



Mitigating Cybercrime

Exploring solutions to help stakeholders combat these threats

Contents

Introduction	3
The current cybercrime landscape	4
Cybercrime as a Service	5
A Problem of Scale	5
The long-term consequences of major data breaches	7
Emerging technologies and cyber crime	8
Organizing to mitigate cybercrime	10
Contacts	11
Endnotes	12

Introduction

Long-term shifts in technology and threats to cyber security today permeate society. Some estimates put the cost of cybercrime at US\$8 trillion in 2023 – an amount equivalent to effectively the world’s third largest economy.¹ Cybercrime creates both challenges and opportunities for policy makers, law enforcement, the judiciary, and participants in the criminal justice ecosystem.

This paper will examine the state of cybercrime, its impact on criminal justice systems globally, and what can be done about it. Today’s increasingly sophisticated cyber threats stem in part from the rapid proliferation of Cybercrime-as-a-Service (CaaS), which has significantly lowered the barriers to entry for malicious cyber actors. The resultant frequency of major data breaches has long-term consequences for both victims and society that challenges justice systems. Yet there are many opportunities for stakeholders to help prevent and mitigate these threats. Global in scope, they require collaboration among policymakers, law enforcement agencies and cybersecurity professionals globally—and an ability to keep up with the speed and agility of cybercriminals.



The current cybercrime landscape: cybercrime and cyber-enabled crime

Cybercrime has been defined as a criminal undertaking in which individuals or groups orchestrate cyberattacks for malicious and/or financial gain. It is typically committed against individuals or businesses through mediums such as information and communications technology (ICT) and fall into one of two categories: cyber-dependent or cyber-enabled crime. In either case, the activities are attractive to criminals thanks to their mix of anonymity, which leads to a lower risk of detection, and potentially high returns.² What's more, rapid online advancements allow cybercriminals to exercise agile approaches in exploiting weaknesses in infrastructures, networks, and platforms.³

Cyber-enabled crime

Is traditional crime, such as theft, harassment, child exploitation or fraud, that can be committed without a computer but are enabled by a computer in certain circumstances.

Cyber-dependent crime

are offences carried out against computers and any other related devices that are in violation of laws, including hacking, ransomware, DDoS attacks and malware.

For law enforcement and cybersecurity professionals, responding to the cybercrime landscape is especially tricky, thanks to its constantly evolving nature. One of the key issues is the speed and agility of cybercriminals, who can adapt to new technologies swiftly. As a result, law enforcement professionals should be able to identify and react to cyberattacks expeditiously.⁴

Another challenge is the global reach of cybercriminals, who can operate from anywhere in the world and target victims in any location. That borderless capability makes it difficult both to prosecute these actors and recover stolen assets. As a result, international cooperation and collaboration among policymakers, law enforcement agencies and cybersecurity professionals⁵ are critical to detecting and prosecuting cybercriminals effectively. Doing so creates a foundational case for ongoing evaluation and harmonization of international legal frameworks and data sharing across borders.

Cybercriminals are also becoming more sophisticated in their work, rapidly developing new methods and techniques to evade detection and infiltrate systems. What's more, with the growing number of connected devices and the expansion of the Internet of Things (IoT), the scale of cyberattacks is also increasing. That means cybersecurity professionals must continually innovate and adapt to stay ahead of these evolving threats and engage in frequent upskilling to develop the greater technical understanding required to combat cybercrime⁶. Importantly, they should learn how to identify and respond to large-scale attacks that can impact multiple systems and organizations quickly.

Cybercrime as a Service: A Problem of Scale

Cybercrime-as-a-Service (CaaS) is a crime model where actors sell tools, knowledge, and services in the market. As the cybercrime ecosystem has matured, competitive pressure has forced threat actors to refine their value propositions. To that end, they're increasingly specializing in niches, selling those capabilities to other cybercriminals.⁷

Market Participants

Organized crime:



Organized crime groups, both traditional and cyber-oriented, use the CaaS market as customers to increase their cyber capabilities and as a place to sell their own CaaS offerings. For example, ransomware gangs will pay to use crime infrastructure hosting services as command-and-control centers to launch ransomware attacks. They will then sell data exfiltrated in these attacks on dark web markets.

