malware infections on locally hosted C&C servers:
  - Despite a significant fall of about 40% when compared to 2021, **Cobalt Strike** continues to top the list of malware families infecting locally hosted C&C servers. An infected server becomes a platform for threat actors to deploy a 'beacon' into targeted machines, providing the ability to execute commands remotely, log keystrokes, transfer files, etc.
  - Locally hosted C&C servers infected by **Emotet** mirrored global trends and developments i.e. a threefold increase was observed from 2021 to 2022. The resurgence of Emotet following its crackdown by law enforcement agencies in 2021 has been marked by more sophistication and evasion, making it more challenging for defenders to adapt and block the malware. For instance, previous iterations of Emotet typically installed the TrickBot or Qbot trojans to deploy Cobalt Strike on targeted devices. However, a new trend has seen Emotet malware installing Cobalt Strike beacons directly without these trojans, greatly accelerating attacks.
  - As a malware downloader used to proliferate various trojans, **Guloader** is constantly evolving with new techniques to evade detection. With Guloader applied to more remote access trojans and infostealers such as Netwire, FormBook and Agent Tesla, the malware has seen significant growth, globally and locally.
- Top three malware found on locally hosted botnet drones: **Gamarue**, **Nymaim**, and **Mirai** accounted for nearly 80% of Singapore IP addresses infected by malware in 2022. Notably, these three have remained some of the most prevalent in Singapore cyberspace since 2019. Gamarue steals personal information from affected systems, and like Nymaim, distributes other malware by acting as a downloader. Both malware accounted for about 60% of infected Singapore IP addresses collectively. Mirai and its associated variants predominantly exploit vulnerabilities (including weak/default login credentials) in Linux-based servers and Internet of Things (IoT) devices. A significant uptick in Mirai infections in Singapore from June 2022 till the end of the year corresponded to global campaigns to expand the botnet for conducting DDoS attacks during the same timeframe.

[5] The average number of computing devices that can connect to the internet at the household level, for households with internet connection at home and households without internet connection at home but have access to internet elsewhere. Computing devices refers to workable desktops, laptops/notebooks, tablets, and smartphones. These computing devices can belong to anyone in the household and does not differentiate between purchased devices and those issued by employer/school. Source: IMDA Annual Survey on Infocomm Usage by Individuals 2020–2021.

340 websites

19% ↓ from 2021

Website Defacements

Attacks on a website that alter its visual appearance or informational content without permission.

- 340 '.sg' websites were defaced in 2022, a decrease of nearly 20% compared to 2021. Locally, this continues an overall downward trend since 2019, as hacktivists could have continued to shift their activities towards other platforms with a wider reach, such as social media.

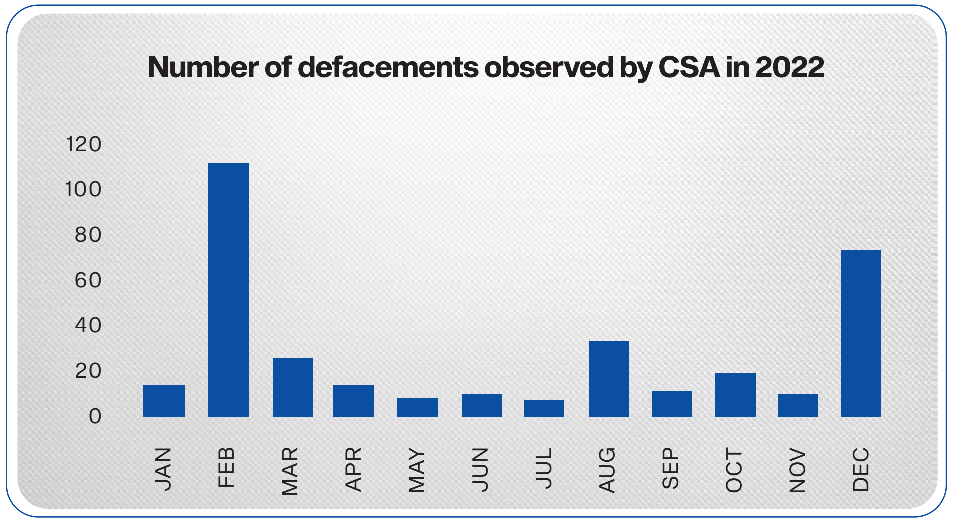
  In general, a downward trend in global website defacements was observed - with the exception of Ukraine and Russia, which has seen hacktivist activities spike amidst the ongoing conflict, including the defacement of more than 70 Ukrainian government websites just before hostilities broke out.

Example of defacement of the Dominican National Controller website by Hunter Bajwa.

- **Top affected.** Webpages of SMEs represented the vast majority of victims. No government websites were impacted.

- Noticeable spikes in website defacements were observed in February and December 2022, which were mostly contributed by the actors "Hunter Bajwa" and "B3g0k[Kurdish Hacker]", respectively.

  - These groups accounted for over half of total website defacements observed in 2022. Notably, both hackers launched their attacks on single-day periods, suggesting these were mass defacements of unpatched websites using automated scripts.



  - The attacks by both groups appear to be opportunistic in nature. Hunter Bajwa exclusively targeted Nginx web servers, suggesting that the hacker leveraged vulnerabilities in open-source web servers to carry out the defacement attacks. The group was observed promoting weblinks to sites that sold illegal programs for spamming purposes.

  - Despite the emergence of hacktivist groups over 2022, there was no significant uptick in Singapore website defacements due to the Russia-Ukraine conflict.

- Worryingly, re-defacements accounted for almost 40% of total observed defacements. In addition, websites published on the WordPress platform were the most defaced in 2022; about 60% were running on outdated versions (before Version 6.0) of WordPress. This highlights how some website owners are still negligent or even unaware of the need to regularly patch websites that are outdated or contain known vulnerabilities, which are often avenues for hackers to carry out defacements.

WHAT IS SINGAPORE DOING FOR A TRUSTED, RESILIENT AND SAFER CYBERSPACE?

The Singapore Cybersecurity Strategy 2021, outlines Singapore's updated goals and approach to adapt to a rapidly evolving strategic and technological environment. With talent and ecosystem development as the foundation, the Strategy seeks to actively defend our cyberspace, simplify cybersecurity for end-users, and promote the development of international cyber norms and standards.

The Strategy comprises three strategic pillars and two foundational enablers:

Strategic Pillar 1: Build Resilient Infrastructure
Strategic Pillar 2: Enable a Safer Cyberspace
Strategic Pillar 3: Enhance International Cyber Cooperation

Foundational Enabler 1: Develop a Vibrant Cybersecurity Ecosystem
Foundational Enabler 2: Grow a Robust Cyber Talent Pipeline

In this chapter, we look back at the key efforts in 2022 in support of the Strategy – how they strengthen the security and resilience of our digital infrastructure, enable a safer cyberspace to support our digital way of life, and how Singapore can support an open, secure, stable, accessible, peaceful, and interoperable cyberspace.

Strategic Pillar 1

Build Resilient Infrastructure

Strategic Pillar 2

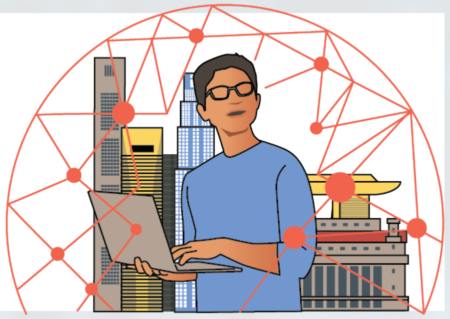
Enable a Safer Cyberspace

Strategic Pillar 3

Enhance International Cyber Cooperation

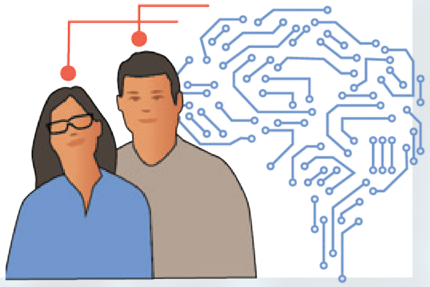
Foundational Enabler 1

Develop a Vibrant Cybersecurity Ecosystem



Foundational Enabler 2

Grow a Robust Cyber Talent Pipeline



Pillar 1: Build Resilient Infrastructure

Strengthen the security and resilience of our digital infrastructure

Guidelines and Legislation

Cybersecurity Code of Practice Second Edition

- On 4 July 2022, the Second Edition of the Cybersecurity Code of Practice (CCoP)[1] was issued to enable Critical Information Infrastructure (CII) Owners to achieve three objectives:
  - Improve their readiness to defend against cyber threat actors who use sophisticated Tactics, Techniques and Procedures
  - Be agile in responding to emerging risks in specific domains
  - To coordinate with the Government and the private sector to respond more readily to cyber threats

- The Second Edition of the CCoP focuses on:
  - Adopting a threat-based approach to identify threat actors' common tactics and techniques used in a cyber-attack life cycle. This will allow CSA to identify actions, develop new practices and/or enhance existing practices to counter and impede the threat actors' activities in a cyber-attack
  - Enhancing agility in addressing emerging risks by allowing the flexibility to add domain-specific practices e.g. guidelines on the use of 5G technologies in specific CII sectors

- Non-CII entities can also take reference from the CCoP to enhance the security and resilience of their systems and networks.

- For more information on the CCoP and CSA's responses to feedback received during consultations, please refer to https://go.gov.sg/ccop-cii.

[1] The CCoP was first issued under the Cybersecurity Act in 2018. It stipulated a set of mandatory cyber-hygiene practices for CII Owners across the 11 CII sectors to implement. This was followed by an addendum to the CCoP in 2019, which introduced a set of mandatory OT Specific cybersecurity practices for OT CII Owners to elevate the nascent cybersecurity state of their OT CII.

Critical Information Infrastructure Supply Chain Programme

- On 27 July 2022, CSA published the Critical Information Infrastructure (CII) Supply Chain Programme paper.

- The CII Supply Chain Programme is a multi-faceted national programme for improving cyber supply chain resilience. It aims to enhance visibility and management of risks, improve cybersecurity education, and create structures for local and international stakeholders to collaborate.

- The programme includes a standardised cyber supply chain risk assessment toolkit, certifications for vendors that meet baseline cyber supply chain requirements, and a learning hub for sharing of cyber supply chain risk management best practices.

Cybersecurity (Composition of Offences) Regulations 2022

- On 8 April 2022, CSA gazetted the Cybersecurity (Composition of Offences) Regulations 2022 under the Cybersecurity Act (CS Act). The CS Act requires and authorises the taking of measures to prevent, manage and respond to cybersecurity threats and incidents as well as to regulate owners of CII and cybersecurity service providers.

- The Regulations 2022 came into force on 11 April 2022, and support the CS Act by identifying the offences that should be prescribed as a compoundable offence under Section 41 of the Cybersecurity Act.

- Composition provides the option of acquitting a criminal charge through payment of fines in lieu of prosecution and conviction. This allows the optimising of CSA, the Attorney-General's Chambers and the courts' resources.

Exercises, Alerts and Advisories

Minister for Communications & Information & Minister-in-Charge of Smart Nation and Cybersecurity, Mrs Josephine Teo interacting with exercise participants.

Exercise Cyber Star 2021

- Exercise Cyber Star 2021 (XCS21) was conducted from November 2021 to January 2022 to practise operational processes and incident management of Singapore's government agencies and CII sectors.

- More than 200 participants across technical, operational and leadership roles participated in XCS21, demonstrating the breadth and depth of the exercise.

- Participants were provided with various scenarios such as ransomware, supply chain and compromise of OT systems. This led to greater awareness of the threats faced and resulted in renewed efforts at improving the sectoral and national cyber response plan.

- XCS21 was an opportunity for CSA to exercise incident management on a national scale for a cyber crisis.

- Minister for Communications and Information & Minister-in-Charge of Smart Nation and Cybersecurity, Mrs Josephine Teo visited XCS21 on 28 January 2022. She was apprised by sectoral senior leadership on their incident management and remediation plans.

Exercise participants being briefed at Security & Emergency's Sectoral Exercise.

Sectoral Cyber Exercises

- Five CII sectors completed their sectoral cyber exercises in 2022. These exercises helped validate their cybersecurity readiness and provide valuable insights for areas of improvements.

- Each sectoral cyber exercise involved about 100 to 300 participants across multiple incident management roles. This enabled the sectors to exercise coordination of holistic crisis responses in a realistic setting.

- The exercises provided senior sectoral leadership with a better appreciation of sector-specific threats, which enabled efforts to improve their sector's cyber incident management and response.

Timely Advisories to CII Sectors

- To strengthen the resilience of CII Sectors, the National Cyber Threat Monitoring Centre (NCTMC) issued 102 advisories to the CII Sectors in 2022 to warn them about relevant cyber threats. This included an alert advisory on potential cyber-attacks arising from the prevalent use of the Pipedream[2] malware toolkit by Advanced Persistent Threat (APT) threat actors to target vulnerable industrial control systems across various sectors globally.

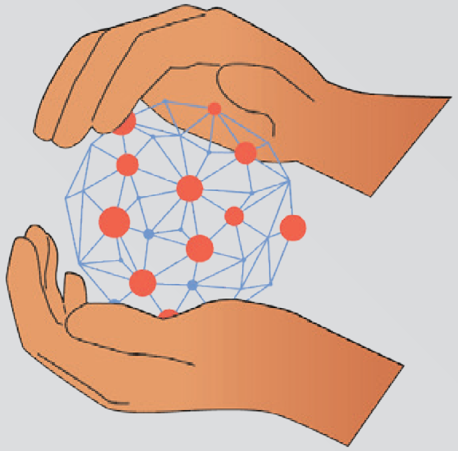
- These timely advisories were issued in response to global threat campaigns and critical vulnerabilities which NCTMC tracks closely.

[2] Pipedream is known to be the most versatile malware toolkit ever made (at the time of discovery) to target a wide range of industrial control system equipment.

Critical Information Infrastructure Supply Chain Programme

Background

The Critical Information Infrastructure (CII) Supply Chain Programme is a national effort, led by CSA, to establish and implement robust processes and sound practices for all CII stakeholders to manage supply chain risks holistically. This approach is encapsulated in our CII Supply Chain Programme paper published in July 2022.



Motivation

Most organisations engage vendors to support their delivery of products and services. Malicious actors may exploit the supply chain ecosystem to infiltrate an organisation to steal data or cause service disruptions. Securing the supply chain can thus be a challenging task as vulnerabilities can be introduced at any point in the supply chain. The increasing complexity of supply chains affects both public and private sectors. It is both a domestic and international challenge. It was with this challenge in mind that CSA developed the CII Supply Chain Programme to uplift the cyber supply chain resilience of Singapore's essential services through five foundational initiatives involving the development of a (i) CII Cyber Supply Chain Assessment Toolkit, (ii) Cyber Contractual Handbook for CIIs, (iii) Vendor Certification Programme, (iv) Cyber Supply Chain Learning Hub, and (v) Platform for International Cooperation.

The Journey

The cyber supply chain issue is multi-faceted and multi-layered, and there are seldom any "perfect" or "easy" answers to this wicked problem. The current context of supply chain management in Singapore is that CII Owners already have some control and measures at the organisational level through regulations. However, regulations alone and individual efforts by our CII owners are insufficient to address the increasingly complex supply chain risks from increased digitalisation and cyber-attacks.

At the local level, interviews and consultation sessions were conducted with Sector Leads, CII Owners and industry experts to understand their supply chain management approach and challenges. We also consulted industry experts and benchmarked international standards to develop the Programme. The subsequent publication of our programme paper catalysed collaboration between like-minded countries and industry groups to collectively address cyber supply chain resilience. The programme paper has also received favourable comments from industry luminaries.

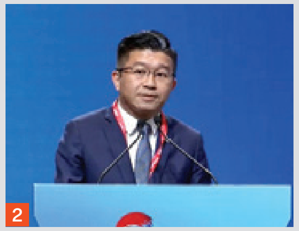
The CII Supply Chain Programme is a voluntary programme designed to aid CII Owners in strengthening their organisational cybersecurity posture. These initiatives will help CII Owners develop a deeper understanding of their supply chain (e.g. identify critical vendors) and support them in managing their supply chain cybersecurity risks (e.g. by establishing cybersecurity requirements on their vendors).

> *"The organisations critical to our daily lives and economies are making great strides to improve their cybersecurity. But as they harden their own defences, they realise that they are connected to a large and complex supply chain of companies. Each of these may represent some risk, because cyber attackers do not give up when they meet hard defences - they look for softer ways in. Understanding this complex and fast-moving supply chain risk, and reducing it, is therefore a key priority for Singapore and for every country."*
>
> Mr Robert Hannigan, Head of International Business, Europe and Middle East, BlueVoyant
>
> *"CI around the world are experiencing increasingly sophisticated attacks by foreign actors who exploit the software supply chain. At the same time, the CI ecosystem has become much more complex; the typical software package now contains components from hundreds of different open source and commercial suppliers. No one company or agency can secure the software supply chain on its own - only a coordinated multi-stakeholder programme can achieve that. This CSA report [CII Supply Chain Programme paper] lays out a framework to successfully create and maintain such a programme. The five initiatives it proposes are exactly what is needed to ensure the long-term security of the infrastructures that are essential to every Singaporean's well-being."*
>
> Mr Eric Byres, Founder and Chief Technical Officer, aDolus Technology Inc, Senior Partner, ICS Secure Ltd

Cyber Supply Chain Conversation at SICW 2022

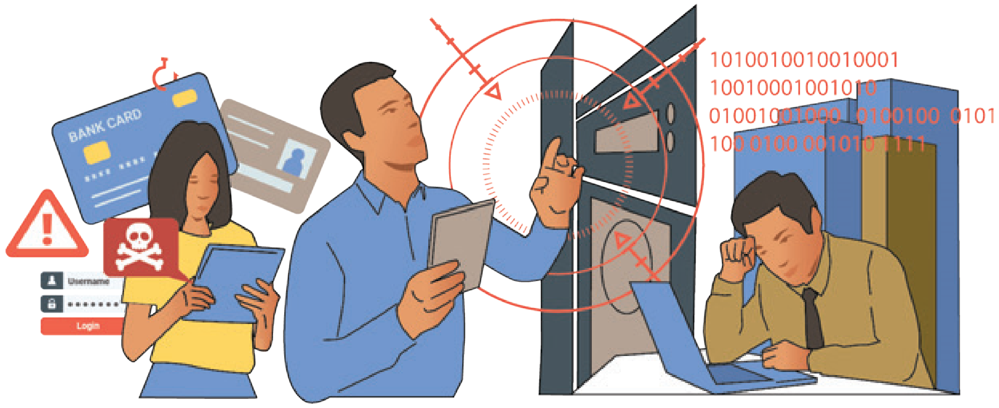
At the international level, the Cyber Supply Chain Conversation convened during the Singapore International Cyber Week (SICW) 2022. It brought together stakeholders to take a whole-of-ecosystem approach on what governments, business owners and vendors can do collectively. The discussions during the session reflected a synergistic effort in leveraging technology to address systemic risks from increased digitalisation and cyber-attacks.

