

Research Project

- By Sri Pemmireddy

Cyber situation awareness for incident response in Organizations:

Introduction

Cybersecurity is one of the most complex technological issues, and it is essential to understand today's challenges and those we will face in the future. The cyber threat to an organization's critical infrastructure and sensitive information continues to grow and represents one of the most modern severe security challenges we must confront. Organized, sophisticated and persistent cyber-threat-actors pose a significant challenge to large, high-value organizations. Cyber security and cyber situational awareness (CSA) are critical influences protecting an organization's critical infrastructure and data. The CSA has become the focal point and is a critical influence in proactive cyber risk management to help organizations to detect and mitigate cyber-attacks and swiftly respond to cyber incidents in the constantly changing cyber-threat landscape.

Background

An average of 164 cybercrime reports are made by Australians every day - about one report every 10 minutes - according to the Australian Cyber Security Centre (ACSC). The ACSC saw 67,500 cybercrimes reported in Australia last financial year, a 13% increase. This cost Australian businesses \$33 billion dollars, and the cause of the majority of these breaches human errors. Cyberattacks continue to be prevalent irrespective of the size of the organizations. Whilst the security and IT systems while IT security teams are getting better at preventing cyber-attacks from happening, attacks remain a matter of "when" one will occur (if it has not already) rather than "if" it will happen. A business disruption caused by cyberattacks corrupting an organization's critical configuration of their systems can damage its financial well-being and reputation as data theft or complete IT outage.

The PwC digital trust insights survey examined views of 3600 plus CEOs and C-suite senior leadership globally, including Australia. It is a severe concern where more than 60% of organizations in Australia anticipate a potential increase in organized, targeted cybercrimes. Around 72% of chief executive officers (CEOs) and C-suite senior leadership teams in Australian enterprises anticipate an increase in cyber incidents in 2022, which is expected to grow in the coming days. However, only 33% have adequately assessed their organization's exposure to this risk and cyber recovery readiness.

Definition of cyber situational awareness (CSA)

In cybersecurity, comprehending the current status and security posture with respect to availability, confidentiality, and integrity of networks, systems, users, and data, as well as projecting future states of these.

The importance of cyber security situational awareness

Cybersecurity is one of the most complex technological issues, and it is essential to understand today's challenges and those we will face in the future. Cyber security situation awareness has become the focal point of businesses worldwide. In this constantly changing cyber landscape, securing, and protecting critical infrastructure and data against cyber threats has become the biggest challenge in the modern digital era and is far-reaching.

The cyber threat to organizations critical infrastructure and data

The Cyber threat to organizations' critical infrastructure and data continues to grow and represents one of the most modern severe security challenges we must confront. Cyberattacks continue to be prevalent irrespective of the size of the organizations. Mainly Organized, sophisticated and persistent cyber-threat-actors pose a significant challenge to large, high-value organizations. Cyber security and cyber situational awareness (CSA) are critical influences in protecting an organization's critical infrastructure and data.

Notifiable data breaches report - January to June 2022 - The Office of the Australian Information Commissioner (OAIC)

- Top 5 sectors to notify data breaches
- 65% of data breaches affected 100 people or fewer
- Sources of data breaches
- 41% of all data breaches resulted from cyber security incidents (162 notifications)

Cyber-attacks are daily headlines in every market and industry

In Australia, we also saw an increase in the number and sophistication of cyber threats, making crimes like extortion, espionage, and fraud easier to replicate at a greater scale.

The following examples are the recent cyber-attacks on Australia's leading enterprises. Cybercriminals target organization's critical infrastructure and sensitive information.

Optus notifies customers of cyberattack compromising customer information

22 September 2022

Please Note: Latest updates & support on the cyberattack here.

Following a cyberattack, Optus is investigating the possible unauthorised access of current and former customers' information. Upon discovering this, Optus immediately shut down the attack. Optus is working with the Australian Cyber Security Centre to mitigate any risks to customers. Optus has also notified the Australian Federal Police, the Office of the Australian Information Commissioner and key regulators.

"We are devastated to discover that we have been subject to a cyberattack that has resulted in the disclosure of our customers' personal information to someone who shouldn't see it," said Kelly Bayer-Rosmont, Optus CEO.

"As soon as we knew we took action to block the attack and began an immediate investigation. While not everyone maybe affected and our investigation is not yet complete, we want all of our customers to be aware of what has happened as soon as possible so that they can increase their vigilance. We are very sorry and understand customers will be concerned. Please be assured that we are working hard, and engaging with all the relevant authorities and organisations, to help safeguard our customers as much as possible."

Information which may have been exposed includes customers' names, dates of birth, phone numbers, email addresses, and, for a subset of customers, addresses, ID document numbers such as driver's licence or passport numbers. Payment detail and account passwords have not been compromised.

Optus services, including mobile and home internet, are not affected, and messages and voice calls have not been compromised. Optus services remain safe to use and operate as per normal.

"Optus has also notified key financial institutions about this matter. While we are not aware of customers having suffered any harm, we encourage customers to have heightened awareness across their accounts, including looking out for unusual or fraudulent activity and any notifications which seem odd or suspicious."

To help protect against fraud, customers are encouraged to look to reputable sources such as:

- moneysmart.gov.au/banking/identity-theft
- [Identity fraud - Home \(odc.gov.au\)](https://identity.fraud - Home (odc.gov.au))

For customers believed to have heightened risk, Optus will undertake proactive personal notifications and offer expert third-party monitoring services.