Individual hackers:



They use CaaS offerings to increase their cyber capabilities. These actors range from experienced hackers purchasing high precision tools and services, to less sophisticated cybercriminals, such as “script kiddies”, who buy high-impact point-and-click cyber-attack tools.

Infrastructure operators:



CaaS infrastructure operators build and manage foundational platforms and technologies necessary to the ecosystem, charging a premium for their use. They also can act as intermediaries between buyer and seller, as well as building the money laundering and crypto tumbling services which are functional necessities in operating this market.

State-affiliated actors:



They offer hacking services and specialized skills to crime groups and ransomware crews. States also employ crime groups to execute cybercrime activities related to their interests.

The CaaS ecosystem is complex, with a variety of market participants, products, services, and enabling technologies. Core products and services range from malware tools to malicious botnets. For example:

- Ransomware malware phishing and exploit kits: The groups that develop and manage these highly effective and technical kits will sell the software to affiliate users who will then execute the software.^{8,9}
- Access brokers and credentials: Market participants sell device access and account credentials for valuable accounts. High-profile crime groups, such as the extortion gang Lapsus\$, are known to buy credentials to initiate their attacks.^{10,11}

- Crime infrastructure: such as command-and-control servers, are available to facilitate cyberattacks.^{12,13}
- Botnets: can be used by operators for a variety of purposes including Distributed Denial of Service (DDOS) attacks and malware installations.^{14,15}

There also are several key technologies underpinning the CaaS ecosystem. Cryptocurrencies, for example, are its core financial instrument. While bitcoin is the most widely adopted, privacy-friendly currencies, such as Monero, are also popular.^{16,17} 'Onion' servers, typically accessed through the Tor browser, enable cybercriminals to get into sites without revealing their own identities or learning any information about the hosting of the site.¹⁸ And encryption, which has also become widely accessible, scalable, and deployable enables actors to share secrets across a network. Without encryption, the CaaS ecosystem would not be able to function.¹⁹

The emergence of CaaS has also had another major effect: by providing access to a vast array of tools and services that would otherwise be beyond reach, it has substantially reduced the entry barrier for cyber criminals. As a result, the number of threat actors within the ecosystem has grown, with lower-skilled threat actors gaining access to once-inaccessible resources.²⁰

Network effects are an additional driver behind the growth of CaaS, with the success of one service provider creating a chain reaction that encourages the entry of more players into the market, leading to a wider range of services and tools on offer. As more actors enter the market, competition intensifies, which, in turn, drives innovation and improvement of services and increases the sophistication of cybercrime.²¹

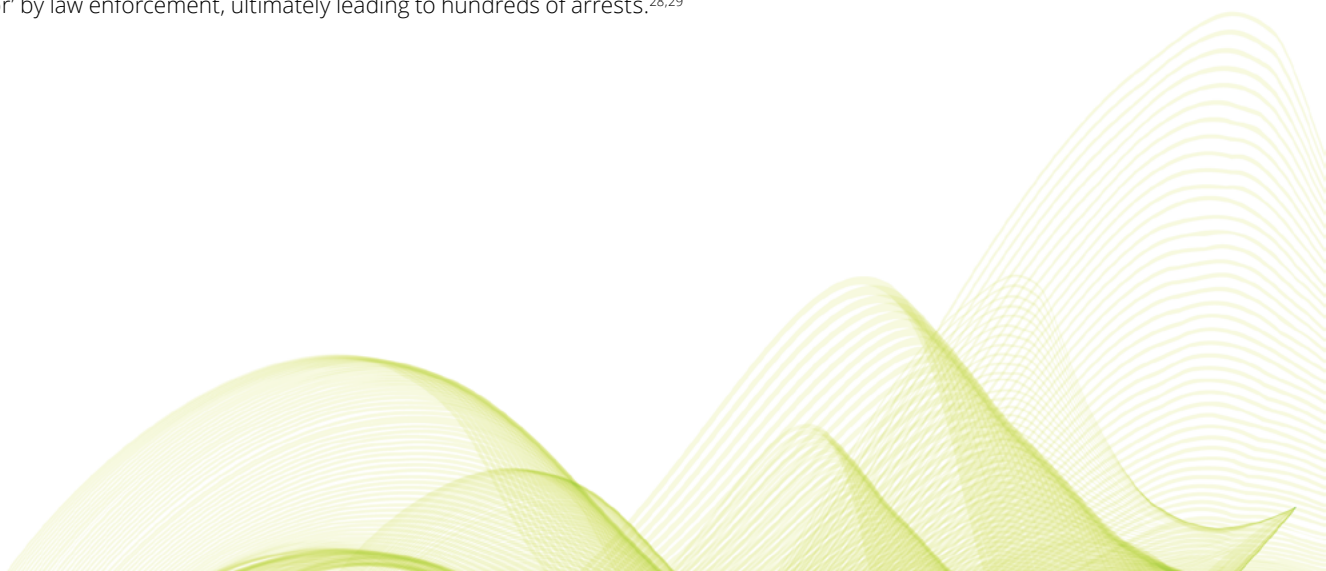
CaaS: Challenges and openings for criminal justice