1. Cyber Supply Chain Panel Discussion during SICW 2022.
2. Opening Remarks delivered by Mr Lim Thian Chin, then-Director of Critical Information Infrastructure Division, Cyber Security Agency of Singapore.
3. Keynote speech of Cyber Supply Chain Conversation delivered by Ms Erika Lewis, Director, Cyber Security and Digital Identity at UK Department for Digital, Culture, Media and Sport.



Pillar 2: Enable a Safer Cyberspace

Create a cleaner and healthier digital environment



Raising Awareness of Cybersecurity

SG Cyber Safe Students Programme

In 2022, several initiatives were rolled out with the objective to educate students on the dangers of the cyber world and how they can stay safe online. These include:

'Better Cyber Safe Than Sorry' Music Video

- Launched on 13 July 2022, the music video garnered more than 10,000 views on YouTube, more than 44,000 views on Instagram and 4,000 views on Facebook.
- To complement the launch of the video, a #BetterCyberSafeSG School Dance Challenge was held to encourage students to sing and dance along to the music video. Over 300 students from seven schools participated in the dance challenge.

Better Cyber Safe Than Sorry
strong passwords enable 2FA
Learn to spot signs of phishing
Use anti-virus software
Update y softwa prompt

A scene from the music video.

The Go Safe Online Pop-up

- The Go Safe Online Pop-up, consisting of information panels and a vending machine with a built-in motion-sensor game, was designed to raise awareness on the importance of cybersecurity and educate members of the public, especially students, on the cyber tips to adopt.

- Since its inception in 2019, the Pop-ups have travelled to 80 locations from schools, libraries to community spaces, reaching more than 130,000 students and members of public.

A young library-goer attempting the motion-sensor game.

Peer Support Leaders Programme

- CSA piloted the Experience Cybersecurity Programme for Peer Support Leaders in November 2022 which aims to give a deeper understanding of cybersecurity to student leaders. The Programme consists of a workshop and a Learning Journey to provide the student leaders with cybersecurity knowledge and guide them on ways to be a cybersecurity advocate in their schools.

- The student leaders visited Singtel's Cyber Security Institute to go through a condensed version of "Capture-the-Flag" exercises to learn about cyber defence.

Student Leaders from New Town Primary School attending a workshop.

SG Cyber Safe Seniors Programme

- CSA used a mix of physical and online platforms to engage seniors. This Programme has reached out to over 80,000 seniors since its roll-out in 2021.

  New initiatives include:
  - A series of six 'Youths Help Seniors Go Digital' workshops were organised in partnership with Singapore Press Holdings and Ngee Ann Polytechnic. Student volunteers from the Polytechnic were paired up with seniors to provide them with a one-on-one tutorial, to help seniors learn how to use digital apps safely.

Seniors were paired up with student volunteers for the workshop and one-on-one tutorial.

  - An update of the Better Cyber Safe Than Sorry - A Guide to Staying Safe Online handbook. A partnership with the Singapore Police Force, the handbook was refreshed with current scam trends and tips. More than 50,000 copies of this latest edition have been distributed to partners for use during one-on-one engagements and at community events.

Cyber Safe in the City

- Two 'Cyber Safe in the City' lunchtime pop-up events in the Central Business District (CBD) were organised to:
  (i) raise awareness of CSA's work and cyber tips, and
  (ii) gain insights from Professionals, Managers and Executives (PMEs) via a short survey on cyber tips and cybersecurity policies, and practices at their workplaces.

Better cyber safe than sorry
CYBER SAFE IN THE CITY
Free ice-cream for sharing how you stay cyber safe!

- This was CSA's first physical outreach to PMEs in the CBD and its first collaboration with a Cyber Essentials mark partner, Andersen's of Denmark. Participants could redeem a free ice cream upon completion of the survey.

- CSA reached out to around 1,960 respondents via pop-up events and gleaned insights from the survey on PMEs' attitudes towards cybersecurity. For instance, PMEs were keen on getting more information on how to deal with the latest cyber threats, e.g. ransomware and business email compromise (BEC), steps to secure IoT devices such as Internet routers, smart appliances and smart security systems, and information on credible cybersecurity apps to download.

Lunch crowd in the CBD completing the online survey and redeeming their ice cream.

Levelling Up Organisations and Enterprises

SG Cyber Safe Programme for Organisations

In 2022, CSA launched a series of cybersecurity initiatives under the SG Cyber Safe Programme tailored to organisations in different stages of their cybersecurity journey:

Awareness

For organisations starting out in cybersecurity

Cybersecurity toolkits were developed for different stakeholders in the organisation:

- Cybersecurity toolkits for business leaders and SME owners: Written in business-friendly language, this toolkit helps business leaders and SME owners to understand why cybersecurity is not just a technical issue, but a business risk management issue. It provides information on how business leaders and SME owners can engage their technical personnel to provide cybersecurity leadership in the organisation.
- Cybersecurity toolkits for employees: The human factor is a major contributor to many cybersecurity incidents. As employees are the weakest links in an organisation, this toolkit helps enable employees to be the first line of defence.
- Cybersecurity toolkits for IT personnel in small organisations: IT personnel in small organisations tend to have many competing priorities to address and often lack the resources to support them in implementing cybersecurity. This toolkit helps organisations prioritise the key baseline cyber hygiene measures for implementation, so that they are protected from most common cyber-attacks.
- Since its launch, these toolkits have been downloaded more than 9,000 times.

Action

For organisations ready to implement cybersecurity

- CSA has launched a scheme to develop cybersecurity health plans with funding support for SMEs. The scheme aims to encourage SMEs to improve their cyber defences by going for cyber health "check-ups" and developing cybersecurity health plans, while working towards national cybersecurity certification such as attaining CSA's Cyber Essentials mark.
- CSA worked with IMDA to include pre-approved solutions for cybersecurity under IMDA's SMEs Go Digital programme. Funding support is available through the Productivity Solutions Grant.
- These initiatives have helped more than 860 organisations.

Adoption

For organisations that have implemented cybersecurity and are ready for cybersecurity to be their competitive advantage

- CSA developed cybersecurity certifications in the form of the Cyber Essentials and Cyber Trust marks.
- The Cyber Essentials mark is targeted at smaller or less digitalised organisations such as SMEs and recognises organisations that have implemented good cyber hygiene.
- The Cyber Trust mark is targeted at larger or more digitalised organisations. It helps them communicate their investments in cybersecurity as a competitive edge to help build trust with their customers.
- Cyber Essentials and Cyber Trust marks are also published as Singapore Standards.[3]
- Since its launch, more than 75 organisations have been certified, or are in the process of being certified for Cyber Essentials, and more than 25 organisations are certified, or are in the process of being certified for Cyber Trust, bringing this to a total of more than 100 organisations.

Senior Minister of State for Communications and Information Mr Tan Kiat How announcing the launch of the Cyber Trust and Cyber Essential Marks certification schemes on 29 March 2022.

Senior Minister of State for Communications and Information Mr Tan Kiat How acknowledging the standards community[4] in Singapore for their contribution to developing Cyber Essentials and Cyber Trust Marks certification schemes as Singapore Standards.

[3] Singapore Standards are nationally recognised documents established by consensus. Standards are published documents setting out specifications and procedures for the design, use or performance of materials, products, processes, services, and systems.

[4] The Singapore Standards Council comprises 12 Standards Committees, three Coordinating Committees and a Standards Promotion Committee to lead standards development and implementation in various sectors. Under these Standard Committees are various Technical Committees and Working Groups that oversee, draft, and review standards.

Cybersecurity Labelling Scheme (CLS)

- The Cybersecurity Labelling Scheme for consumer smart devices seeks to improve IoT security, raise overall cyber hygiene levels and better secure Singapore's cyberspace.

- Since its launch in 2020, more than 250 products from leading global brands such as Google, Asus, TP-Link, D-Link, Linksys, Netgear, Nokia, Signify Philips, and Polar have been labelled. Consumers will have wider access to a range of more secure IoT devices from Wi-Fi Routers and Smart Home Hubs, to Smart Lighting and home appliances.

Signing of the MRA with BSI (Germany) at SICW 2022.

- A Mutual Recognition Arrangement (MRA) between Singapore and Germany was signed in October 2022 to recognise the cybersecurity labels issued by CSA and the Federal Office for Information Security of Germany.

- Complementary to the CLS, the CLS-Ready Scheme allows CLS products to leverage security functionalities provided by CLS-Ready certified platforms to meet CLS Level 4 requirements.[5]

Cybersecurity Labelling Scheme for Medical Devices

- CSA launched the Cybersecurity Labelling Scheme for Medical Devices [CLS (MD)] in collaboration with the Ministry of Health, Health Sciences Authority, and Integrated Health Information Systems.

Announcement of CLS (MD) by by Senior Minister of State for Communications and Information Dr Janil Puthucheary at SICW 2022.

- The CLS(MD) was developed in consultation with industry representatives from both the cybersecurity and medical technology communities.

- Under the CLS (MD), medical devices are evaluated according to their levels of cybersecurity provisions. This will motivate manufacturers to adopt a security-by-design approach to develop more secure products for the medical device industry. It will also allow consumers and healthcare providers to make informed decisions about the uses of medical devices.

- The CLS (MD) will apply to medical devices that handle health data or are able to connect to other devices, systems and services.

[5] The CLS has four progressive rating levels with the highest being Level 4.

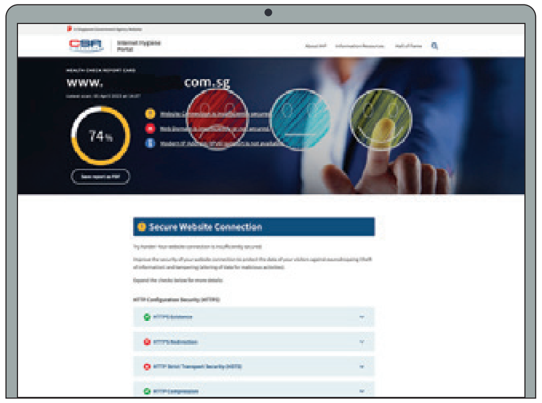
Cybersecurity Labelling Framework – ISO/IEC 27404

- Singapore is working with experts, industry and government partners to develop an international standard, ISO/IEC 27404, a cybersecurity labelling framework for consumer IoT. This framework provides guidance for countries seeking to develop their own labelling schemes and facilitates their mutual recognition among countries.

- The ISO/IEC 27404 project was officially approved through a ballot among International Organisation for Standardisation (ISO) member countries in November 2022 and is now in the Working Draft stage.

Internet Hygiene Portal

- On 19 October 2022, Senior Minister and Coordinating Minister for National Security Mr Teo Chee Hean launched the Internet Hygiene Portal (IHP), a one-stop platform for enterprises. It provides easy access to resources and self-assessment tools for adopting Internet best practices in an organisation's digitalisation journey.



- Since its launch, the IHP has been used to conduct more than 60,000 (12,000 unique) website and email scans, with more than 2,300 scanned domains showing an improvement in their Internet hygiene.

- The IHP also provides visibility on the cyber hygiene of digital platforms by publishing an Internet Hygiene Rating (IHR) table. This helps consumers make informed choices to better safeguard their digital transactions from cyber threats.

- CSA collaborated with the 10 most popular e-commerce platforms to provide better visibility of their Internet security postures through the IHR table. As of end-2022, all 10 have attained 'green' rating on the IHR table.

- Moving forward, CSA will partner with different sectors that leverage the Internet to deliver their services, such as banking and finance, and healthcare, to advocate the importance of maintaining good Internet hygiene.

Asset Based Cyber Defence

- Asset Based Cyber Defence (ABCD) aims to protect SMEs and individuals by solving key security problems, i.e., dealing with malware, data theft, insider threats, and more. It simplifies cybersecurity for end-users as ABCD is offered as a Security-as-a-service model (SecaaS) using Managed Security Service Providers that provide one-stop service including 24/7 managed security monitoring and response.
- Currently, over 500 SMEs have come onboard ABCD SecaaS. Not-for-profit entities such as the Singapore National Co-operative Federation are also using ABCD to attain the Cyber Essentials mark, a cybersecurity certification for organisations embarking on their cybersecurity journey.
- As of May 2022, ABCD has detected and defended against nearly 4,000 cyber threats.

Licensing Framework for Cybersecurity Service Providers

- On 11 April 2022, CSA launched the Licensing Framework and set up the Cybersecurity Services Regulation Office (CSRO) to administer it.
- With the Framework, CSA hopes to better safeguard consumer interests and address the information asymmetry between consumers and cybersecurity service providers. The initiative is also aimed at improving the standards and standing of service providers over time.
- For a start, CSA is licensing two types of cybersecurity service providers: Penetration testing and managed security operations centre monitoring. These services have been prioritised because these service providers can have significant access to their clients' computer systems and sensitive information.
- As of 31 December 2022, CSRO has received around 730 applications and approved close to 400 licenses.

Counter-Ransomware Task Force (CRTF)

- In recognition of the multi-disciplinary nature of the challenge, the CRTF brought together government agencies across relevant domains, capabilities and operational plans to strengthen Singapore's counter-ransomware efforts and put Singapore in a better position to push for international action against the global ransomware threat.
- The CRTF's work delivered three key outcomes:

  Outcome 1
  A consolidated understanding of the ransomware kill chain, upon which government agencies can coordinate and develop counter-ransomware solutions

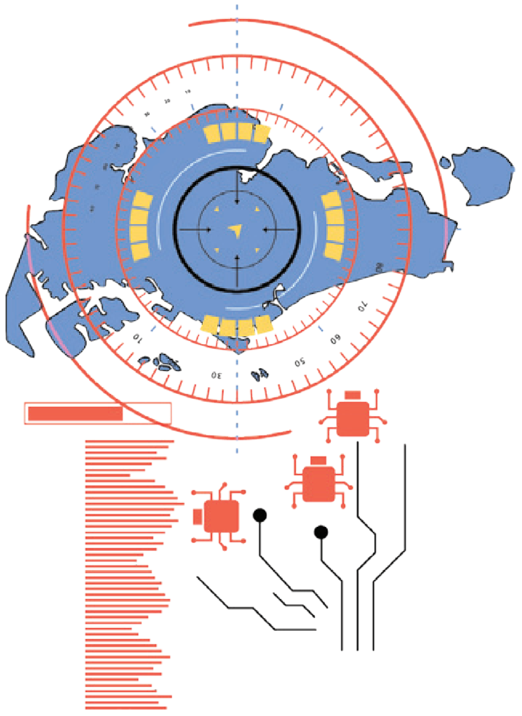
  Outcome 2
  Reviewed Singapore's policy towards making ransom payments to ransomware actors

  Outcome 3
  Recommended strategies under four different pillars for Singapore to counter ransomware effectively:

  - **Pillar 1:** Strengthen defences of high-risk targets such as CII sectors and businesses, to make it harder for attackers to launch successful attacks
  - **Pillar 2:** Disrupt the ransomware business model to reduce the pay-off for ransomware attacks
  - **Pillar 3:** Support recovery so that victims of ransomware attacks do not feel pressured to pay the ransom, which fuels the ransomware industry
  - **Pillar 4:** Work with international partners to ensure a coordinated global approach to countering ransomware

Proactive Threat Watch

- To better protect Singapore's cyberspace, the National Cyber Threat Monitoring Centre (NCTMC) generated threat reports in 2022. These were shared with stakeholders such as CII sectors and members of the public to better help them protect themselves against potential global and local threats.
- NCTMC is proactively involved in raising awareness among CSA's stakeholders. In 2022, it worked with SingCERT and CII sector leads to inform affected companies of over 5,000 leaked credentials and over 50 phishing websites belonging to Singapore enterprises.
- NCTMC continues to seek opportunities to extend its reach to local enterprises to help enhance their cybersecurity posture through information-sharing communities.



Countering Ransomware Together

Background

The Counter-Ransomware Task Force (CRTF) was commissioned to address the growing ransomware threat, which has become an urgent challenge for our companies and potentially national digital infrastructure.

The CRTF convened government agencies across relevant domains, capabilities, and operational plans to strengthen Singapore's counter-ransomware efforts and put Singapore in a better position to push for international action against the global ransomware threat. Agencies contributed manpower, expertise, and capabilities to develop collaborative recommendations to strengthen our cybersecurity posture, thwart ransomware criminal groups, and support victims.

Over the course of the year, the CRTF developed a practical and concrete blueprint to guide the Government and respective agencies' efforts to secure Singapore from ransomware attacks.

Why set up the CRTF?

Prior to the CRTF, ransomware was largely addressed as a matter of sporadic criminal activity in many jurisdictions, including Singapore, and affected small networks and individual computers. While this has historically been sufficient, in the past three years, there has been a step change in ransomware attack trends around the world. Ransomware criminal groups have exhibited capabilities to launch large scale attacks targeting thousands of computer systems, and have started targeting essential services and infrastructure, in hope of eliciting larger ransoms. This means that a ransomware attack has the potential to cause crippling real-world challenges and even pose national security risks, especially as we grow increasingly reliant on digital technologies for our economy and way of life. Given the prevalence of ransomware attacks, Singapore needed to take the ransomware scourge seriously and treat it as a question of when, not if.

Given that ransomware is a cross-border and cross-domain problem, the CRTF is the first-of-its-kind in recognising that governments need to rethink how we organise ourselves to counter ransomware, not only so that we can better secure Singapore, but also take down and thwart the burgeoning ransomware criminal industry together with our international partners.

Achievements of the CRTF in 2022

Over the course of one year, the CRTF managed to achieve WOG alignment on the urgency of the ransomware threat, understanding the threat, what needs to be done collectively to counter ransomware, and how government agencies should respond if critical information infrastructure within their sectors were to suffer a ransomware attack. These efforts culminated in a report that will serve as a blueprint for Singapore's counter-ransomware efforts to better secure ourselves in the longer term. The CRTF's report was also lauded by industry, and several companies across the cybersecurity, tech and financial services sector have already reached out to offer their support and seek collaboration.

As a result of the work done by the CRTF to sharpen national counter-ransomware efforts and marshal cross-domain expertise and resources, Singapore was able to play an instrumental role in shaping and leading the international charge against ransomware. For example, in 2022, Singapore became a pioneering and leading member (together with countries such as the US, UK, Germany) of the CRI, a plurilateral effort compromising 39 countries (and counting) aimed at forging international collaboration to arrest the global ransomware threat. In addition, through the CRTF, government agencies were also able to seize opportunities across various international platforms, such as the Financial Action Task Force and the United Nations Office of Drugs and Crime, to strengthen our collective global effort against the ransomware criminal industry.