The use of anonymous communication channels and encryption technologies poses a significant challenge for law enforcement in identifying and tracking cybercriminals involved in the CaaS ecosystem. Cybercriminals can conceal their identities and activities, allowing them to evade law enforcement efforts relatively easily.²² In addition, law enforcement, service providers, and platform owners may be in jurisdictions with varying laws and regulations, making it difficult to share intelligence and obtain evidence or legal recourse for victims of cyberattacks.²³

Another problem is the unequal access to technology that exists between law enforcement and cyber criminals. Cybercriminals often have access to sophisticated technology, while law enforcement agencies may lack the resources and expertise to respond to these threats effectively. The dynamic nature of the CaaS ecosystem, with new services and tools continuously being developed, can further exacerbate the challenges law enforcement bodies can face when trying to keep pace with evolving cyber criminality.²⁴ There's also the risk of unintended consequences: the process of investigating these crimes can lead to the potential disruption of legitimate businesses or violations of individuals' privacy rights.²⁵

At the same time, law enforcement can take advantage of multiple opportunities. The CaaS ecosystem relies on a degree of trust between market participants, who are often unaware of each other's real identities. This creates points of dislocation that law enforcement agencies can leverage to compromise and disrupt the market. In 2023, a multijurisdictional law enforcement operation dubbed "Operation Cookie Monster", saw the takedown of "Genesis", a prominent dark web market, leading to multiple arrests²⁶. Such law enforcement activity lowers the trust cybercriminals have in the ecosystem and raises the bar for their own operational security to prevent arrest.²⁷

The fragmented and anonymous nature of the CaaS ecosystem also gives law enforcement more openings to insert themselves into the market and gain intelligence about cyber criminals. For example, the ANOM communication service, branded as an end-to-end encrypted channel, was, in fact, built as an application 'backdoor' by law enforcement, ultimately leading to hundreds of arrests.^{28,29}



The long-term consequences of major data breaches

The incidence of major data breaches, where data is exposed inadvertently to, or accessed maliciously by, an unauthorized third party, is on an upswing. That trend highlights the inability for organizations to protect their systems and the sensitive data collected through their operations adequately.


The shift to the Cybercrime-as-a-Service (CaaS) model has law enforcement, companies, and individuals playing catch-up with a set of outdated frameworks that fail to capture the impacts of a major data breach and provide sufficient victim care. With organisations often short of skilled cyber professionals, the current approach of securing organizations and their data individually is often not scalable across industries and societies.

With little regulation in place regarding the capture and storage of long-term data, cybercrime operators are pivoting to extortion based on exfiltrated sensitive data, rather than infecting systems directly with malware. While many organizations previously relied on robust backup strategies and recovery plans, they are now often forced to deal with a new reality—risks associated with extortion when their systems are breached. That requires a greater understanding of the data they have stored and the potential impact of disclosure on their end users.

Organizations that fall victim to a major data breach can face multiple consequences, including reputational damage, financial loss, technical costs associated with business system outage and recovery, and potential payments to alleviate the threat of extortion³⁰. While these consequences are typically material and can impact the bottom line of the company, most of them are quantifiable and understood, with a finite lifespan in the public eye. Once a major breach occurs at another enterprise, the public spotlight shifts from one to the next organization, and the first one carries on with its operations with minimal public scrutiny.