Participants at the Counter-Ransomware Initiative Summit at the White House, Washington DC. Mr David Koh, Chief Executive of CSA, represented Singapore.

Pillar 3: Enhance International Cyber Cooperation

Foster an open, secure, stable, accessible, peaceful, and interoperable cyberspace

International Engagements

Cyber Events & Conferences

7th Singapore International Cyber Week (SICW)

- The 7th Singapore International Cyber Week (SICW) was held in-person from 18 to 20 October 2022 after two years of being held online.
- It brought together over 10,000 senior government representatives and non-state stakeholders from 65 countries to discuss key cybersecurity issues.
- Three SICW Ministerial Roundtables were held to discuss the challenges of a transboundary cyberspace, the importance of safeguarding our digital commons, and ensuring open channels of communications to build and enhance trust in cyberspace.
- The SICW Sessions on Confidence-Building Measures and the Future of International Cyber Discussions saw meaningful and constructive conversations that drew from diverse perspectives in a deeply divided world. It brought together perspectives from government, civil society and industry representatives. Underscoring the cross-cutting and dynamic nature of cybersecurity that affects both States and non-State stakeholders, the discussions in both Sessions highlighted the international community's keen interest in constructive dialogue and international cooperation on Confidence Building Measures (CBMs).
- The 7th SICW saw extensive and prominent participation from CSA's international partners, including ministerial officials from ASEAN Member States (AMS), Australia, Czech Republic, Ghana, New Zealand, the UK and the US. It also saw first time attendees from Canada, Germany, Japan, Jordan, the Netherlands, Qatar, Rwanda, UAE/Abu Dhabi and Ukraine, while China sent in-person representation for the first time.

SICW Ministerial Roundtable I on Cyber Resilience in the New Normal.

The 7th ASEAN Ministerial Conference on Cybersecurity (AMCC)

- The 7th ASEAN Ministerial Conference on Cybersecurity (AMCC) discussed how ASEAN and its Dialogue Partners could strengthen cooperation and reaffirm their support for advance capacity-building initiatives.
- Participants expressed continued support for the work undertaken by the OEWG in developing rules, norms and principles of State behaviour in cyberspace.
- Participants underscored the need to expedite the implementation of ASEAN Cybersecurity Cooperation Strategy 2021-2025. They welcomed progress made on the establishment of the ASEAN CERT, a key initiative to building regional cyber resilience and strengthening regional CERT-to-CERT collaboration with other AMS.

The 7th ASEAN Ministerial Conference on Cybersecurity.

17th ASEAN CERT Incident Drill 2022

- Singapore has hosted the annual ASEAN CERT Incident Drill (ACID) since 2006. The aim of ACID is to test incident response procedures and strengthen cybersecurity preparedness and cooperation among CERTs in AMS and Dialogue Partners.
- The theme of the 17th ACID was 'Dealing with Disruptive Cyber-Attacks Arising from Exploitation of Vulnerabilities'. It was chosen in light of the Log4j vulnerabilities discovered in late 2021, which presented the potential for highly disruptive cyber-attacks due to the ubiquitous presence of its service.
- The scenario simulated an emerging triple extortion tactic employed by threat actors to extract a ransom from victim entities.
- The 17th ACID saw participation of 15 CERTs from AMS and Dialogue Partners. Participating CERTs provided feedback that the drill was well-organised and helpful for gaining incident response experience.

Counter-Ransomware Initiative

- Singapore participates in the Counter-Ransomware Initiative (CRI), a plurilateral grouping of 39 countries plus the European Union convened by the US National Security Council to build collective resilience and response capabilities against the growing threat of ransomware. At present, Singapore is the only AMS currently invited to be a member of the CRI.
- In 2022, Singapore and the UK co-led a CRI working group on countering the illicit financing activities of ransomware actors. Chief Executive of CSA Mr David Koh represented Singapore at the 2nd CRI Summit hosted by the White House in Washington D.C. in November 2022. Singapore, along with CRI member nations and the EU, released a joint statement committing to further collective action against ransomware actors, including closer info-sharing among countries to disrupt and bring to justice ransomware perpetrators, and enforcing financial measures to prevent ransomware actors from profiting from illegal proceeds.

The UN Open-ended Working Group meeting.

UN Open-ended Working Group on the Security of and in the use of ICTs (2021 – 2025)

- Singapore participates actively in UN cybersecurity discussions. Singapore has participated at the inaugural UN Open-ended Working Group (UN OEWG) on Developments in the field of ICTs in the context of international security, and the 6th UN Group of Governmental Experts (GGE) on Advancing responsible State behaviour in cyberspace in the context of international security. Both processes concluded successfully in 2021 and their respective consensus reports were adopted by the UN General Assembly. The reports contained specific recommendations on how countries should work together towards an open, secure, stable, accessible and peaceful cyberspace.
- Singapore chairs the ongoing five-year UN OEWG on Security of and in the use of ICTs (2021 – 2025), which builds on the work of the inaugural UN OEWG and the 6th UN GGE. It adopted its first Annual Progress Report by consensus in 2022. This set out a clear roadmap for the next steps that the OEWG will take to foster practical international cooperation on areas such as rules, norms and principles, confidence-building measures and capacity building.

Participation in Renowned Digital and Cyber Conferences

- Minister for Communications and Information & Minister-in-charge of Smart Nation and Cybersecurity Mrs Josephine Teo spoke at the Tallinn Digital Summit (TDS), an annual event hosted by the Estonian Prime Minister held in October 2022. The TDS gathers leaders of like-minded and digitally-advanced countries, international organisations and the private sector to address the issues towards a connected digital future.

Bilateral Cooperation

Participants at the inaugural US-Singapore Cyber Dialogue.

Singapore has been actively involved in various international platforms on cybersecurity, from multilateral discussions on international cyber norms to bilateral cooperation. It is in Singapore's continued interest to work with partners internationally and regionally through dialogue exchanges. Some of the key bilateral exchanges in 2022 include:

- Prime Minister Lee Hsien Loong and US President Joseph Biden announced the establishment of the US-Singapore Cyber Dialogue (USSCD) in March 2022; and the inaugural USSCD co-chaired by CSA's Chief Executive Mr David Koh and US Ambassador at Large for Cyberspace and Digital Policy Mr Nathaniel C. Fick was held on 20 October 2022. The USSCD was well represented by several Singapore and US agencies across government.
- USSCD saw discussions on a wide range of US-Singapore cooperation topics, including developments in multinational and regional cyber fora, protection of critical information infrastructure, countering ransomware, supply chain security, regional capacity building, and combatting digital scams.
- Both sides agreed to establish a Working Group on the Intersection of Technology and Cyber between CSA and the Office of the National Cyber Director.
- Participated in Cyber UK, the UK Government's flagship conference on cybersecurity in May 2022.
- Met US National Cyber Director Mr Chris Inglis in May 2022 in Singapore. Mr Inglis called on Senior Minister and Coordinating Minister for National Security Mr Teo Chee Hean and met Senior Minister of State for Communications and Information Dr Janil Puthucheary during his visit.

1. US National Cyber Director Mr Chris Inglis' call on Senior Minister and Coordinating Minister for National Security Mr Teo Chee Hean.
2. Chief Executive of CSA Mr David Koh speaking at the Aspen Global Cybersecurity Group's inaugural meeting, 9 November 2022.
3. Participants at the Aspen Global Cybersecurity Group inaugural meeting.
4. CSA briefing US National Cyber Director Mr Chris Inglis on 12 May 2022.

- Met with Mr Andres Sutt, Estonia's Minister of Entrepreneurship and IT at the Ministry of Economic Affairs and Communications in June 2022. Mr Sutt was in Singapore to attend Asia Tech x Singapore .
- Signed a Mutual Recognition Arrangement between Singapore and Germany in October 2022 to recognise the cybersecurity labels issued by CSA and the Federal Office for Information Security of Germany.
- Co-chaired the Aspen Global Cybersecurity Group, a closed-door gathering of top cybersecurity leaders from government, the private sector, and civil society in Prague, Czech Republic in November 2022[6].
- Hosted various courtesy calls and bilateral meetings between CSA's Senior Leadership Team with Bulgaria, Czech Republic, Israel, Poland and Romania.

[6] Chief Executive of CSA Mr David Koh co-chairs the Aspen Global Cybersecurity Group in his personal capacity.

1. Participants at the 2nd ASEAN-China Cyber Dialogue.
2. Mr Wang Lei, Coordinator for Cyber Affairs at China's Ministry of Foreign Affairs and Mr Joseph Leong, Permanent Secretary for Communications and Information.

- At SICW 2022, Mr Joseph Leong, Permanent Secretary for Communications and Information held a bilateral meeting with Mr Wang Lei, Coordinator for Cyber Affairs at China's foreign ministry, on cyber and digital cooperation between Singapore and China, including under the ambit of China's Dialogue Partnership with ASEAN. During Mr Wang's visit to Singapore for the SICW, he also spoke at an SICW 2022 Ministerial Roundtable on Building Confidence and Trust in Cyberspace alongside senior representatives from Australia, the Czech Republic, and the United Kingdom, and co-chaired the 2nd ASEAN-China Cyber Dialogue.

Capacity Building Initiatives

Confidence-builders Group at the United Nations (UN) Open-ended Working Group (OEWG) on Security of and in the Use of ICTs 2021-2025

- Singapore is part of the Confidence-builders Group, formed to exchange ideas on advancing CBMs at the OEWG.

- The Group has submitted joint working papers to the UN OEWG discussions, including a seminal paper on the UN global points of contact (POCs) directory.[7]

- This joint working paper, presented at the OEWG inter-sessional meeting in December 2022, sets out concrete proposals on how to establish the global POCs directory at the UN. This includes:
  (i) the role of regional POCs directories vis-à-vis a global POCs directory
  (ii) how the global POCs directory at the UN can be kept up to date
  (iii) the role of the global POCs directory at the UN
  (iv) administrative matters to be addressed in order to set up a global POCs directory at the UN
  (v) the way forward to establishing a global POCs directory.

[7] In the OEWG Annual Progress Report, States agreed to establish a global, inter-governmental points of contact directory.

United Nations-Singapore Cyber Fellowship (UNSCF)

- The UNSCF is a joint initiative with the United Nations Office of Disarmament Affairs (UNODA) as part of the UN-Singapore Cyber Programme.

- The UNSCF seeks to empower senior officials with inter-disciplinary expertise to effectively oversee national cyber and digital security policy, strategy, and operations requirements.

- The inaugural UNSCF was held in August 2022. It saw the participation of 22 Fellows from 18 countries across Asia, Africa, Europe and South America.

UNSCF in session.

Group photo of the UNSCF Fellows.

UN-Singapore Cyber Fellowship

Background

To bridge the gap between the policy and technical officers in cybersecurity, the ASEAN-Singapore Cybersecurity Centre of Excellence had put together a flagship programme, the UN-Singapore Cyber Fellowship (UNSCF) in partnership with the UN Office of Disarmament. The UNSCF falls under the ambit of the UN-Singapore Cyber Programme.

Targeted at Cyber Ambassadors and the heads/deputy of national agencies overseeing cybersecurity, the Fellowship seeks to empower Fellows with inter-disciplinary expertise to effectively oversee national cyber and digital security policy, strategy, and operations requirements. The topics discussed during the Fellowship include best practices in cybersecurity management covering topics such as strategy, legislation, operations capacity development, workforce and ecosystem development, and international policy.

What were the benefits of the Fellowship?

As shared by UNSCF Fellow, CEO of Sri Lanka CERT, Jayasiri Amarasena

a) Experience

My experience in this great event revolves around two main points:

(i) Knowledge, and

(ii) Professional Networking.

The topics presented during the six days covered a broad spectrum of activities related to cybersecurity. These topics covered, in general, technical, and non-technical areas which are essential for the top-level management of any Cyber Regulatory Agency, or a CERT. The topics addressed challenges in cybersecurity due to rapidly changing technologies, legal backgrounds and regulatory frameworks in handling issues related to cyber incidents, and most importantly cybersecurity diplomacy. Each presentation provided me with a new dimension, and broaden my vision on handling our own cybersecurity issues.

Participation at this event allowed me to mix with a great team of multi-cultural professionals from various geographical regions and exchange our ideas and issues related to cybersecurity. Association with the other participants made me realise that while there are many common issues, there are also localised issues which we have experienced due to our regional/cultural backgrounds. I take this as a value addition to the event.

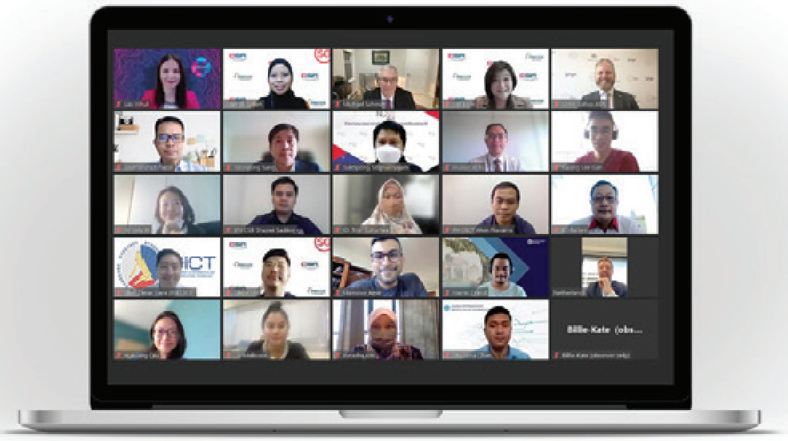
b) Relevance

As I have stated previously this fellowship is relevant to the activities of the organisation I represent. Personally, it has extended my knowledge into areas which I have not paid attention previously. I realised the importance of these areas only after the presentations and the discussions we had during the fellowship.

Being a technical person, I was mainly focused on technology-based solutions. But I now appreciate that there are many non-technical areas which needs to be built into the solution. Areas such as Cyber Stability Framework Confidence Building Measures, Cyber Ecosystem Development, Crisis Communications for Cybersecurity, Digital and Cybersecurity Diplomacy are some of the areas which I will introduce in my own organisation's agenda.

c) What made an impression

One specific area that I came across during the fellowship is Crisis Communication and its practical exercise. This was an eye-opener for me as handling a crisis smoothly requires special skills in "presenting the facts without disturbing" the general public. I felt that this was not about hiding the truth but being cautious and not to cause panic. I felt that we need to focus on possible scenarios and prepare beforehand, especially to handle the media as even the truth disseminated at the wrong time could lead to catastrophic events. I will pay special attention to this area and will prepare the staff at Sri Lanka CERT for such unforeseen events.

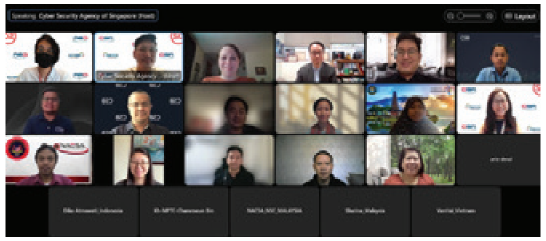


ASEAN-Singapore Cybersecurity Centre of Excellence (ASCCE) Webinar Series

- The ASCCE Webinar Series was launched during the COVID-19 pandemic to maintain momentum in capacity building for AMS.
- Six webinars were conducted in partnership with various ASEAN Dialogue Partners. They covered topics such as cybersecurity strategy, ransomware, threat hunting, cybersecurity awareness, confidence-building measures and effective cyber coordination at the national level.
- ASCCE will continue to offer the webinar series to complement in-person capacity-building programmes for AMS and beyond.

Norms Implementation Checklist Workshop

- The Norms Implementation Checklist Workshop is a joint initiative with UNODA. To date, ASCCE has conducted two workshops:
  (i) a virtual workshop for AMS in March 2022; and
  (ii) an in-person workshop at the UN Headquarters in July 2022 for UN Member States, including members of the Group of Friends on e-Governance and Cybersecurity.
- When developed, the Checklist aims to serve as a simple guide for a set of actions that countries can take towards implementing the 11 voluntary, non-binding norms of responsible State behaviour in the use of information and communication technologies (ICTs) as laid out in the Framework for Responsible State Behaviour in Cyberspace.
- Both Workshops focused on developing a preliminary Checklist for Norms on Protection of Critical Infrastructure, Reporting of ICT Vulnerabilities, and Protection of CERTs.



Participants at the Norms Implementation Checklist Workshop.

Foundational Enabler 1: Develop a Vibrant Cybersecurity Ecosystem

Build a cybersecurity ecosystem underpinned by research and innovation for our security and economic needs

CyberCall

- CSA developed the Cybersecurity Industry Call for Innovation to catalyse the development of innovative cybersecurity solutions for national cybersecurity, strategic, and commercial application. It provides a platform for cybersecurity companies to innovate in partnership with large, trusted end-users in Singapore such as private and public sector owners of critical infrastructure.

- CyberCall benefits both cybersecurity companies and end-users. Cybersecurity companies get an opportunity to innovate for a potential reference customer and access data and implementation testbeds. End-users potentially benefit from innovative solutions to cybersecurity problems.

- Since 2018, CyberCall has supported 22 cybersecurity companies to develop over 30 solutions in areas including cloud security, AI, Internet of Things and OT security, and privacy-enhancing technologies. A total of S$10 million was awarded to all projects in past CyberCalls. Companies were able to raise another S$40 million in external investments to support the next-stage development of these projects, which reflects their significant commercial potential.

- On 31 August 2022, Dr Janil Puthucheary, Senior Minister of State for Communications and Information, and Health, announced the launch of CyberCall 2022 at the Cybersecurity Innovation Day 2022.

OPENING ADDRESS
Dr Janil Puthucheary
Senior Minister of State,
Ministry of Communications and Information & Ministry of Health,
Singapore
CYBERSECURITY INDUSTRY CALL FOR INNOVATION 2022

Senior Minister of State for Communications and Information Dr Janil Puthucheary speaking at Innovation Day 2022.

From University Lab to the Global Stage

Background

The National Cybersecurity R&D (NCR) Programme seeks to develop research and development expertise and capabilities in cybersecurity in Singapore. It aims to improve the trustworthiness of cyber infrastructure with an emphasis on security, reliability, resiliency and usability. It also seeks to promote collaboration among government agencies, academia, research institutes and private sector organisations. As such, NCR is coordinated by various government agencies, including the National Research Foundation, National Security Coordination Secretariat, CSA, MHA, MINDEF, GovTech, IMDA and Economic Development Board.

Featured Enterprise – Scantist

One of the beneficiaries of the NCR Programme is Scantist, a spin-off cybersecurity research laboratory in Nanyang Technology University (NTU) founded by Professor Liu Yang in 2016, which currently employs more than 50 employees.