But individual victims—those whose data was leaked during a major data breach—are left to deal with much longer lasting consequences. Their sensitive information, now in the hands of actors often outside the jurisdiction of applicable law enforcement agencies, can be used to commit identity or financial theft, perform fraudulent activity, or even perpetuate a cycle of revictimization. Often the most susceptible to these consequences are the most vulnerable organizations and individuals in society, who lack the means to protect themselves. What's more, while many governments have instituted notifiable data breach regulations³¹, determining the impact of a data breach is often subject to interpretation, with no standard for reporting or victim care.

In the face of the numerous challenges associated with major data breaches, however, there are steps that law enforcement, policymakers, and organizations can take to lessen the impact on the individuals whose data is compromised. They include:

- Modernizing the view of privacy obligations as they relate to the ethical collection, usage, and storage of data across government and industry.
 - Collaborating across borders to quantify the costs of data breaches, thereby contributing to increased recognition of the problem and attention to building cyber resilience at scale.
 - Adoption of privacy enhancing technologies (PETs) that allow governments and organizations to continue toward their goal of being data-driven, while protecting the individuals providing the underlying data.
 - Engaging in regulatory reform discussions, such as those related to the regulation of payments for ransomware and extortion attempts, and minimum cyber security framework compliance
 - Implementing more responsibilities for data collection, storage, and notification of breaches.
- 

Emerging technologies and cyber crime

There are multiple emerging cybersecurity technologies further complicating the cybercrime landscape. Artificial intelligence (AI) technologies can be used to coordinate more sophisticated attacks through the automatic collection of mass information to create highly convincing phishing email attacks and social media campaigns. AI can also be employed to create malware that mimics trusted system components.³²

Another instance is the increased use of Internet of Things (IoT) devices within society which continues to expand the attack surface of cybercrime, while the limited security of these devices, due to their small size and low processing power, makes them attractive targets.³³ The expansion of IoT integration beyond the home and into wider critical infrastructure sectors, such as healthcare and agriculture, paired with often-limited security, means that IoT-related compromise can have widespread, devastating effects.³⁴

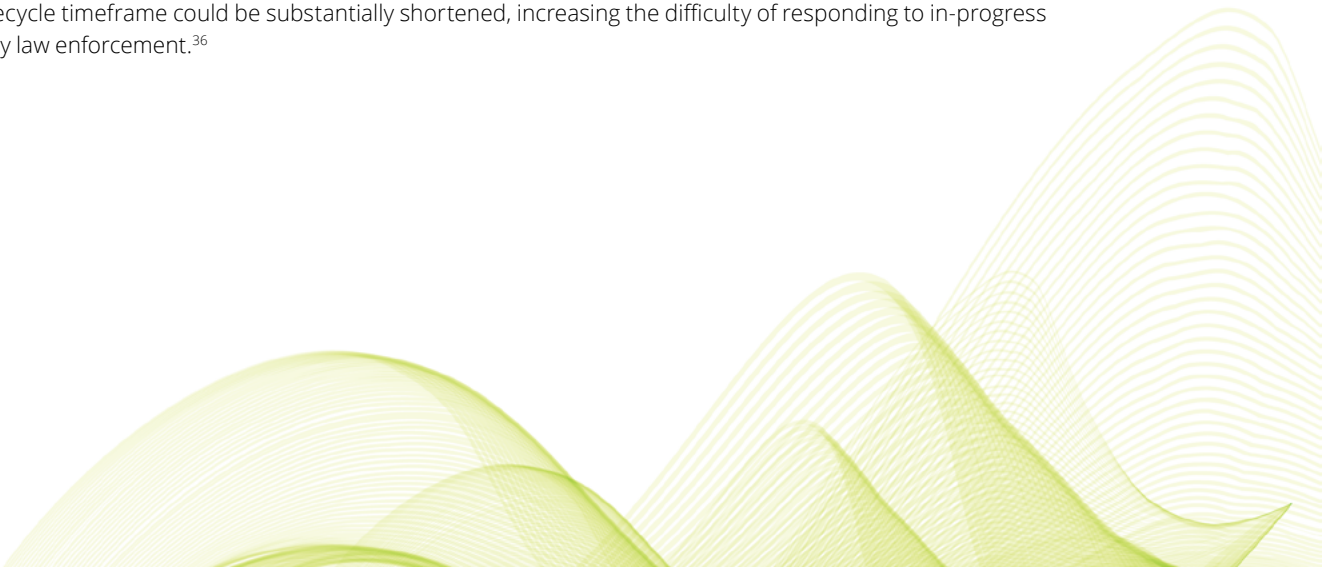
Also important is the matter of Operational Technology (OT) systems, which are core to the monitoring and control of industrial processes that underpin critical infrastructure (CI). They often have long in-service lifespans (some exceeding 30 years) and high uptime requirements, but are often based on dated technology, such as complex passwords, that constrain the retrofitting of modern cyber controls. There also are challenges in retaining sufficient workforce knowledge to recover or rebuild OT systems after critical incidents.