Seed funding from the NCR Programme helped Professor Liu to expand Scantist to twice its initial size and commercialise their cybersecurity research in the subsequent years. Scantist later won CSA's Call for Innovation Grant in 2020 and an innovation award at Huawei's Spark Programme in 2021.

Scantist is currently an industry collaborator in the National Integrated Centre of Evaluation's (NiCE[8] – a collaboration between CSA and NTU) research into cybersecurity tools to help identify and fix software vulnerabilities.

Since its humble beginnings in a university laboratory, Scantist has grown to be a rising star playing an essential role in ensuring a safer cyberspace in Singapore and placing us on the global cybersecurity stage. In Scantist founder Professor Liu's own words:

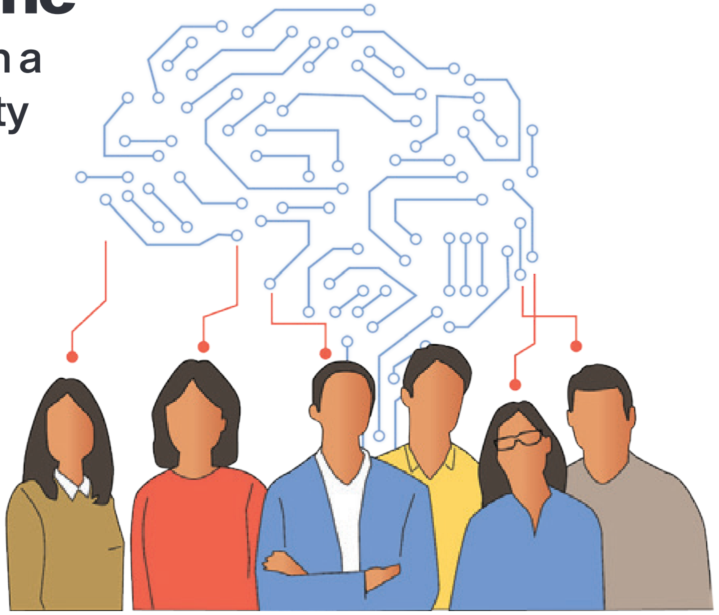
> ***As the founder of Scantist, I am proud to say that our start-up has greatly benefited from the support of CSA. It started via CSA's involvement in the NRF's National Cybersecurity Research Grant Call in 2017, where Scantist successfully secured funding for our proposal. This enabled us to build a strong research team that most start-ups struggle to create and sustain and helped us commercialise our research on security fuzzing and binary analysis. This later formed the foundation for our Software Composition Analysis product that helps organisations identify and fix known vulnerabilities in their software, which is critical in today's digital landscape.***
>
> ***The CSA Innovation Award in 2020 also helped Scantist to expand our product lines and further develop our capabilities. This award not only provided financial support, but also accorded additional credibility to Scantist, thereby helping attract potential investors and customers like Continental, IMDA, and Huawei. In the two years after receiving the award, Scantist has nearly doubled in size and closed our largest round of funding to date.***
>
> ***In short, CSA's support has enabled Scantist to research and develop innovative products, establish a strong foothold in the industry, and attract investment for further growth and expansion.***

Scantist's Founder, Professor Liu Yang

[8] NiCE pools industrial and research expertise together to develop a sustainable academia-industry-government ecosystem for production evaluation and certification in Singapore (www.ntu.edu.sg/nice).

Foundational Enabler 2: Grow a Robust Cyber Talent Pipeline

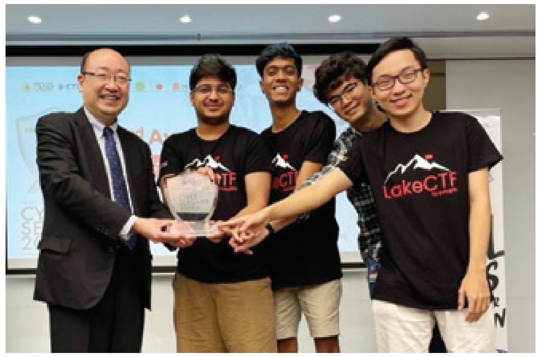
Develop and sustain a strong cybersecurity workforce to meet our security and economic needs



SG Cyber Olympians

- The SG Cyber Olympians programme trains passionate Singaporean youths with exceptional cybersecurity talent to represent Singapore in international competitions (e.g. DEFCON, Cyber SEA Games) and build a strong pipeline of future tech leaders.
- In 2022, CSA identified 47 youths to enter the SG Cyber Olympians Programme and selected seven top performers to represent Singapore in international competitions. Four participants represented Singapore at the annual Cyber SEA Games 2022 held in Bangkok, Thailand from 10 to 11 November 2022. The participants came in second out of 10 ASEAN teams.

SG Cyber Olympians undergoing thematic and CTF training at a monthly Sparring Session.



The Singapore team, comprising (from left) Akash, Ravin, Ron and Zeyu, receiving the second place award in the Cyber SEA Games 2022.

CSLP Participants with Minister for Communications and Information & Minister-in-Charge of Smart Nation and Cybersecurity, Mrs Josephine Teo and Chief Executive of CSA, Mr David Koh.

Cybersecurity Strategic Leadership Programme

- Strong cyber leaders are important for leading and grooming the next generation of cyber talent. A strong local cybersecurity leadership core is also important to supporting Singapore's ambition as an Asia-Pacific cybersecurity hub.
- CSA partnered with Singapore Management University (SMU) to develop the Cybersecurity Strategic Leadership Programme (CSLP). The CSLP is an executive MBA-type training programme specially catered to senior cyber leaders and aimed at strengthening their knowledge, leadership and networks. It helps them achieve a deep understanding of key global drivers shaping cybersecurity strategies, develop a culture of innovation, and lead cybersecurity functions in their organisations effectively.

Minister for Communications and Information & Minister-in-Charge of Smart Nation and Cybersecurity, Mrs Josephine Teo delivering a speech at the Graduation Ceremony held at SMU.

- Twenty-one local senior cybersecurity leaders from private and public organisations in the CII sectors, including Energy, Finance, Government, Healthcare, and from cybersecurity companies, participated in the inaugural CSLP, which ran from September 2022 to January 2023.

The Smart Nation Scholarship in 2022

- Developing deep digital tech capabilities in the Public Service is a critical part of Singapore's development as a Smart Nation. The Smart Nation Scholarship, jointly offered by CSA, GovTech and the Infocomm Media Development Authority (IMDA), has provided young Singaporeans with a career in technology since 2018. Recipients of the scholarship contribute towards the public good, specialising in any of seven key tech domains: 1) Application Design, Development & Deployment, 2) Cybersecurity, 3) Data Science & AI, 4) Geospatial, 5) ICT Infrastructure, 6) Sensors & Internet of Things, and 7) Tech Policy & Governance.
- The three agencies have been actively involved in outreach efforts to promote Smart Nation Scholarship since its inception. In 2022, CSA, IMDA and GovTech reached out to numerous schools and education institutes, engaging with hundreds of students over numerous virtual and physical events. Subsequently, a total of 17 Smart Nation scholarships were awarded; these recipients can look forward to a multifaceted career, specialising in a range of tech domains across different public agencies.

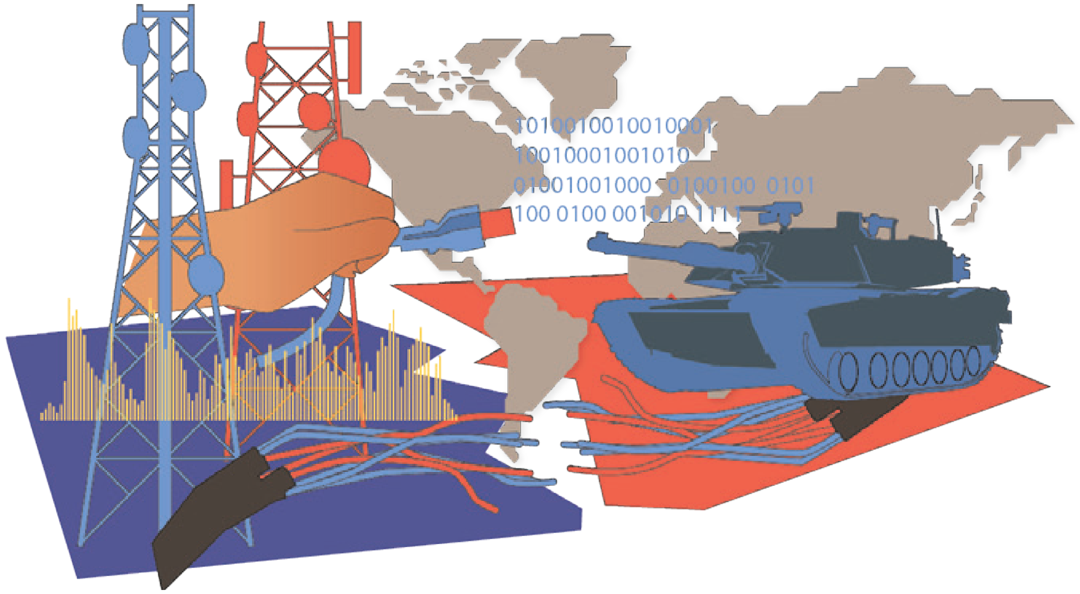
Exercise Cyber Knights 2021

- Exercise Cyber Knights 2021 (XCK21) was conducted from November 2021 to January 2022 as part of efforts to sharpen the skills of Singapore's cyber responders.
- More than 80 participants across various incident response roles participated in XCK21, honing their skills in incident response.
- Sophisticated attack scenarios were delivered through a cyber range. Participants were able to benchmark their performance against the advanced threats made by a persistent attacker.

Participants at Exercise Cyber Knights 2021.

- XCK21 allowed CSA to better appreciate the crucial roles that various incident responders play and refine incident response operations.

What Singapore Government Partners are Doing for a Safer Cyberspace



Ensuring a Safer and More Secure Digital Future

Contribution by
Security and Resilience Division (SRD), Ministry of Communications and Information (MCI)

The digital future offers unprecedented opportunities for Singapore's economy and society. In the digital world, we can overcome our traditional geographical constraints, scale our market size, and grow economic activity exponentially. An ever-growing plethora of digital platforms and services also provide us new ways to strengthen our community bonds, enhance public-private collaborations, and enrich our way of life.

At the same time, there is a dark side to this digital realm, with risks we must address. These risks can undermine the security and resiliency of our digital ecosystem or the safety of our digital citizens and companies. They will only continue to grow as individuals and companies transact and engage digitally.

An Evolving Digital Threat Landscape

Unlike physical domains like air, sea, and land, the digital domain is borderless. This means that the security and resiliency of our digital ecosystem can be undermined by a variety of risks that can come from anywhere.

APTs, ransomware, data breaches, denial of service, and other cyber-attacks have become commonplace. These are increasing in scale and sophistication, and according to analysis by the US Government Accountability Office (GAO), losses due to major attacks rose from US$470 million in 2016 to US$2.6 billion in 2021. This attack surface will increase with the proliferation of personal and IoT devices

2022 Cyber-attacks on Costa Rica

On 17 April 2022, around 30 government agencies in Costa Rica were hit by a large-scale ransomware attack. This included the Ministry of Finance, the national Internet Service Provider (ISP) RACSA, the Costa Rican Social Security Fund, and the Administrative Board of the Municipal Electricity Service of Cartago. The security of sensitive information (e.g. tax returns) and availability of key government services (e.g. systems to manage trade imports and exports) were disrupted, cutting off key streams of Costa Rica's national revenue and causing losses of up to US$30 million per day.

The cybercriminal group Conti claimed responsibility for the attacks and demanded a ransom of US$10 million to restore digital services. The Costa Rican government rejected their demands and sought assistance from other countries such as the United States, Israel, and Spain, and companies like Microsoft to repair the damage to its ecosystem.

across all aspects of our lives including Smart Wi-Fi routers, virtual assistant devices, and autonomous vehicles. It is estimated that by 2025 there will be more than 55 billion of these interconnected devices.

Threats to cybersecurity will continue evolving as new technology is introduced to the market. For example, quantum computing is projected to be able to break the encryption we use to protect digital communications today. This threatens the confidentiality and integrity of our communications and potentially allows malicious actors access to sensitive information. Singapore must keep abreast of these emerging technologies and address the risks early.

Cybersecurity vulnerabilities aside, there are other risks to the complex network of digital infrastructure that supports our digital activities. This infrastructure can be affected by a variety of events ranging from power outages and environmental disasters to geopolitical conflicts. For example, submarine cables carrying critical Internet traffic can be severely damaged, stopping users from transacting and interacting online. Just last year, Tonga was disconnected from the Internet for more than a month when an earthquake cut its only telecoms cable.

More recently, a simple power surge resulted in a disruption of data centres that support Microsoft Azure's cloud services in Southeast Asia. Numerous business operations and digital services were affected by the outage. It is worth reviewing our approach to the security and resilience of such digital infrastructure and services, especially given their increasing ubiquity across all aspects of our digital lives.

We have also seen how access to digital technologies and infrastructure can be used as a lever of influence or form of protest. For example, tech companies pulled out of Russia within weeks of the Russia-Ukraine conflict, leaving Russian citizens without access to a vast range of digital services and platforms. Notwithstanding the geopolitical context of the above example, what is clear is that tech companies have an outsized influence and control over our digital lives. It would be wise not to take the digital connectivity and access to digital services and platforms we enjoy today for granted.

The security and resiliency of our digital infrastructure will also be impacted by the growing tech contestation between countries. Economic competition and geopolitical conflict will likely affect how global supply chains are structured, the availability of technological components (e.g. chips), infrastructure costs, and what services we can operate in our digital ecosystem. This will impact whether our digital economy continues to have the assets such as technology, capabilities, and services needed for growth.

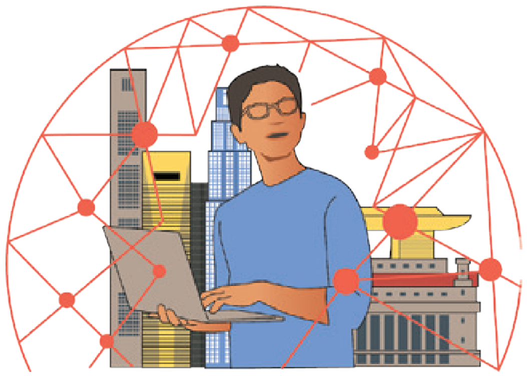
With increasing digitalisation of all aspects of our lives, users will also have to deal with a range of online harms. Malicious actors will leverage technology to conduct scams, distribute harmful content, and proliferate other online harms at speed and scale from anywhere in the world. In the last two years, we have seen sophisticated cybercriminal groups offering Scams-as-a-Service, which enables more scammers to mount campaigns at low cost. Emerging technology (e.g. generative AI) is also being exploited, such as to create convincing phishing emails and deepfakes (e.g. images, videos). We can expect that the information landscape will become increasingly distorted with misinformation and disinformation, making it difficult for us to discern what is and is not real. All these risks can destabilise our collective trust and confidence in our digital future, as well as our sense of safety and security in the digital world.

MongoDB's Decision to Terminate Services in Russia and Belarus

In 2022, following the roll-out of trade sanctions against Russia by the US and other western countries, MongoDB made a unilateral decision to stop provision of all software and services in Russia and Belarus. This applied to all customers, including private businesses and civilians who were not responsible for Russia's actions in the ongoing conflict. This reportedly caused significant disruption to business operations and economic activities until affected customers could switch digital infrastructure.

Exploiting ChatGPT as Harmful AI

Checkpoint Research reported in January 2023 that malicious actors with minimal developer experience were learning to use OpenAI and ChatGPT to develop cyber-malicious programmes despite OpenAI's claims that ChatGPT had safeguards in place. ChatGPT was able to generate simple data-stealing programmes that copy sensitive data to a remote location or full encryption programmes necessary for ransomware attacks. ChatGPT was also able to create the software infrastructure for a dark web marketplace, enabling other modes of cyber-crime. These trends indicate that AI is an attractive target for abuse by malicious actors for its ability to boost "productivity" for scam and cyber-attack operations.



An Ecosystem Approach

An ecosystem approach is required to effectively deal with the above-mentioned digital risks, anchored by three objectives:

- Safety of our companies and citizens online
- Security of our digital ecosystem to guard our nation against malicious actors
- Resilience of our digital ecosystem against potential disruption and damage to our digital ways of life

The government, industry, and public all have a role to play in this.

Government

The government must sharpen regulatory incentives for the private sector to prioritise safety, security, and resilience, to ensure that citizens and businesses are well-protected. Rules and regulations must be updated to ensure that they remain fit-for-purpose amidst the changing landscape of technology and digital services. This will ensure that we maintain a sustainable balance between economic growth, digital innovation, and security. For example, the government can establish default "baseline requirements", which set out the critical security measures that must be built into new infrastructure and services.

However, the government cannot do this alone. Beyond regulation, we need to explore new models of collaboration with trusted, like-minded partners in the private sector. We should leverage their expertise and capabilities to develop solutions efficiently and to customise safety or security programmes to our local context. Collectively, we can ensure that Singapore remains at the forefront of technology, navigate new industry developments, and identify potential risks early. This will be useful to cope with emerging risks stemming from generative AI, quantum computing, and other technologies on the horizon.

Governments must also work together. Many digital security issues are cross-border in nature and require good cooperation between countries and organisations on mutual areas of interest. Collaborating with like-minded partners will help further our common interests, harmonise common standards for security and safety, and build consensus on international rules and norms. For example, countries could work together to establish a common understanding on the security, safety and resilience requirements we expect from technology.

Industry

The private sector continues to design, own, and operate a majority of the digital ecosystem, especially consumer-facing products and services like social media, e-commerce marketplaces, and content platforms. Therefore, industry must take a fair share of responsibility for safety, security, and resilience. This could include upstream measures to moderate content and ban false advertising to protect users from misinformation and scams. It could also include proactive enhancements to the cybersecurity of the company's infrastructure to protect user data against theft and loss. Industry must transform its approach to development to ensure that technology is made more secure-by-design. Companies may need to balance their business interests and profit with upstream investments in features that will ensure consumer safety and security of the digital ecosystem. This will ensure that the digital economy and the broader digital domain can continue to grow sustainably.

The public

Development of digital technologies and services are primarily driven by consumer demand. Therefore, individuals can do their part to choose products and services that are safe and secure, and do not pose a large risk to our digital ecosystem. For example, individuals can choose to shop with e-commerce platforms that comply with Transaction Safety Rating (TSR) standards as published by MHA. One can also make informed choices about IoT devices like Smart wi-fi routers using the CLS to identify products with better cybersecurity provisions.

Users must also keep vigilant and adopt skills needed to protect themselves and their community against digital threats. It is critical to reinforce this layer of defence, which can significantly help to mitigate risks. For example, individuals can play a more active role in identifying and reporting scams efficiently, contributing to our overall detection capabilities. Corporate consumers can also adopt cyber-safe measures to guard their enterprise ecosystem against attempted cyber-attacks and prevent data loss.

Safety, Security, and Resilience

Building a safe, secure, and resilient Digital Singapore requires deep collaboration and co-operation across the entire ecosystem of government, industry, and the public, with the support of international partners. Each will have a role to play in managing these risks to safeguard trust and confidence in our digital future.

Building a Safer Cyberspace with the Community

Contribution by **Government Technology Agency (GovTech)**

Visit any government website or application and you may notice a 'report vulnerability' button.[9] Behind this simple feature lies a team of in-house security researchers and cybersecurity specialists who work with members of the public to identify, validate, and remediate vulnerabilities on Internet-facing government systems. This is part of GovTech's Vulnerability Disclosure Programme (VDP) that allows anyone to report security flaws in an organisation's Internet-facing systems.

The VDP is one of three initiatives under GovTech's Crowdsourced Vulnerability Discovery Programmes (CVDP). The other two — the Government Bug Bounty Programme (GBBP) and Vulnerability Rewards Programme (VRP) — involve close engagement with security researchers registered under HackerOne. Together, the CVDP fosters an active community of researchers and members of the public working with GovTech's Cyber Security Group (CSG) to build a safer cyberspace for all.

Importance of engaging the public to report vulnerabilities

Today, 99% of citizen transactions for government services are conducted digitally from end to end. For instance, Singpass allows more than 5 million Singapore residents to transact with more than 2,700 services from 800 organisations.[10] LifeSG, which integrates and bundles related services across government agencies, enables users to access more than 400 services for key life stages.[11]

The accessibility of these digital services, however, can be a double-edged sword as it provides many touchpoints for malicious actors to launch cyber-attacks. All agencies have security teams to monitor threats and vulnerabilities, but as the saying goes, "There is safety in numbers". This is why the government also taps the 3.5 million users of government online services to identify and report vulnerabilities as part of VDP.

Validating vulnerability reports

In a typical reporting process, a GovTech triage team from CSG will validate a submitted vulnerability report. This team also checks if there are similar vulnerabilities in other government systems and applications.

The discovery of valid vulnerabilities has prevented many potential cyber incidents. In 2021, a researcher found a vulnerability in a website's authentication module, where a malicious actor could redirect users to phishing websites by exploiting the authentication process. After the GovTech team received the researcher's report, they discovered similar vulnerabilities across a few other agencies' websites through proactive bug hunting. The vulnerability was patched and redirects can now only be made to whitelisted websites.

[9] Read out more about GovTech's Vulnerability Disclosure Programme here https://www.tech.gov.sg/report_vulnerability.
[10] Statistics derived from Singpass, https://www.singpass.gov.sg/main/
[11] Statistics derived from LifeSG, https://www.life.gov.sg/app

Local white hat community with GovTech CSG Jaga, the STACK competition winners, and Senior Minister of State for Communications and Information Dr Janil Puthucheary at the appreciation event in 2022.

The close collaboration between security researchers and the triage teams effectively created a multiplier effect, illustrating that vulnerabilities in other government systems can be identified and remediated by a single community report's finding.

Fostering an active community

Since the launch of CVDP in 2018, over 2,000 members of the public and cybersecurity researchers have identified and promptly remediated more than 1,000 valid vulnerabilities in government systems.[12]

To recognise the efforts of security researchers, GovTech presents various awards to the researcher community. Invited researchers for the GBBP and VRP are eligible for cash bounties that correspond to the severity of the vulnerability rewarded. Members of the public who submit a valid vulnerability under the VDP will also receive a digital badge that can be shared on their social media[13].

Top local security researchers for CVDP were awarded an exclusive Jaga Golden Trophy.

Top security researchers are recognised in an annual appreciation event, which also provides an opportunity for them to network and exchange learnings. Beyond awards, VDP researchers found the programme useful for sharpening their skills. Benjamin Lee, 2022's top VDP researcher, shared that the VDP "helped (him) hone (his) skills in web-penetration testing, as well as gain recognition in (his) workplace through (his) VDP achievements".

Securing our cyberspace together

As cybersecurity threats become more complex, an all-hands-on-deck partnership approach between GovTech's CSG, the research community, and the public help to identify vulnerabilities and share knowledge. This close partnership will continue to enhance the security of our shared cyberspace.

[12] As of February 2023.

[13] Example of digital badges can be found on the Hackerone website https://hackerone.com/govtech-vdp?type=team

Safeguarding Our Everyday Lives – CIDeX and Our National Cyber Defence

Contribution by **Digital and Intelligence Service (DIS), Ministry of Defence (MINDEF)**

CIDeX 2022 at the National University of Singapore.

The inaugural Critical Infrastructure Defence Exercise (CIDeX) was held over two days in November 2022 with the aim of training CII operators as part of national efforts to secure our national cyberspace. CIDeX 2022 was organised by the Digital and Intelligence Service (DIS), the fourth and a new service of the SAF in partnership with CSA. It involved key Singapore CII sector leads and agencies from the Water, Power, Telecommunications, and Transport sectors. It also featured participants from 16 organisations including SingTel, SMRT, Sembcorp, and ST Engineering alongside cyber-defenders from the DIS. This was the largest cyber defence drill of its kind in Singapore and the first such cyber exercise held by the DIS since its inauguration in October 2022.

CIDeX 2022 featured a realistic exercise scenario enabled by collaboration with the National University of Singapore's (NUS) National Cybersecurity R&D Laboratories (NCL) and Singapore University of Technology and Design's (SUTD) iTrust Centre for Research in Cyber Security. The exercise simulated a large-scale "nation under attack" scenario that allowed cyber defenders from CII agencies to defend the simulated network together at the same time. During the exercise, participants were split into various groups to identify attacks in real-time and recommend mitigating strategies. The exercise took place in cyberspace with not only IT infrastructure but also OT physical testbeds (e.g. structures fitted with real pipes, generators, and solar panels equipped with more than 100 sensors) that simulated actual water and power plants.

CSA & DIS Senior Leadership with Lieutenant-General Melvyn Ong, then-Chief of Defence Force.

CIDeX 2022 helped strengthen Singapore's collective ability to protect its CIIs by allowing cyber defenders from different entities to train together. Best practices and ideas gleaned from CIDeX 2022 were distilled and brought back to their respective home organisations to be implemented. This not only improved our cyber defenders' skills and knowledge, but helped foster a sense of collaboration and teamwork among the organisations for greater interoperability in times of crises.

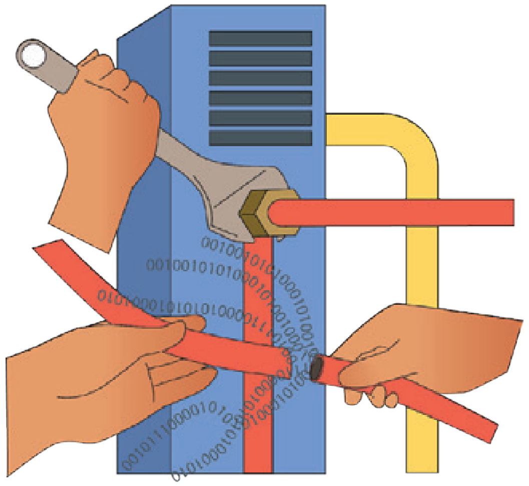
In the digital domain, we are only as strong as our weakest link. Malicious cyber actors are acutely aware of this. Hence, every organisation and agency has a role to play in our national cyber defence. As CSA Chief Executive Mr David Koh stated, "Cybersecurity is a team sport." It is on this basis that CIDeX was organised. The SAF's Defence Cyber Chief BG Edward Chen said platforms like CIDeX allow cyber defenders from national agencies to train together, strengthening Singapore's ability to protect its critical information systems.

CSA's then-Deputy Chief Executive (Development) Mr Gaurav Keerthi said, "CSA has a longstanding partnership with MINDEF/SAF on national cyber defence. Exercises such as CIDeX ensure our collective preparedness for cyber incidents and emergencies..." The SAF will continue to lean forward in partnership with CSA and train Singapore's CIIs as part of national efforts to secure Singapore's national cyberspace against malicious cyber actors. Plans to build on and expand CIDeX are in the pipeline, with more advanced and challenging training scenarios in store for participants in subsequent iterations. Stay tuned for CIDeX 2023!

CSA-DIS Joint Operations Agreement signing ceremony on the sidelines of CIDeX 2022.

Minimise Data Breach Risks with Security

Contribution by Personal Data Protection Commission (PDPC)



The COVID-19 pandemic brought about rapid acceleration of digitalisation, and with it, increasing data protection and privacy concerns. Today, more than 120 countries have engaged in some form of data protection regulations to protect their citizens and data.

The Personal Data Protection Act (PDPA) was introduced in 2012 as the first step towards ensuring that Singaporeans' data is offered the rigorous protection and controls it deserves. The law was enhanced in 2020, taking into consideration the fast-changing digital environment where organisations make use of their customers' data for business improvements and innovation whilst ensuring the personal data is kept secure.

Data breaches will happen

Data beaches can lead to financial losses and loss of consumer trust in the organisation. Individuals whose personal data have been compromised can be exposed to significant harm if they do not take steps to protect themselves. It is important for organisations to be accountable to individuals by prevention through security solutions and data breach management when the worst happens.

Under the PDPA, this is reflected in the Data Breach Notification that was recently mandated as an obligation. It requires that organisations notify the Personal Data Protection Commission (PDPC) and their customers if a data breach of significant scale has occurred or if the incident is likely to cause significant harm to the affected individuals.

In 2022, the PDPC investigated over 60 of such data breaches and categorised over 60 percent of them as cyber incidents. The bulk of these was related to ransomware or phishing attacks, where the threat actor would gain access to the organisation's system and/or its database. This sends a strong signal that in this digital economy, data breaches are no longer an "if" but "when". Organisations must have ready drawer plans to recover quickly from data breaches.

Securing data means securing business

One such cyber incident involved an electronics retailer plagued by ransomware, which targeted its database containing customers' personal data. Customer details such as names, addresses, and email addresses, were compromised. The threat actor(s) managed to exploit vulnerabilities in the organisation's system to retrieve data in its customer database via Structured Query Language (SQL)[14] injection. This is one of the most common web hacking techniques that uses malicious code to attack data-driven applications. Fortunately, the retailer was able to take swift measures to disable the use of the affected system and subsequently add security measures against such SQL injections. Because the retailer had regularly backed up its data, it was able to restore all affected personal data with minimal disruption to its operations.

[14] SQL is a type of computer language used to communicate with a data base.

The retailer learned an important lesson: Cybersecurity is integral to business continuity. Apart from conducting periodic security reviews on its systems, the retailer is committed to conducting vulnerability testing to discover potential vulnerabilities in its servers/systems and prevent similar attacks. It has learned to exercise due diligence when managing vendors and stipulate personal data protection requirements to IT vendors, making clear the job specifications.

Birth of data protection essentials

Cyber incidents like this got the PDPC team thinking: As the collection and use of data by organisations grow, it seems inevitable that most organisations will eventually experience a data breach. With the acceleration of digitalisation and small businesses rushing to join the bandwagon, are they equipped with sufficient security to protect the customers' data they hold?

Apart from providing guidance through resources such as Data Protection Practices for IT Systems, the team consulted the industry and found that smaller organisations were struggling with the foundation of data protection and cyber security as they digitalised. Since SMEs make up the bulk of Singapore's businesses, the team felt it was imperative to provide a one-stop professional service for them to build up basic data protection and security capabilities.

Hand-in-hand with IMDA, PDPC developed a programme that appoints relevant service providers to help small businesses put in place basic data protection and security measures to protect their customers' data and support business continuity. This came to be known as Data Protection Essentials (DPE). As SMEs mature in digitalisation and increase collection and use of personal data, implementation of the DPE will be the cornerstone for attaining the higher standard Data Protection Trustmark (DPTM) certification.

Inculcating a data protection culture through DPE

One of the first organisations to implement DPE was Georges Group, which started as a small sea sports centre with a beverage kiosk. It gradually evolved into a beach bar serving western cuisine, good music and great hospitality. Today, the Georges Group has six outlets across the island and offers a loyalty rewards programme that provides food and beverage deals.

The organisation handles a diverse amount of data belonging to both employees and customers. Its management deemed it paramount to have all its data handled appropriately and to meet its corporate obligations under the PDPA.

"One of our top priorities is the safety of our customers' personal information," shared Georges Group's Data Protection Officer, Ms Grace Sia. "We decided to implement DPE to assure our customers that their data will be used for the purpose it was collected for and managed safely on our membership platform. With DPE, we can offer customers peace of mind about how their data is managed by Georges."

The DPE's one-stop professional service provided Georges Group with a setup service that included basic data security and accountability practices, incident management, communications and training, a six-month review, and a retainer service. Apart from ensuring its data is secure, this initiative has helped Georges Group build good internal culture to develop strong and applicable data protection and security policies that can be followed by all employees.

Ms Sia added: "The DPE training also educates our employees to properly handle the data obtained from our customers. Everyone plays a part in data protection and you are only as strong as your weakest link. The responsibility of business owners is to ensure that consumer information is processed safely in this digital age."

The Fight Against Scams – The Singapore Approach

Contribution by **Anti-Scam Command (ASCom), Singapore Police Force (SPF)**

31,728 **+33%**

scam cases in 2022

33,669 **+25%**

cybercrime cases in 2022

Based on SPF's Annual Scams and Cybercrime Brief 2022

Scams are increasing at a blistering pace, with no sign of abating. They are now pervasive not only in Singapore but worldwide. Since 2017, Singapore has faced an upward trend, with more money lost every year. Scam cases contributed to more than half of Singapore's overall crime, increasing from 23,933 cases in 2021 to 31,728 in 2022, where at least S$660.7 million was reported to have been lost to scams.

The Singapore Police Force (SPF)'s Anti-Scam Command (ASCom) was operationalised on 22 March 2022 to achieve greater synergy between the various scam-fighting units within the SPF. It integrates incident response, intervention, sense-making capabilities, enforcement, and scam investigations under a single umbrella. The command comprises the Anti-Scam Centre and three Anti-Scam Investigation Branches. It also oversees the Scam Strike Teams situated within each of the seven Police Land Divisions. The opening of the ASCom office was officiated by Mrs Josephine Teo, Minister for Communications and Information and Minister-in-Charge of Smart Nation and Cybersecurity, on 6 September 2022.

To fight scams, ASCom employs the concept of S.C.A.M.S:

S	Strengthened sense-making and leveraging technology
C	Close collaboration and enhanced partnerships
A	Agile response in advancing international co-operation
M	Maximise effective management of scam cases
S	Swift and strategic actions

Strengthened sense-making and leveraging technology

ASCom focuses on upstream interventions to disrupt scammers' operations and leverages technology to strengthen its sense-making capabilities. In this way, it can detect and alert potential scam victims even before they discover that they have been scammed. ASCom proactively screens police reports for

The opening of the ASCom office was officiated by Minister for Communications and Information & Second Minister for Home Affairs Mrs Josephine Teo and Minister of State for Ministry of Home Affairs & Ministry of Social and Family Development Miss Sun Xueling.

online monikers, URLs, and advertisements linked to scammers' activities. It works with online marketplaces to take down suspicious online advertisements and monikers, and with telecommunications companies to terminate scam-tainted phone numbers and WhatsApp lines. ASCom continues to work with banks and fintech companies to develop Anti-Fraud Financial Systems and leverage the use of AI to identify and block suspicious financial transactions. In 2022, through sense-making, ASCom detected and sent advisories to more than 11,100 potential victims.

Close collaboration and enhanced partnerships

ASCom partners more than 80 institutions in the fight against scams. These include local and foreign banks, card security groups, non-bank financial institutions (e.g. Grab and Singtel DASH), fintech companies and cryptocurrency houses (e.g. Wise, Xfers Pte Ltd and Coinhako), and remittance service providers in Singapore. Through establishing direct communication channels and close working relationships, ASCom and its partners seek to swiftly freeze accounts, recover funds and reduce losses suffered by victims.

In May 2022, strong public-private partnership involving ASCom and DBS Bank led to the recovery of US$11.5 million, the largest amount recovered from a single scam arrangement to date. Four overseas victims fell prey to Business Email Compromise (BEC) scams and were deceived by spoofing emails purportedly from the victims' business clients into making large transactions amounting to more than US$15.5 million to bank accounts held with DBS. Upon receipt of the report, ASCom immediately worked with DBS to conduct fund flow tracing, which led to the swift recovery of scam-tainted funds.

As part of the continued collaboration in combating scams, ASCom and MAS worked with banks to co-locate their staff within ASCom premises. There are currently six banks – namely DBS, OCBC, UOB, SCB, HSBC and CIMB – which have come onboard to enhance real-time coordination with the Police in investigative efforts, tracing the flow of funds and freezing bank accounts suspected to be involved in scammers' operations. Since the co-location, proactive fund flow tracing has led to an improved seizure rate. In 2022, ASCom froze more than 16,700 bank accounts based on reports referred to its Anti-Scam Centre. About 27 percent of the amount lost by victims, amounting to about S$146.6 million, was recovered by ASCom.

Agile response in advancing international cooperation

On the international front, the SPF works closely with foreign law enforcement agencies such as the Royal Malaysia Police and Interpol to exchange information and conduct joint investigations and operations against transnational scams. Through this close collaboration, the SPF and overseas law enforcement agencies successfully took down 13 scam syndicates comprising six job scam syndicates, three Chinese officials impersonation scam syndicates, two phishing scam syndicates, and two Internet love scam syndicates in 2022, leading to the arrest of more than 70 people responsible for close to 300 cases.

Maximise effective management of scam cases

ASCom works with relevant units in SPF to target people who facilitate scam-related activities such as money mules who assist in bank transfers, relinquish bank accounts and disclose Singpass and Internet-banking credentials to scammers. More than 150 such mules have been charged under the Computer Misuse Act 1993, Penal Code 1871 and Payment Services Act 2019 in 2022.

Swift and strategic actions

Through close collaboration with the new Scam Strike Teams in the seven Land Divisions, ASCom is dedicated to taking swifter and more holistic action to tackle scam cases that plague Singapore and the world. In 2022, ASCom coordinated 25 anti-scam enforcement operations, resulting in the arrest or investigation of more than 8,000 scammers and money mules.

Conclusion

As the number of scam victims continues to be a concern, everyone has a part to play in keeping Singapore safe and secure, especially during these uncertain times. Members of the public can learn to be aware of signs of scams and help spread the word to their friends and loved ones. Business operators such as banks, online marketplaces and telcos have a responsibility to prevent, deter and detect crimes committed through their platforms. Putting in place anti-scam measures will help business operators keep their customers safe. Together, we can help stop scams and prevent our loved ones from falling prey to them.