OT systems historically have been protected by isolation (i.e., “air-gaps”) as the main control mechanisms, but this model is under pressure as more mainstream technologies, such as IP networking and industrial IoT are adopted. The OT supply-chain can also present key risks in terms of the underlying hardware and software supply. Due to these supply chain issues; many systems have resorted to third-party support agreements with offshore vendors connecting to core systems to diagnose and support issues or maintenance of systems.

Ongoing OT vulnerabilities to ransomware and other criminal attack vectors risk the failure of CI, with an asymmetrical impact on the economy and essential services. Recent high-profile ransomware attacks on CI, such as those on critical utilities demonstrate how criminal actions intended to target one entity can have cascading impacts on society.

Other technologies, such as The Onion Router (Tor) and dark web “crypto markets”, allow users to anonymize their network traffic through layered encryption. As a result, engaging in malicious activities using such technologies can make it difficult—though still possible—for law enforcement to link cybercrimes to perpetrators.³⁵

As quantum computing continues to advance, the speed at which data can be decrypted is anticipated to increase exponentially. As a result, cyberattacks using quantum computers could facilitate significantly faster decryption of data on victims’ networks, greatly reducing the required duration of sustained access to target systems. Hence, the attack lifecycle timeframe could be substantially shortened, increasing the difficulty of responding to in-progress attacks by law enforcement.³⁶



Challenges for policymakers

Technological advancements present a major challenge for policymakers trying to keep up with the changing cybercrime landscape. With that in mind, legislation should adapt to address³⁷:

- Data privacy implications associated with the ever-increasing scale of data generation, handling and storage associated with big data.
- Intellectual property and impersonation issues related to AI.
- Required security of IoT devices at the point of manufacturing and manufacturer's liability.

The most vulnerable members of society will likely continue to be those experiencing the greatest impacts of these emerging cybercrime trends. To respond, the justice system should develop measures to advise and protect this population, which includes victims of domestic violence, those in witness protection programs, and those with lower levels of digital literacy.



Organizing to mitigate cybercrime

The seismic shift in technology indicates wholesale changes in approach, policy, technology, and relationships. Central to these efforts is the role of industry—specifically, its participation in new public-private collaborations that recognize cybersecurity as a fundamental building block for mitigating cyber-threats across the economy globally.

By sharing lessons learned from previous cyber programs and security technologies, stakeholders can develop critical necessities—new technologies, policies, and initiatives with security built-in at their cores. This will also provide industry with market differentiation opportunities. With that in mind, governments should set minimum open standards, to enable intelligence sharing globally.

Industry-led consortiums represent a strong model for threat blocking. To evolve and meet the challenges of speed and scale, these initiatives should interoperate in a common national, and even cross-jurisdictional, ecosystem. Crime prevention can also be tackled by sectoral collaboration. Where limited resources exist, efforts can be scaled through alliances with industry subject matter experts, law enforcement, and incident response teams.

Sectoral Information Sharing and Analysis Centers (ISACs) represent another compelling next generation of cybersecurity resilience. That applies to sectors where there is the potential to augment existing sectoral initiatives, as well as share insights that can drive preventative and timely incident response activities.³⁸

Working in collaboration, industry and government can also advance privacy enhancing technologies. With identity theft on the rise, customers are increasingly wary about the use of their personally identifiable information (PII). In response, initiatives are underway across the globe to find protective solutions.³⁹ Also, government and private industry can adopt Privacy Enhancing Technologies (PETs) at scale. The key goal: allowing government and businesses to extract value from data without exposing the underlying information itself.

Cyber awareness

Society comprises people with widely varying degrees of cyber literacy. While building public awareness is important, not all organizations or institutions are funded or structured to perform resource-intensive cyber tasks (e.g., risk assessments and incident response) in-house, or educate their stakeholders. A crucial first step is implementing basic cyber practices in schools so they can undertake the fundamental actions to protect themselves from various cyber threats and enhance their overall cybersecurity postures.

Sustainably growing the cyber professional pool requires a long-term curriculum planning approach. Integrating cybersecurity topics throughout the broader education lifecycle, as opposed to offering them as standalone tertiary disciplines or programs, could support broader cyber hygiene awareness and contribute to a stronger pipeline of future cyber-proficient professionals.

Managed cyber services, delivered by industry or government, can be critical to unlocking efficiencies in resource-constrained cyber workforces. These services can include workforce training, cyber threat sharing and blocking, attack surface management, and incident response and sharing. Sustained investments in these services could be critical to their successes.

Ultimately, policy makers, law enforcement professionals, and others in the broader criminal justice ecosystem face multiple challenges fighting increasingly sophisticated cybercriminals. But there are many opportunities available to mitigate these crimes and prevent them from happening in the first place.

Contacts



Beth McGrath

Global Government &
Public Services Leader
Deloitte Global

bmcgrath@deloitte.com



Andrew Colvin

Partner
Deloitte Australia
ancolvin@deloitte.com.au



Sean Choi

Principal
Deloitte Australia
seanchoi@deloitte.com.au



Matt Burgess

Senior Manager
Deloitte Australia
mburgess@deloitte.com.au



Karlee Jackson

Senior Manager
Deloitte Australia
karleejackson@deloitte.com.au

Endnotes

1. Esentire (2022). 2022 Official Cyber Crime Report. Retrieved from <https://www.esentire.com/resources/library/2022-official-cybercrime-report#:~:text=According%20to%20Cybersecurity%20Ventures%2C%20the%20global%20annual%20cost,is%20expected%20to%20reach%20%2410.5%20trillion%20by%202025.>
2. ACSC. (2021). Retrieved from: ACSC Annual Cyber Threat Report, July 2021 to June 2022 | Cyber.gov.au
3. Department of Foreign Affairs and Trade. (2021). Retrieved from: Cybercrime | Australia's International Cyber and Critical Tech Engagement (internationalcybertech.gov.au)
4. Gartner. (2021). Top 5 Security and Risk Management Trends. Retrieved from <https://www.gartner.com/smarterwithgartner/top-5-security-and-risk-management-trends/>
5. Interpol. (2021). Cybercrime. Retrieved from <https://www.interpol.int/en/Crimes/Cybercrime>
6. Ibid.
7. <https://cybernews.com/security/crimeware-as-a-service-model-is-sweeping-over-the-cybercrime-world/>
8. MIT, op.cit.
9. United States Government Accountability Office. (2020). Public and Private Entities Face Challenges in Addressing Cyber Threats: <https://www.gao.gov/products/gao-07-705>
10. MIT, op.cit.
11. United States Government Accountability Office, op. cit.
12. MIT, op. cit.
13. United States Government Accountability Office, op. cit.
14. MIT, op. cit.
15. United States Government Accountability Office, op. cit.
16. Ibid.
17. Office of the Director of National Intelligence. (2020). Annual Threat Assessment of the US Intelligence Community <https://www.dni.gov/index.php/newsroom/reports-publications/reports-publications-2022/item/2279-2022-annual-threat-assessment-of-the-u-s-intelligence-community>
18. Ibid.
19. Cybercrime investigation and the protection of personal data and privacy retrieved from <https://rm.coe.int/16802fa3a3>
20. Zdnet (2017). Low-cost tools making cybercrime more accessible Retrieved from <https://www.zdnet.com/article/low-cost-tools-making-cybercrime-more-accessible-secureworks/>
21. Australia in the grip of cybercrime-as-a-service <https://www.afr.com/policy/foreign-affairs/australia-in-the-grip-of-cybercrime-as-a-service-20221112-p5bxbpm>
22. INTERNET ORGANISED CRIME THREAT ASSESSMENT (IOCTA) 2020: <https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment-iocta-2020>
23. United States Government Accountability Office, op. cit.