Minister for Communications and Information & Second Minister for Home Affairs Mrs Josephine Teo engaging with officers from ASCom, with Minister of State for Ministry of Home Affairs & Ministry of Social and Family Development Miss Sun Xueling looking on, on the right.

SPECIAL FEATURE

Understanding the SocGholish Malware Compromise: Implications and Protective Measures for Organisations

Cybersecurity firm **Ensign InfoSecurity** provides a detailed look at the technical workings behind its response to a SocGholish malware compromise, mapping the threat actor's techniques against the MITRE ATT&CK framework, as well as key learning points from the incident.

Introduction to SocGholish

The SocGholish malware compromise has emerged as a significant threat to organisations over the past five years. Primarily known for its 'drive-by' style of initial infection (T1189: Drive-by Compromise[15]), the SocGholish malware allows user information and credentials (T1003: OS Credential Dumping) to be exfiltrated, while providing lateral access across affected networks (T1021.002: SMB/Windows Admin Shares). The malware can be deployed for a standalone infection or as a loader for subsequent attacks. SocGholish has been used by ransomware groups such as LockBit to perform Drive-by Compromise and system and domain information discovery. Unlike typical phishing tactics that employ email attachments, SocGholish applies more sophisticated social engineering (T1566.002: Phishing: Spearphishing Link). Attacks masquerade as software updates using fake share links on malicious websites that unsuspecting users click on (T1204.001: User Execution: Malicious Link). This downloads a ZIP archive embedded with a malicious payload (T1204.002: User Execution: Malicious File).

As software update phishing lures become more commonplace, SocGholish has evolved to now leverage malicious scripts embedded within legitimate web pages to prevent security software from detecting its activity. Ensign observed a "radio silence" mode that allows the malware to remain dormant in the victims' environment for a pre-set duration before attempting to communicate externally.

new.medunlv.lviv.ua
chrome
You are using an older version of Chrome
Update now to keep your Chrome browser running smoothly and securely.
Your download will begin automatically. If not, click here:
Update Chrome

[15] Tactics and techniques referenced in this section are mapped to MITRE's Adversarial Tactics, Techniques and Common Knowledge (ATT&CK) framework, which provides a guideline for classifying and describing cyber-attacks and intrusions.

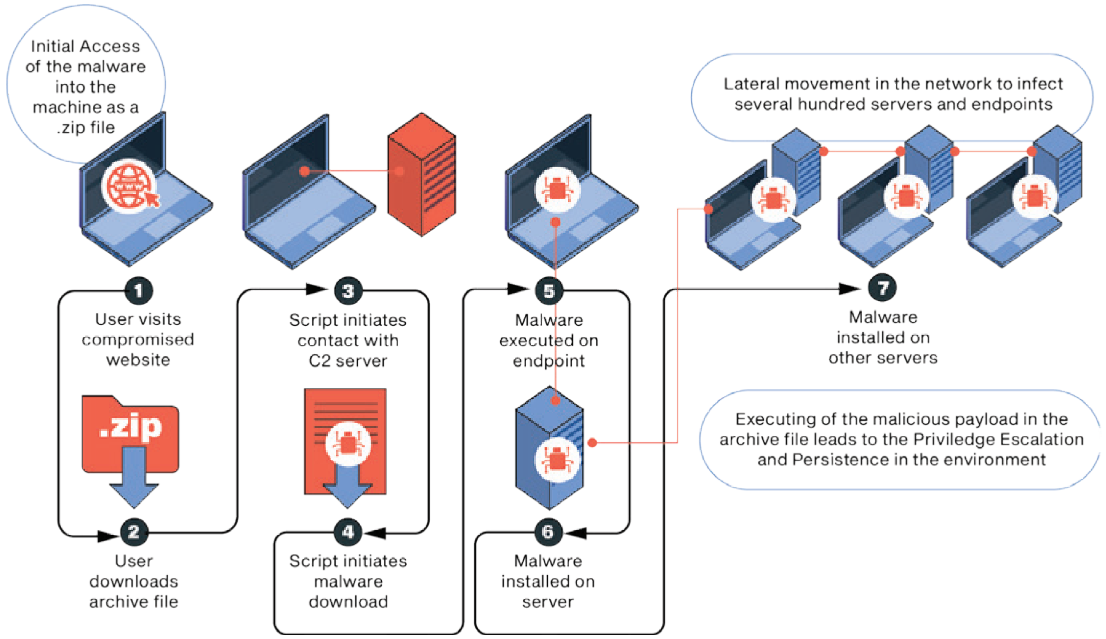

Initial Access of the malware into the machine as a .zip file
1 User visits compromised website
.zip
2 User downloads archive file
3 Script initiates contact with C2 server
4 Script initiates malware download
5 Malware executed on endpoint
6 Malware installed on server
Executing of the malicious payload in the archive file leads to the Priviledge Escalation and Persistence in the environment
7 Malware installed on other servers
Lateral movement in the network to infect several hundred servers and endpoints

Figure 3: Schematic diagram of the attack campaign

(Source: Ensign InfoSecurity)

Ensign's Threat-Informed Incident Response Case Study

Ensign provides clients with threat hunting, incident response and threat intelligence services that enables them to navigate the evolving cybersecurity landscape and tackle data breaches and ransomware attacks. In a recent incident where an employee's account was compromised leading to a breach in the client's network, Ensign's Hunt & Incident Response (HIR) and Cyber Threat Intelligence (CTI) teams executed a threat-informed incident response.

The victim was browsing the Internet on a company-issued computer and accessed a website embedded with a malicious pop-up (T1566: Phishing). The pop-up indicated that the browser required an update and provided a download link to the malware disguised as the update (T1036: Masquerading) (See Figure 3). Mistaking it for a legitimate update, the victim downloaded and executed the obfuscated malware (T1204.001: User Execution: Malicious Link, T1204.002: User Execution: Malicious File, T1027: Obfuscated Files or Information.

This led to the deployment of a backdoor that allowed the threat actor to remotely access the victim's computer (T1059: Command and Scripting Interpreter). By employing credential dumping and privilege escalation techniques (T1003: OS Credential Dumping), the threat actor successfully acquired administrator privileges and proceeded to create administrator accounts (T1136: Create Account) that allowed it to move laterally (T1550.002: Use Alternate Authentication Material: Pass the Hash) across the network and infect other machines and endpoints across the environment.

A new service was installed on the infected servers (T1543.003: Create or Modify System Process: Windows Service) to gather information (T1007: System Service Discovery, T1005: Data from Local System) and execute batch file for command-and-control connection (T1059: Command and Scripting Interpreter, T1095: Non-Application Layer Protocol, T1053.005: Scheduled Task/Job: Scheduled Task, T1071.001: Application Layer Protocol: Web Protocol).

Ensign Security Operations Centre (EnSOC) detected the anomalous network traffic and immediately escalated it to the client. The HIR and CTI teams were activated and successfully contained the incident within 48 hours, before the threat actor could gain super admin access through the domain controller.

The HIR team's customised and automated triage tool expedited the collection of information crucial to the investigation. Ensign's in-house analytics platform allowed for quick examination of the collected data, enabling a rapid identification of SocGholish malware behaviour and anomalous activities by the threat actor. Using its threat actor database, Ensign tailored the identification, containment, and recovery procedures to the perpetrator's attack vectors while minimising the likelihood of future attacks. Security findings and recommended procedures were given to the client, along with assistance in the implementation of recovery procedures.

MITRE Tactics, Techniques, and Procedures observed in the incident

Tactics	Techniques
TA0001: **Initial Access**	T1189: **Drive-by Compromise** T1566: **Phishing**
TA0002: **Execution**	T1059: **Command and Scripting Interpreter** T1204.001: **User Execution: Malicious Link** T1204.002: **User Execution: Malicious File**
TA0003: **Persistence**	T1053.005: **Scheduled Task/Job: Scheduled Task** T1136: **Create Account** T1543.003: **Create or Modify System Process: Windows Service**
TA0005: **Defence Evasion**	T1027: **Obfuscated Files or Information** T1036: **Masquerading** T1550.002: **Use Alternate Authentication Material: Pass the Hash**
TA0006: **Credential Access**	T1003: **OS Credential Dumping**
TA0007: **Discovery**	T1007: **System Service Discovery**
TA0008: **Lateral Movement**	T1021.002: **SMB/Windows Admin Shares** T1550.002: **Use Alternate Authentication Material: Pass the Hash**
TA0009: **Collection**	T1005: **Data from Local System**
TA0011: **Command and Control**	T1071.001: **Application Layer Protocol: Web Protocol** T1095: **Non-Application Layer Protocol**

Potential operational and business impact

Affected servers were taken offline for several days to remediate the issue. Some data was lost during this time as there was a gap between the last backup and the date of the incident. The business's financials may have been impacted and the organisation may have to account for the potential implications of any misuse of the stolen data.

KEY LEARNING POINTS

The increasing sophistication of SocGholish is a concerning trend. Hence, it is crucial for organisations to be aware of SocGholish and other emerging forms of malware, and take appropriate measures to protect themselves from these threats.

Round-the-clock surveillance by a security operations centre (SOC) and prompt response by an incident response team are crucial for promptly detecting and stopping potential threats. Organisations should:

- Implement strong email and firewall security defences
- Regularly back up critical data
- Update software and operating systems with the latest security patches
- Educate employees about cyber threats, phishing scams, and social engineering
- Encourage official tools for system and software updates (Windows Update, in-app updates, or official vendor sites)
- Enforce cybersecurity best practices across the organisation
- Be cautious with legitimate websites and email advertising campaigns distributing malware
- Recognise Search Engine Optimisation (SEO) and online advertising as potential exposure points to SocGholish attacks
- Uninstall unused or deprecated components and plugins, and actively monitor for unauthorised changes
- Implement the Principle of Least Privilege to reduce the impact of a potential incident

CRACKING THE CODE: LESSONS LEARNT FROM CYBER-ATTACKS

In today's digital world, all organisations face the grim likelihood of encountering cyber-attacks. Phishing, ransomware, and Business Email Compromise (BEC) scams are just some common threats today. In this chapter, we explore case studies drawn from actual incidents — from a ransomware attack that encrypted the entire corporate network, to a business email compromise that resulted in heavy financial losses. These not only highlight the devastating impact of cyber-attacks on organisations, but more importantly, the key lessons learnt. We also talk to **Mr Wayne Lim**, CSA's Head of Incident Response & Management, about his experiences dealing with these threats.

Decrypting the Lessons Learnt From a Ransomware Attack

In 2022, a Singapore-based precision engineering company with more than 1,000 employees suffered a ransomware attack. The company's systems and data were encrypted by a ransomware group and was held for a ransom of 200 bitcoins or approximately S$7 million.

Following the incident, CSA spoke to the company's Chief Executive Officer (CEO) Tan and Chief Information Officer (CIO) Lim, to understand their key takeaways and learning points from the attack.

This account is based on an actual incident. However, the names, the organisation and individuals have been changed to safeguard their privacy.

Q: How did you discover that your company had experienced a ransomware attack? What were your immediate reactions?

CEO Tan: It all started at 5.30am one morning in April, when I woke to find that I had missed several calls from CIO Lim. I could tell from CIO Lim's anxious tone that this was serious. As CIO Lim explained what happened, it became apparent that the company systems had been hit by a ransomware attack.

CIO Lim: I initially thought it was a localised IT issue. Some employees complained that they couldn't log into their systems; others said they couldn't open certain files. More serious cases saw employees unable to even boot up their computers. More and more such reports came in. That's when we knew something was wrong and that the entire network was behaving abnormally. Our worst nightmare that we were under attack was confirmed when all the files on many of our computers were renamed to gibberish and a single 'readme.txt' file appeared on the desktop. It was a note that said something like, "Your data has been encrypted and stolen. Don't bother to recover your files. It will be virtually impossible, without our decryptor. You better pay us 100 bitcoins (or S$3.5 million at the time of the incident) within three days: 50 bitcoins for the decryptor, and 50 bitcoins for not leaking the information we had stolen, or we will leak your data – all two terabytes of it."

After I recovered from the shock, my initial reaction was to try to save all the systems not connected to the network and hence not infected yet. It was quite early, so we started messaging all the staff, telling them not to connect to the company network.

Q: What remediation actions did your organisation take?

CIO Lim: Once we made sure that the ransomware was contained, we started our remediation. This included restoring our offline backups so we could resume our operations and removing malware from affected devices. Fortunately, our company policy is to back up our data every weekend, so we did not lose that much. We also hired a cybersecurity firm to assist with our investigations and forensics.

Q: What was the hardest decision you had to make during this incident?

CEO Tan: Without doubt, the most challenging decision I had to make during this incident was whether or not to pay the ransom. Initially, I held firm in my resolve not to let cybercriminals profit from our company. However, it became far less straightforward when CIO Lim informed me that the schematics and blueprints from our clients' projects have also been stolen. This was very serious, especially if these were to be leaked online. Financially, our clients' competitors may be able to gain an advantage over them if their intellectual property was exposed. Security-wise, bad actors would be able to study the blueprints and find weaknesses in the engineering projects we had built. Reputationally, even as I was ready to accept responsibility for this hack, it would be very unfair if our clients also had to suffer for our error.

In the end, the need to safeguard our clients' interests took priority. We made the difficult decision to pay part of the ransom for the hackers to erase the information they had stolen. We told them we were not interested in the decryptor and would not be paying for it. They agreed. Remarkably, within a mere two days, we managed to resume our business operations. Nevertheless, the setback incurred significant losses, amounting to hundreds of thousands of dollars. Numerous employees found themselves unable to work during this period, and our fabrication work came to an abrupt halt. Our fleet of trucks sat idle, unable to carry out deliveries. Most importantly, the decision to pay part of the ransom is a decision that haunts me. There was no guarantee that the hacker would destroy the stolen information or that they would not leak it at a later date, or sell it to other ransomware groups. Honestly, I have had sleepless nights worrying about it.

In 2022, among organisations that opted to pay a ransom demand, 80% incurred another attack[1].

Q: What are your takeaways from the attack?

CEO Tan: I had three key takeaways:

Lesson 1: A firm foundation in cybersecurity helped reduce the attacks' impact

Several years ago, I pushed for cybersecurity to be taken seriously by the company. I made it a point that cybersecurity was discussed at board meetings and treated as a board-level risk to our business, rather than just an IT issue. I checked in quarterly with CIO Lim on how our cybersecurity posture could be improved over time. Fortunately, I was fully supported by my board, which saw the importance of investing in regular penetration testing exercises and drills.

The average cost of cyber-crime for a company was US$13 million, up from US$11.7 million in 2019, representing a 11% year-on-year increase.[2]

Our relationship with the board vis-à-vis cybersecurity has matured. At first, we started with convincing the board that cybersecurity

[1] Ransomware: The True Cost of Business 2022, 2022, CyberReason, https://www.cybereason.com/ransomware-the-true-cost-to-business-2022.

[2] The Cost of Cybercrime, Accenture, 2020, Accenture, https://www.accenture.com/_acnmedia/pdf-81/accenture-health-cost-of-cyber-crime-study.pdf.

risk was important. Our board has, in turn, kept the company accountable all these years, making sure we track and mitigate such risks.

This emphasis on cybersecurity is very much aligned to our company's DNA. As an engineering company, safety has always been important to us. Just as we need to keep our workers and clients safe in the physical world, so too in cyberspace, with strong cybersecurity measures. It is precisely because of this foundation in cybersecurity that the impact of this ransomware attack was reduced.

Lesson 2: Cyber-attacks can still occur even with the best cybersecurity practices in place

We had done all we could. We worked to ensure that our cybersecurity strategy and framework were robust and referenced established cybersecurity frameworks or standards, such as the National Institute of Standards and Technology Cybersecurity (NIST) Framework and "International Organisation for Standardisation (ISO) 27001. Additionally, we conducted penetration testing exercises and vulnerability assessments periodically to ensure that our systems were secure.

Despite this, the company was still hit. I suppose the risk is greater when your firm's systems run 24/7. Especially in this case, where the threat actor seemed sophisticated. Our vendor told us they were in our network for nearly two weeks before they sprang their attack. But I would say that I have learnt not to be complacent and to continue to examine how to improve the organisation's cybersecurity, even if we feel it is already at a high level.

Lesson 3: An effective response to a cyber-attack requires the coordinated efforts of a cross-functional team

Besides working closely with CIO Lim and the IT team, I was supported by the legal and public communications departments. The legal team helped navigate the legal implications of the attack and protect our interests, such as reviewing legal obligations, working with law enforcement, etc. We reported the incident to SPF, PDPA and CSA as soon as possible. Our public communications department managed our external communications with internal and external stakeholders, keeping them apprised of what had happened and how the company was managing the incident, etc. These cross-functional teams proved invaluable as the implications of a ransomware attack were complex and multi-faceted. They could not have been easily handled by the IT team alone. The existing culture of trust cultivated between the Board, CIO Lim and myself, also allowed me to act swiftly and confidently.

Beyond the Inbox: A Business Email Compromise (BEC) Lesson

In 2022, a Singapore-based law firm with 15 employees became a victim of a BEC, a type of email scam that involves an attacker impersonating or taking control of a legitimate email account to defraud others. The threat actor impersonated the firm, sending out 2,000 phishing emails to defraud customers into providing details like banking credentials. This resulted in financial losses amounting to more than S$100,000.

Following the incident, Ms Sharifah, one of the law firm's partners, shared her experience and what they learnt.

This account is based on an actual incident. However, the names, the organisation and individuals have been changed to safeguard their privacy.

Q: How did you discover that your firm had experienced a BEC? What were your immediate reactions?

I received a call from my staff. My heart sank when I heard that several of our clients had likely been scammed. The team discovered that several clients had received emails from "our firm" asking them to provide their banking credentials so that "we" could credit compensation received from their cases. The clients later realised that instead of receiving compensation, unauthorised deductions had been made from their accounts. The worst thing was that the email looked like it had been sent by us from our legitimate email address.

Several questions swirled in my head: "What had happened? Was this an insider job? Did any of our clients' case files get taken?" But I had to put this all aside for the time being. I immediately instructed our staff to inform all our clients about what had happened and to provide advice, such as not to respond to such emails and fall for the ruse. As monies and possible data loss were at stake, we reported the case to CSA, SPF and PDPC.

From January to March 2022, at least 93 victims lost S$56.2 million to BEC scams in Singapore.[3]

[3] At least 93 victims have lost S$56.2 million to business email compromise scams from Jan to March 2022: Police, 29 July 2022, The Straits Times, https://www.straitstimes.com/singapore/courts-crime/at-least-562-million-lost-to-business-e-mail-compromise-scams-between-jan-and-march-2022-police.