24. Office of the Director of National Intelligence. (2020). Annual Threat Assessment of the US Intelligence Community <https://www.dni.gov/index.php/newsroom/reports-publications/reports-publications-2022/item/2279-2022-annual-threat-assessment-of-the-u-s-intelligence-community>
25. Cybercrime investigation and the protection of personal data and privacy retrieved from <https://rm.coe.int/16802fa3a3>
26. Krebs on Security (2023). FBI Seizes Bot Shop 'Genesis Market' Amid Arrests Targeting Operators, Suppliers. Retrieved from <https://krebsonsecurity.com/2023/04/fbi-seizes-bot-shop-genesis-market-amid-arrests-targeting-operators-suppliers/>
27. MIT, op. cit.
28. Ibid.
29. New York Times (2021). The Criminals Thought the Devices Were Secure. But the Seller Was the F.B.I.. Retrieved from <https://www.nytimes.com/2021/06/08/world/australia/operation-trojan-horse-anom.html>
30. <https://www.mauriceblackburn.com.au/class-actions/join-a-class-action/optus-data-breach-2022/>
31. <https://www.oaic.gov.au/privacy/notifiable-data-breaches/about-the-notifiable-data-breaches-scheme>
32. Deloitte 2021, "Defending against ransomware in emerging technology", p. 2, <https://www2.deloitte.com/content/dam/Deloitte/us/Documents/risk/us-defending-against-ransomware.pdf>
33. Ibid.
34. IoT Alliance Australia 2017, "Internet of Things Security Guideline", <https://www.iot.org.au/wp/wp-content/uploads/2016/12/IoTAA-Security-Guideline-V1.2.pdf>
35. Australia Parliamentary report on the Dark Web: https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Law_Enforcement/NewandemergingICT/Report/c03
36. Deloitte, Ibid.
37. Australia Parliamentary report on Operational challenges and vulnerabilities: https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Law_Enforcement/NewandemergingICT/Report/c05
38. Deloitte (2022) Information Sharing and Analysis Centres (ISACs) The next generation of security resilience for Australian industry <https://www2.deloitte.com/content/dam/Deloitte/au/Documents/risk/deloitte-au-risk-information-sharing-analysis-centres-isac-deloitte-paper-160223.pdf>
39. World Economic Forum (2019) The Next Generation of Data-Sharing in Financial Services: Using Privacy Enhancing Techniques to Unlock New Value September 2019 Prepared in collaboration with Deloitte https://www3.weforum.org/docs/WEF_Next_Gen_Data_Sharing_Financial_Services.pdf



Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited ("DTTL"), its global network of member firms, and their related entities (collectively, the "Deloitte organization"). DTTL (also referred to as "Deloitte Global") and each of its member firms and related entities are legally separate and independent entities, which cannot obligate or bind each other in respect of third parties. DTTL and each DTTL member firm and related entity is liable only for its own acts and omissions, and not those of each other. DTTL does not provide services to clients. Please see www.deloitte.com/about to learn more.

Deloitte provides industry-leading audit and assurance, tax and legal, consulting, financial advisory, and risk advisory services to nearly 90% of the Fortune Global 500® and thousands of private companies. Our professionals deliver measurable and lasting results that help reinforce public trust in capital markets, enable clients to transform and thrive, and lead the way toward a stronger economy, a more equitable society, and a sustainable world. Building on its 175-plus year history, Deloitte spans more than 150 countries and territories. Learn how Deloitte's approximately 415,000 people worldwide make an impact that matters at www.deloitte.com.

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited ("DTTL"), its global network of member firms or their related entities (collectively, the "Deloitte organization") is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser.

No representations, warranties or undertakings (express or implied) are given as to the accuracy or completeness of the information in this communication, and none of DTTL, its member firms, related entities, employees or agents shall be liable or responsible for any loss or damage whatsoever arising directly or indirectly in connection with any person relying on this communication. DTTL and each of its member firms, and the unrelated entities, are legally separate and independent entities.

©2024. For information, contact Deloitte Global