Q: Did you find out what happened later?

Yes, we found that someone had hacked into our firm's mail server and sent out 2,000 phishing emails to our clients. Because the premise of monetary compensation was so convincing and a legitimate email address was used, several of our clients fell for the ruse and provided their banking credentials. The threat actors used these credentials to make unauthorised deductions from our clients' bank accounts. To date, our clients' financial losses have amounted to more than S$100,000. We were at a loss as to how we should proceed with the matter: Whose liability was this? Should we compensate our clients? At the same time, we were also thankful that no other data, such as case files, was exfiltrated because this could have compromised ongoing cases or even cause further lawsuits.

Q: What were the remediation actions taken?[4]

Once our IT vendor narrowed the problem to the mail server, we suspended the affected mailboxes and reconfigured them to prevent more phishing emails from being sent. To avoid recurrence, we worked with our IT vendor to strengthen our cybersecurity, e.g. implementing robust email security solutions, diversifying the ways that employees can authenticate their devices.

Q: What did you learn from this incident?

I would say we learnt two things. First, a cybersecurity compromise affects our clients. We rarely consider cybersecurity as a duty of care to our clients who entrust us with keeping their privileged information safe. This incident has shown us that "it will never happen to me" is a myth! We must actively keep our computer systems secure to ensure we do all we can to prevent such things or any other cyber breaches from happening.

Second, the reputational cost of cybersecurity breaches is real. Following this incident, several major clients switched law firms, resulting in a serious loss of revenue. They simply did not have faith that we were doing enough for our cybersecurity and did not want to risk any potential compromise or data leak. We knew that we not only had to put the necessary cybersecurity measures in place, but we also restore our clients' faith and confidence in our cybersecurity. Hence, we are working towards demonstrating this by getting certified against relevant security standards or marks, such as ISO 27001 and CSA's Cyber Trust mark[5].

[4] For more information on how to prevent or respond to BECs, see Business Email Compromise (BEC) PlayBook, CSA, https://www.csa.gov.sg/docs/default-source/publications/singcert/pdfs/playbook-for-business-email-compromise.pdf?sfvrsn=96f41227_1

[5] Cyber Trust, CSA, https://www.csa.gov.sg/cyber-trust/

Lessons Learned the Hard Way: Tales of Exploited Unpatched Vulnerabilities

In 2022, a local tuition centre with five employees saw threat actors exploiting unpatched vulnerabilities in their computer systems to steal student data, such as academic records and personal information.

Anu, the tuition centre's owner, talked about about this harrowing experience and what he learnt.

This account is based on an actual incident. However, the names, the organisation and individuals have been changed to safeguard their privacy.

Q: How did you discover that your tuition centre's computer system had been exploited?

At first, we had noticed our computers running a lot slower than usual and several files becoming mysteriously corrupted. Alarm bells started ringing when one of our parents reported that he was able to access the personal information and academic records of other students using our tuition centre's web portal, which should not have been the case. After a thorough investigation, we discovered that a hacker had exploited vulnerabilities in our computer systems, which allowed them to gain access to our sensitive data.

62% were unaware that their organisations were vulnerable before the data breach.[6]

Q: We understand that a patch for the vulnerabilities had been available some months before the incident. Why didn't you patch them earlier?

Truth be told, we did not even know that our computer systems had any vulnerabilities. We are a small business and cannot afford to have a dedicated IT staff look after our systems. Usually, it is our administrative manager, who is a little savvier with computers, who troubleshoots any problems that arise. Otherwise, the computer systems are left on their own. We don't fix what isn't broken. We update our software when the system prompts us to, but cybersecurity was really the last thing on our minds when working with a shoestring budget.

[6] Ponemon Study on Gaps in Vulnerability Response, Service Now, 19 March 2023, https://www.servicenow.com/lpayr/ponemon-vulnerability-survey.html

60% of breach victims said they were breached due to an unpatched known vulnerability where the patch was not applied.[7]

Q: How did you remediate this incident?

We knew that this time things were serious because our students' sensitive personal data had been exposed and parents were getting angry. We quickly got a cybersecurity expert to thoroughly check our systems and clean it of any malware. The affected systems were immediately isolated and the compromised systems disabled. We notified the PDPC, as well as all our customers, giving them guidance on how they could protect themselves from possible identity theft or other malicious activity.

We also made longer-term plans to engage managed security services to provide us with ongoing monitoring and management of our computer systems. In this way, we can prevent a repeat of such issues, especially knowing that this incident could have been prevented with timely patching.

Q: What advice would you give SMEs that may not have the resources to hire cybersecurity experts?

I can't say that I am an expert, but from this incident, I would say that it is important to have IT or cybersecurity support, whether from a managed security service provider, online remote support services, or a freelance CISO. Ongoing monitoring and management of computer systems and regular patching could have prevented costly remediation efforts for us. By our estimates, we spent nearly triple the amount remediating the incident (not including the loss of revenue) compared to what it would have cost us to have taken preventive measures.

It is estimated that the percentage of total cost spent on preventing an attack was nearly **20%.**

The average cost savings from preventing the attack was **US$682,650.**[8]

We also learnt that there are several government resources, such as from CSA, which we can tap. This includes cybersecurity resources, such as SME owner toolkits[9] and a grant-supported programme that helps SMEs develop cybersecurity health plans by tapping on cybersecurity consultants onboarded by CSA[10].

[7] Ponemon Study on Gaps in Vulnerability Response, Service Now, 19 March 2023, https://www.servicenow.com/lpayr/ponemon-vulnerability-survey.html

[8] The Economic Value of Prevention in the Cybersecurity Lifecycle, Deep Instinct, April 2020, https://info.deepinstinct.com/value-of-prevention

[9] SME Owner Toolkits, CSA, https://www.csa.gov.sg/leaders-toolkit

[10] Cybersecurity Health Plans, CSA, https://www.csa.gov.sg/cybersecurityhealthplan

Ask the Incident Responder:

Mr Wayne Lim, Head of Incident Response & Management, CSA

SingCERT
Singapore Cyber Emergency Response Team

Mr Wayne Lim has over 20 years of cybersecurity experience in the public and private sectors as a digital forensics investigator and incident responder. He has led various incident response and cybersecurity operations teams, investigating hundreds of incidents at the organisational, sectoral and national levels. He is also an Adjunct Senior Fellow teaching Digital Forensics at the SUTD Academy.

Q: Describe what you do at CSA.

As Head of Incident Response & Management at CSA, I oversee the response and investigation of significant cyber threats and incidents to Singapore's critical digital systems (such as CII systems) and safeguard Singapore's cyberspace through the Singapore Cyber Emergency Response Team (SingCERT).

Q: Tell us more about your key responsibilities.

There are many! However, I would say that my key roles are to prevent and protect against cybersecurity threats, and to respond to them when they occur. In matters of incident response, we work closely with our stakeholders, such as the CII sector leads and owners to help get them back on track. We help ensure that cyber incidents are properly contained and investigated, with the necessary remediation measures put in place. Just like crime scene investigators, we collect and analyse evidence on the systems to reconstruct the sequence of events and identify if any malware was used in the attack. Any findings form part of our remediation and preventive measure recommendations to these stakeholders.

Through SingCERT, we work to facilitate the detection, resolution, and prevention of cybersecurity incidents in Singapore. Internationally, SingCERT works with other national CERTs to foster closer working relationships and promote information sharing. Domestically, SingCERT provides alerts, advisories, and incident handling guidelines to assist businesses and members of the public in preventing and recovering from an incident.

Q: What are the top three cyber threats that organisations in Singapore face today?

From my experience in both the private and public sectors, I would say that the top three cyber threats observed include ransomware, actors exploiting unpatched vulnerabilities, and BEC:

Ransomware:
Increasingly, threat actors are using double extortion ransomware that exfiltrates the victim's data in addition to encrypting it. This puts pressure on the victim to pay even if they have backups or other ways to restore their data.

Actors exploiting unpatched vulnerabilities:
Among cases reported, we observed a trend of organisations breached due to unpatched

vulnerabilities, especially ones whose email servers are hosted on on-premises Microsoft Exchange Servers. Since early 2021, threat actors have actively targeted Microsoft Exchange Servers to deploy backdoors and malware, including ransomware. Although Microsoft released security updates to address those Exchange vulnerabilities, the vulnerabilities remain unpatched due to the complexity of the environment, limited resources, and underestimation of impact when the vulnerabilities are successfully exploited.

BEC:
A type of scam that involves an attacker impersonating or taking control of a legitimate email account to defraud companies. We observed about 50 reported cases to SingCERT in 2022.

Q: Were there differences between the incidents you handled within government and the private sector?

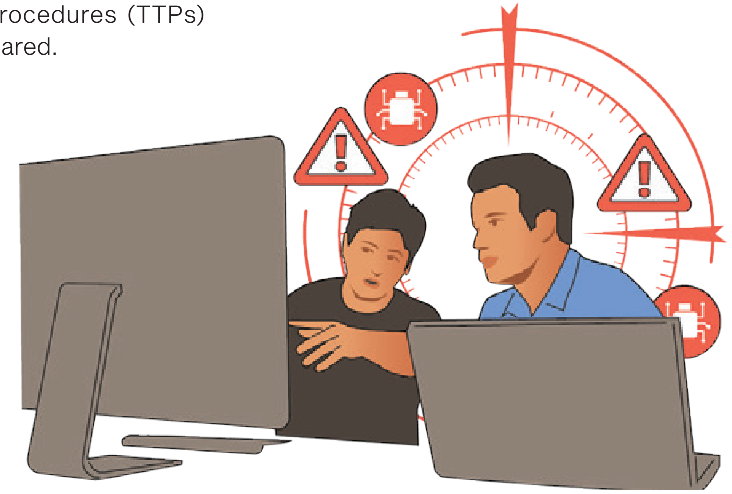
The majority of incidents in the private sector were financially motivated and opportunistic attacks, including data breaches, ransomware and crypto miners. Incident response was a mixed bag — most private sector organisations may not have a dedicated incident response team, particularly the smaller ones. The typical approach is to quickly recover from the incident and resume business normalcy. The root cause analysis and understanding of the threat actor's tactics, techniques, and procedures (TTPs) may not be conducted or shared.

As the public sector deals with cyber espionage and politically or financially motivated cyber-attacks, we focus on identifying the indicators of compromise, root causes and threat actors' TTPs for broader sharing, so that proactive action can be taken to secure the wider cyberspace.

Q: What strikes you the most about the incidents you have handled?

Besides the technical aspects of the cases, what strikes me most is the human face behind these incidents. Real people, real livelihoods are at stake when a business is affected by a cyber-attack. What has left a vivid impression is what a Chief Information Security Officer (CISO)[11] once told me: "There is huge risk in being a CISO. When all is good, things are taken for granted. But when a cyber-attack hits your organisation, it is no good saying, 'I told you so'. The cost of an attack on our reputation and the remediation cost far outweighs regular investments in cybersecurity. We take an outsized gamble to say we accept our cyber risk without knowing its true cost."

His organisation was attacked, and they spent far more on remediation and working to restore their reputation with clients. Although the organisation did step up its security posture after the incident, it was a hard lesson to learn. Their entire legacy system had to be decommissioned and rebuilt from scratch.



[11] The CISO is a senior-level executive who oversees an organisation's information, cyber and technology security.

Q: What are the top three things organisations in Singapore can do to protect themselves?

Cyber threats are constantly evolving. Completely protecting against all possible cyber-attacks is unlikely. While it is difficult to prevent incidents arising from sophisticated cyber-attacks, a large portion of incidents due to opportunistic attacks can be prevented by practicing good cyber hygiene. These are three things organisations can do first to reduce the risk and impact of a successful cyber-attack:

Set up multi-factor authentication:
Requiring additional forms of authentication increases the difficulty for threat actors to gain access using stolen or leaked credentials.

Establish an effective patch management regime:
This reduces the risk of successful cyber-attacks through known vulnerabilities.

Back up data regularly:
Having recent backup data can help organisations recover quickly from a ransomware attack.

Besides the above, a multi-layered approach involving technical and non-technical measures should be taken. Organisations should adopt the following best practices to better prevent, detect and respond to cyber threats.

Prevent: Use anti-virus software, minimise exposure on the Internet by allowing only necessary services, and limit user privileges to prevent installation or execution of unauthorised software.

Detect: Train employees to recognise phishing emails, assess the security posture regularly to identify vulnerabilities, and configure alerts to notify potential incidents and suspicious activities.

Respond: Develop an incident response plan and playbooks. Conduct regular cyber exercises to test the plan.

Q: How do you set up your home network so you do not become a victim of hackers? What brand of routers and modems do you use?

The brand is a secret! (Laughs), though I can share that my router is rated at Level 4 of the CLS[12]. The CLS Level 4 rating gives me more assurance that my router has undergone penetration testing by specialists, and cannot be hacked easily. Under the CLS, the router's manufacturer is obligated to update the software and to remediate the security flaws. Since the router is the gateway between the Internet and my home network, getting a more secure one to protect my personal data is definitely worth it.

In addition to buying CLS-labelled products, I would do a few things when setting up my home network. First, I make sure that I would always use a strong and unique password (including the username, if possible). Secondly, I will ensure that automatic update is enabled so that the software running on my devices are always up to date. Thirdly, for CLS-labelled products, remote management is disabled by default. I will only enable this feature if I truly have the need for it and understand the risks. Together, these changes should help to prevent hackers from gaining unauthorised access to my router and from possibly gaining control of my work.

[12] Read more about the CLS here: www.csa.gov.sg/cls

TOMORROW'S DIGITAL SECURITY CHALLENGES

We interact with a rapidly evolving cyberspace, where changes are inevitable as the world becomes increasingly digitalised and connected. This is exacerbated by geopolitical and socio-economic developments amidst the ongoing Russia-Ukraine conflict, just as the world is returning to normalcy after the prolonged COVID-19 pandemic.

In this chapter, we look ahead through the lens of society, policy, technology, and economics to discern key developments of concern on the horizon and how these developments might translate to implications for cybersecurity. We begin with a look at the notion of "collective efficacy" in cybersecurity from our partners in academia, **Mr Benjamin Ang** and **Ms Teo Yi-Ling**, from the Centre of Excellence for National Security (CENS) at the S. Rajaratnam School of International Studies (RSIS) in NTU. This is followed by a look at the repercussions of 'ransom for reputation' (R4R) and legislating against ransomware payments, the threats and opportunities posed by AI, the systemic risks that might arise for cybersecurity due to economic adversity before wrapping up with a revisit of quantum computing.

On the Horizon - Cybersecurity and Collective Efficacy

Contribution by Mr Benjamin Ang
and Ms Teo Yi-Ling[1]
CENS, RSIS

How would you feel to discover that you have fallen victim to a complex and convincing phishing scam (because you would never have been fooled by a simple one) by criminals impersonating your bank, leading to you losing a huge sum of money from your bank account? How would you feel if your bank then told you, its loyal customer, that this is totally your responsibility (or fault), according to the standard terms and conditions, and that they are not required to help you?

This scenario isn't far-fetched – it has happened to some of us. Cyber threats are rising. Cybercrime scams are growing more sophisticated over time. Digitalisation is spreading throughout the world, accelerated by the COVID-19 pandemic, which in turn exposes everyone to more risk.

Unfortunately, the response of some businesses, even some sectors, has been to pass the risk to everyday people like you and I. They do so through their standard terms and conditions, which may state, among other things, that cyber risk is borne by customers, or liability for loss due to cyber incidents is excluded, or that the duty is on customers to protect ourselves. But seeing how sophisticated the attackers are, is this a realistic or fair obligation?

On one hand, this is in line with conventional business principles of contractual risk allocation. On the other, consumers of digital services often have little or no bargaining power because we must click "accept" to the standard terms and conditions (which we usually don't read, since we have no choice anyway) before we can use these services. As more products and services go online – food delivery, groceries, retail, education – us everyday people find ourselves agreeing to more and more of these onerous terms.

We could appeal to the law, because in theory, contractual clauses that are manifestly unfair, burdensome, or too broadly drafted will be construed against the party seeking to rely on them. But how many people know how to take on a legal dispute or are willing to risk their time and money?

In the OCBC phishing scam incident, the bank made a goodwill gesture of making up the losses incurred by customers who were victims of the scam and made technical improvements to the way it communicates digitally with customers. While laudable and the moral thing to do, reimbursement or goodwill may not be a sustainable policy. And it fails to address the root of the problem. Customers do bear some responsibility for their own security, but building the company's agency and efficacy in cyber hygiene serves the public interest.

There may be better gains if banks and other businesses that provide products and services digitally invest in a few things from the start: Redesigning processes to obstruct scammers, educating customers on cybersecurity, giving customers tools to protect themselves, and working with customers to build collective security. This investment can pay off in stronger customer relationships and reduced losses if all stakeholders cooperate to identify where the risks are and how to mitigate them.

New cybersecurity behavioural research shows that while building "personal efficacy" in cybersecurity (i.e., the individual's ability to spot scams) is good, building "collective efficacy" in cybersecurity (where others can help the individual spot scams) is even better. This principle has been observed in neighbourhood groups overcoming crime, groups of educators helping students, and sports teams.

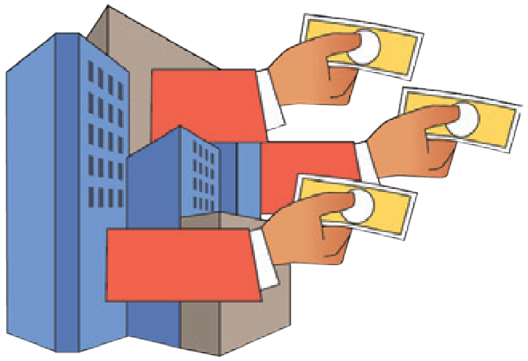
One example of a successful collective model could be in families where younger members help their senior elders navigate confusing digital goods and services and help them to avoid scams. This works best with an encouraging, non-judgmental, and caring support group, whether provided by family or by other groups like SG Digital Community Hubs.

This could even be adopted by groups of employees or suppliers working with customers, or other scenarios where individuals or businesses need help to fend off cyber threats.

When this happens, it is an organic outcome of different parts of society reaching across to and supporting one another in building cybersecurity. We know that cybersecurity is a team sport; perhaps it is time to make it a family activity as well.

[1] Mr Benjamin Ang is a Senior Fellow and Deputy Head of Centre of Excellence for National Security; Coordinator of Cyber and Homeland Defence Programme. Ms Teo Yi-Ling is a Senior Fellow with the CENS at RSIS.

Over the Horizon - The Anticipated Emerging Cyber Threats in the Mid and Far-term



Ransom for Reputation (R4R) and Legislating Against Payment

Given the spate of high-profile data breaches in 2022 (e.g. Nvidia, Uber and Optus), organisations might consider mitigating reputational damage as a more compelling reason to pay the ransom than regaining access to their encrypted data in the year ahead. As such, while threat actors will continue to rely on extortion, actual ransomware deployments may decline. RaaS providers might turn their attention to focus more on data exfiltration and public shaming on “leak sites”. With the general willingness of the industry and the public to accept news of a data breach at face value, a threat actor might also conjure fictional breaches by publicising repackaged data from prior breaches or information fused through open-source data scraping.

An October 2022 International Data Corporation survey of more than 500 CIOs from over 20 industries globally highlighted that two-thirds of the respondents paid the ransom. Some cybersecurity researchers commented that this is indicative of some falling prey to ransom for reputation (R4R) or ‘extortionware’. In all, global ransomware damages are expected to exceed US$30 billion by 2023, according to cybersecurity company Acronis.

IMPLICATIONS

Organisations willing to pay ransom to safeguard their reputation could find themselves in a lose-lose situation. Growing global sanctions introduced against Russia in 2022 amidst the Russia-Ukraine conflict means that doing so could constitute a sanctions violation. On a broader scale, research company Gartner expects 30% of countries to pass legislation regulating against ransomware payments by 2025. While well-intended, the focus should not be on penalising organisations that have decided to pay, but rather on fostering a culture of openness, transparency and support for organisations impacted by ransomware.

Legislating against ransomware payments could drive breaches further underground. It might hence be more impactful to educate organisations that paying ransom to any threat actor creates an unvirtuous cycle. It reinforces their nefarious behaviour and empowers them to increase the scale and extent of ransoms demanded.

AI for Bad and Good

The advent of ChatGPT3.5 (Chat Generative Pre-trained Transformer version 3.5) AI chatbot in November 2022 was described by Harvard Business Review as a “tipping point for AI”.

Its successor, ChatGPT4 that was launched in March 2023, is but one of several advanced Natural Language Processing (NLP) chatbots on the horizon; and their capabilities are increasing exponentially with time. On the cybersecurity front, researchers have experimented with ChatGPT3.5 and its successor to perform a variety of offensive and defensive tasks, including (i) crafting phishing emails, (ii) writing “ransomware code” for MacOS, (iii) generating YARA and Sigma malware detection rules, and (iv) identifying buffer overflows in code. Its dual-use nature has led some cybersecurity researchers to compare ChatGPT and similar AI chatbots to legitimate adversary simulation and penetration testing software Metasploit and Cobalt Strike, which have also been exploited by threat actors for malicious cyber activities.

Furthermore, with AI-enabled art generators trained on increasingly large-scale image databases, limited technical savvy is now required to generate photorealistic deepfakes, making such technology more accessible to the masses. While state-of the-art generators are still flawed (e.g. real-time deepfakes can often be foiled by a sideway view), such technology is constantly improving. It might only be a matter of time before threat actors learn to leverage this for their nefarious activities.

IMPLICATIONS

As AI becomes more accessible and advanced, threat actors may leverage such technology to craft highly targeted spear-phishing campaigns. They could do this by automating the collection of open-source information from social media posts and job advertisements and fusing them to Personally Identifiable Information (PII) harvested from prior data breaches. GovTech cybersecurity researchers at the Black Hat Defcon 2021 conference shared that respondents are more likely to respond to AI-generated targeted phishing emails than emails created manually.

Threat actors may also get more creative in the use of AI-enabled deepfakes to impersonate C-suite executives to facilitate account takeovers, business fraud, or impact the share price or reputation of an organisation. Cloud computing company VMware noted in its ‘Global Incident Response Threat Report 2022’ that two-thirds of respondents saw malicious deepfakes used as part of an attack in the past year. Cybersecurity researchers have hence advocated for the use of AI to detect deepfakes, such as through Intel’s FakeCatcher, which claims a 96% accuracy rate.

[cont. next page]

This alludes to AI being a double-edged sword that can be adopted by attackers and defenders alike. AI is expected to be increasingly incorporated for cybersecurity, with an anticipated growth in market size from US$22.4 billion in 2023 to US$60.6 billion in 2028. Specifically, the use of NLP (akin to ChatGPT) and Machine Learning (ML) technologies can empower the creation of an evolving baseline to provide real-time insights for ascertaining potential cyber-attacks by identifying anomalous patterns of system behaviours, augmenting network monitoring for signs of lateral movement, and enabling AI-based behavioural biometrics through tracking mouse and keystroke activity.

While AI-empowered cybersecurity solutions are not new, what will catalyse its adoption in the next few years will be a confluence of (i) continued global shortage of cybersecurity workforce requiring technological augmentation, (ii) vastly improved AI detection efficacy, and (iii) more success stories from industry peers. For example, a 2022 IBM study found that organisations using AI and automation had a 74-day shorter breach lifecycle and saved an average of US$3 million than those without.

Systemic Risks from Economic Adversity

More than a year into the fighting, the Russia-Ukraine conflict shows no signs of abating. Its impact continues to be felt in Europe and beyond in terms of energy prices, food shortages, and increased interest rates to contain inflation. While food and energy commodity prices have come down, inflation remains high in many countries. In particular, the International Monetary Fund (IMF) anticipates a global economic downturn in 2023, having lowered its global growth forecast to 2.7% from 3.2% in 2022.

The resultant financial pressures, coupled with a rise in cost of living, will invariably impact the general workforce, potentially resulting in increased fatigue and distraction. Cybersecurity company 1Password's 'State of Access 2022 Report' indicated that 79% of 2,000 North American workers surveyed felt distracted on a typical workday amidst the ongoing "permacrisis" defined by Collins Dictionary as "an extended period of instability and insecurity, especially one resulting from a series of catastrophic events (such as the prolonged COVID-19 pandemic)".

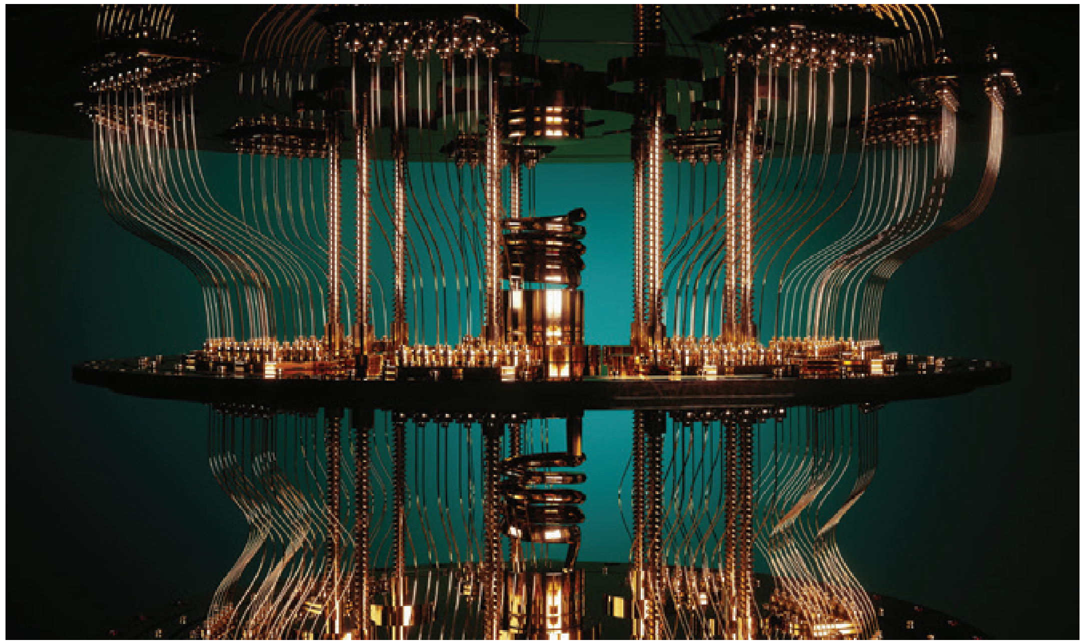
IMPLICATIONS

There is a tenable correlation between cybercrime and economic adversity as underscored by INTERPOL's August 2020 'COVID-19 Cybercrime Analysis Report'. Crises create opportunities for threat actors to exploit via phishing as they capitalise on psychological weaknesses, which are at greater risk at a time of "permacrisis". This includes manufactured urgency and greater inclination to explore opportunities to make up for personal financial shortfalls.

For example, after the UK government announced an automatic £400 energy bill discount for all British households to help offset soaring prices in May 2022, threat actors sent phishing emails and texts to individuals, baiting them to provide their personal details and set up a direct debit to "receive the discount". Economic adversity may also amplify the risks of insider threats in organisations as susceptible individuals are lured by threat actors to facilitate access for monetary gains. For example, the ransomware group Lapsus$ advertised in March 2022 that they were looking to buy remote VPN access from insiders in major technology and telecom organisations such as Microsoft and AT&T.

Impending economic adversity also leads organisations to scrutinise their budgets more closely and focus on cutting what is perceived as non-essential expenditure. Cybersecurity is often seen by uninformed C-suites as an overhead rather than an essential function that helps safeguard the organisation's bottom line and reputation. Although market analysts claim that cybersecurity is a recession-proof industry, organisations may be obliged to freeze or postpone hiring cybersecurity personnel in an economic downturn, thereby exacerbating their cyber talent gap in the longer run.

Tighter cybersecurity budgets and fewer resources may translate to subpar security postures across organisations, an asymmetry which will be capitalised by threat actors, thereby amplifying the risks of ransomware attacks and breaches in 2023. In the year ahead, CISOs will invariably be more pressed to demonstrate how cybersecurity provides broader business value and to promote organisational cyber resilience as a boardroom agenda which requires C-suite involvement beyond just IT. This requires promulgating a common language of risk, resiliency, and reputation to bridge technical cybersecurity requirements and overall business objectives.



Quantum Computing: Boon and Bane, All at Once

Three years ago, SCL 2019 forecasted that quantum computing would disrupt industries despite its nascent stage of development. Since then, there have been significant technological breakthroughs. These include IBM's 433-qubit Osprey chip, touted as the world's most powerful quantum processor, which the company unveiled in November 2022. Its computational power, when translated into conventional computing bits, surpasses the total number of atoms in the known universe. Equally noteworthy is that IBM has committed to delivering a 1,121-qubit processor by the end of 2023 and another that can surpass 4,000 qubits by 2025.

The market, worth US$412 million in 2020, is projected to reach US$8.6 billion by 2027, according to estimates by market intelligence firm International Data Corporation. McKinsey and Company present an even more optimistic projection of it exceeding US$90 billion by 2040. It is no exaggeration to say that the quantum computing market has grown multifold since we last reported on the topic.

The immense potential of quantum computers lies in their ability to exponentially increase computing power over traditional computers. Unlike classic computers that use binary "bits" of 0s and 1s, quantum computers use "qubits" that can exist in a superposition[2] of both states. This enables quantum computers to perform multiple calculations at the same time, resulting in a vast increase in computational efficiency compared to traditional computers. Complex problems, such as global climate modelling, which now take years to solve could be solved in a matter of seconds.

[2] This means that the qubits can be in multiple states at once, allowing them to represent multiple values simultaneously.

IMPLICATIONS

Quantum computing could dramatically amplify current AI capabilities in a wide range of fields including cybersecurity. Its unprecedented processing power can enable AI to analyse trillions of data points to significantly enhance the accuracy and usefulness of their underlying algorithms. With this ability, AI can analyse a much larger data pool to generate real-time insights, which can predict potential cyber-attacks. It could enable the customisation of reference cyber threat scenarios for companies in a selected sector or industry simultaneously, along with bespoke mitigation measures.

However, like AI, quantum computing comes with opportunities and risks. A key cybersecurity — and by extension, national security — risk is the potential of exploiting it to break the encryption algorithms used to protect our data and communications. Encryption algorithms rely on complex mathematical calculations that are immensely difficult to solve. With the power that quantum computing brings, circumventing that complexity is far more achievable. This is why news headlines in January 2023 claiming that researchers had leveraged quantum computing to break Rivest-Shamir-Adleman (RSA), a leading-edge encryption algorithm, was particularly attention-grabbing.

If proven true, its implications would reverberate globally as RSA is a ubiquitous encryption algorithm that safeguards websites and mobile applications. For now, it appears that we have some way to go before quantum computers can do so. According to cybersecurity experts, breaking RSA requires a million or more qubits, a magnitude beyond IBM's 433-qubit Osprey quantum processor. Therefore, despite the substantial advancements in quantum computing, its ability to break RSA's encryption algorithm appears to be an overstatement for now. However, its eventual possibility means that countries and organisations must be proactive in deploying pre-emptive quantum-safe encryption methods.

Despite being a medium to long-term risk, the global conversation on how to prepare for a post-quantum cybersecurity world has already begun. The UK announced £2.5 billion in state funding for quantum research in March 2023, while China has reportedly increased its state funding to US$15 billion. Many countries will likely follow.

GLOSSARY

Advanced Persistent Threat (APT)

An attack in which perpetrators successfully gain access to a targeted system and stay undetected for a long period of time to exfiltrate, modify, or destroy critical data. APTs can also refer to the advanced and often state-linked or state-sponsored threat actors who conduct extended campaigns, such as cyber espionage.

Attack Surface

Refers to all vulnerable resources of a system or the sum of points through which an attacker could try to enter an environment.

Bot/Botnet

An automated software program used to carry out specific tasks. A botnet is a network of compromised computers infected with malicious bots, controlled as a group without the owners' knowledge.

Command and Control (C&C) servers

Centralised devices operated by attackers to maintain communications with compromised systems (known as botnets) within a targeted network.

Critical Information Infrastructure (CII)

The computer or computer system necessary for continuous delivery of an essential service, which a loss or compromise of would debilitate the availability of essential services in Singapore.

Cryptocurrency

A form of digital token secured by cryptography and can be used as a medium of exchange, a unit of account, or a store of value. Used synonymously with digital or virtual currency. Examples include Bitcoin, Ether, and Litecoin.

Cyberspace

The complex environment resulting from the interaction of people, software, and services on the Internet by means of technological devices and networks connected to it, none of which exists in any physical form.

Singapore's cyberspace includes domain names with ".SG" or Singapore-mentions, Internet Protocol (IP) addresses used in Singapore, and Internet Service Providers (ISPs) located here.

Dark Web

A section of the Internet accessible only through software that allows users to remain anonymous or untraceable. The Dark Web is part of the Deep Web, which encompasses web resources that search engines like Google and Yahoo cannot find. These include legitimate but private resources (e.g. email), or public resources behind a paywall or log-in wall (e.g. paid journal subscriptions).

Data Breach

The unauthorised access, collection, use, disclosure, copying, modification, or disposal of personal data or confidential information in an organisation's possession or under its control.

Denial-of-Service (DoS)/ Distributed DoS (DDoS)

Where an attacker attempts to prevent legitimate users from accessing information or services online. The most common and obvious type of DoS attack occurs when an attacker "floods" a network with information. In a distributed DoS attack, an attacker takes unauthorised control of multiple computers that may be harnessed as a botnet to launch a DoS attack.

Hacktivists

An individual or group aiming to undermine the reputation or destabilise the operations of an entity, or to publicise their political or social agenda and gain recognition, usually by conducting DDoS attacks or hacking an organisation's website.

Infected Infrastructure

Compromised devices within SG cyberspace abused by attackers for malicious purposes, such as conducting DDoS attacks or distributing malware and spam.

Internet of Things (IoT)

The vast network of everyday objects, such as baby monitors, printers, televisions, and autonomous vehicles, that are connected to the Internet.

Malware

Malicious software intended to perform unauthorised processes that will have adverse impact on the security of a computer system, such as virus, worm, Trojan horse, spyware and adware.

Operational Technology (OT)

Computing systems used to manage industrial operations. OT systems include production line management, mining operations control, oil and gas monitoring, etc.

Personal Data/ Information

Data which, on its own (e.g. full name, NRIC number) or in combination with other available data (e.g. medical or educational information), can be used to distinguish or trace an individual's identity.

Phishing

A common technique used by threat actors to trick people (typically through emails) into divulging personal information, transferring money, or installing malware.

Programmable Logic Controller (PLC)

An industrial computer that has been ruggedised and adapted for the control of manufacturing processes, such as assembly lines, machines, or any activity that requires high reliability, ease of programme and process fault diagnosis.

Ransomware

Malware that encrypts files on a victim's device, rendering them unusable until a ransom is paid, usually in the form of Bitcoin or other cryptocurrencies. It may spread through phishing emails that contain malicious attachments or links, or malicious pop-ups that appear when users access unsafe websites.

GLOSSARY

Red Teaming

An exercise that focuses on systematically and rigorously (but ethically) identifying an attack path that breaches an organisation's security defences using real-world attack techniques.

Supervisory Control and Data Acquisition (SCADA)

A control system architecture comprising computers, networked data communications, and graphical user interfaces for high-level supervision of machines and processes. Industrial Control Systems are often managed via SCADA.

Spoofing

Tricking computer systems or other users by hiding or faking one's true identity. Commonly spoofed targets include emails, IP addresses, and websites.

Spyware

Software designed to enter a device to gather and forward data to third parties without knowledge or consent.

Trojan

A type of malware that disguises itself as a legitimate software to trick users into downloading and installing it on their systems. Once activated, the malware will carry out malicious actions that it is designed for.

Zero Day Vulnerabilities

A vulnerability in a system or device that has been disclosed but not yet patched.

Editorial Team

Mr Willis Lim

Dr Luke Ho

Ms Grace Dong

Ms Charlene Zeng

Ms Ang Jia Xi

Contributors

Anti-Scam Command (ASCom), Singapore Police Force (SPF)

Mr Benjamin Ang and Ms Teo Yi-Ling, Centre of Excellence for National Security (CENS) in the S. Rajaratnam School of International Studies (RSIS) in Nanyang Technological University (NTU)

Digital and Intelligence Service (DIS), Ministry of Defence (MINDEF)

Ensign Infosecurity

Government Technology Agency (GovTech)

Personal Data Protection Commission (PDPC)

Security and Resilience Division (SRD), Ministry of Communications and Information (MCI)

Ms Tan Xin Ying, CSA Intern

Contact Details

If you have any feedback on this publication, or wish to find out more about Singapore's efforts in cybersecurity, please visit the following websites or contact us:

Cyber Security Agency of Singapore
Website: www.csa.gov.sg
General enquiry/feedback:
contact@csa.gov.sg

If you wish to report a cybersecurity incident, please contact **SingCERT**.
Cyber Incident Reporting Form:
https://go.gov.sg/singcert-incident-reporting-form
Contact Email: singcert@csa.gov.sg

If you wish to seek scam-related advice, please contact **ScamAlert.**
Anti-scam Helpline:1800 722 6688
Website: www.scamalert.sg

CSA
SINGAPORE

www.csa.gov.sg