The rest up to date information will be available via optus.com.au. For customers who have specific concerns, they can contact Optus via the My Optus App (which remains the safest way to interact with Optus) or by calling 133 337. Optus will not be sending links to any emails or SMS messages.

Source: OPTUS, September 2022

medibank

ASX release

13 October 2022

Medibank cyber incident

Yesterday the Medibank Group detected unusual activity on its network.

In response to this event, Medibank took immediate steps to contain the incident, and engaged specialised cyber security firms.

At this stage there is no evidence that any sensitive data, including customer data, has been accessed.

As part of our response to this incident, Medibank will be isolating and removing access to some customer-facing systems to reduce the likelihood of damage to systems or data loss.

As a result our ahm and international student policy management systems have been taken offline. We expect these systems to be offline for most of the day.

This will cause regrettable disruptions for some of our customers. ahm and international student customers will still be able to contact our customer teams via phone but at this stage our people won't be able to access policy information.

Source: Medibank, October 2022

Hacked again: Toll Group systems hit by fresh ransomware attack


Logistics giant Toll Group says it suffered a second major cyber attack this year, revealing it has closed numerous internal and customer-facing systems after being infected by a new form of ransomware.

The company faced over a month of costly disruptions to its operations earlier this year when its systems were [compromised by Russia based hackers](#), who unsuccessfully sought a hefty ransom to unlock Toll's systems.

May 9, 2020 - 4:50pm

Paul Smith
Technology editor

Save Share



Toll Group is fighting to get systems back online after a second cyber attack this year. [Wikt Lewczak](#)

Source: Australian Financial Review, May 2020

International car sales firm hit with \$30m cyber ransom

Another company crippled by ransomware.

By Denham Sadler on Mar 12 2020 10:25 AM

Print article

Tweet In Share

A major car auction company has been hit by a malware attack that has locked its computer networks, with the hackers demanding a \$30 million ransom.

The Australian branch of Manheim Auctions, which runs car auctions online and in person, was the subject of a cyber attack last month that locked staff out of its computer system, forcing it to stop trading for several weeks.

Earlier, the firm revealed it had been the subject of a cyber attack but the full extent was not revealed until a statement from Western Australia Consumer Protection this week, which confirmed the cyber criminals were demanding a \$30 million payment for access to Manheim Auctions' computer network to be restored.

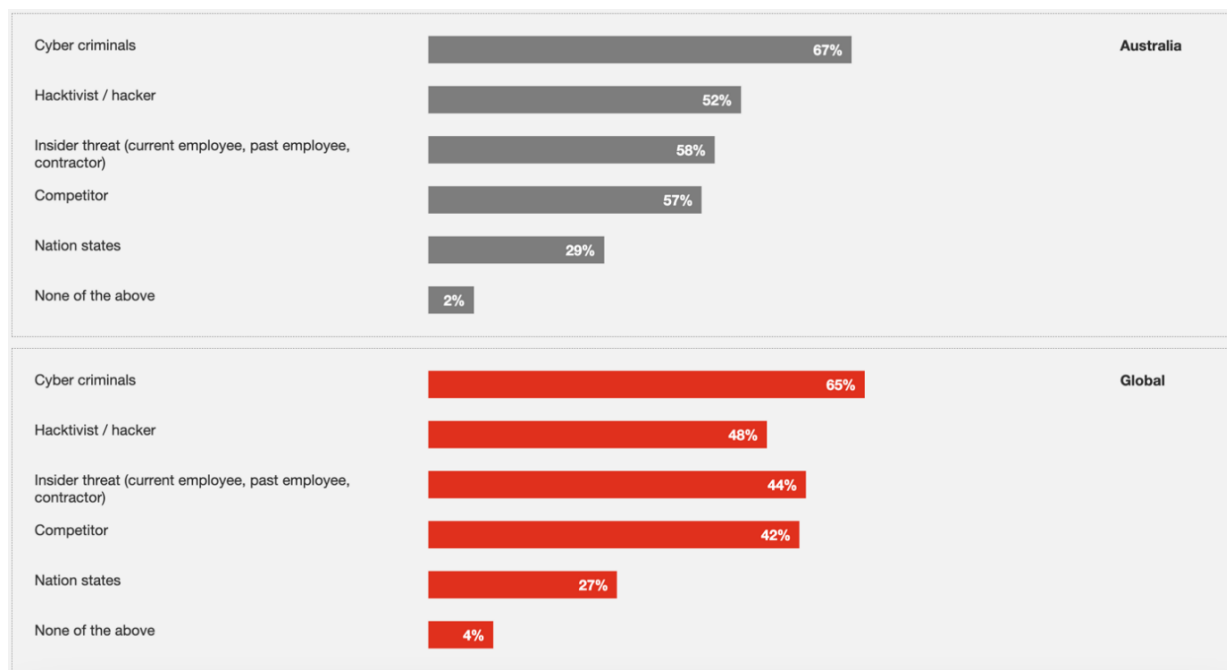


Source: Australian Financial Review, May 2020

Threat actors

The top two cyber threat actors expected to impact Australian organizations significantly were *cyber criminals* and *insider threats*. Nowadays, ransomware attacks have evolved to be highly targeted attacks and have spread through systems with unpatched vulnerabilities, including an organization's critical infrastructure and data systems. Globally, digital transformation enables businesses and their invocations how the business expands and operates. Especially during this global pandemic, we connect, and then we work changed, the IT systems that underpin every day and the way we view security.

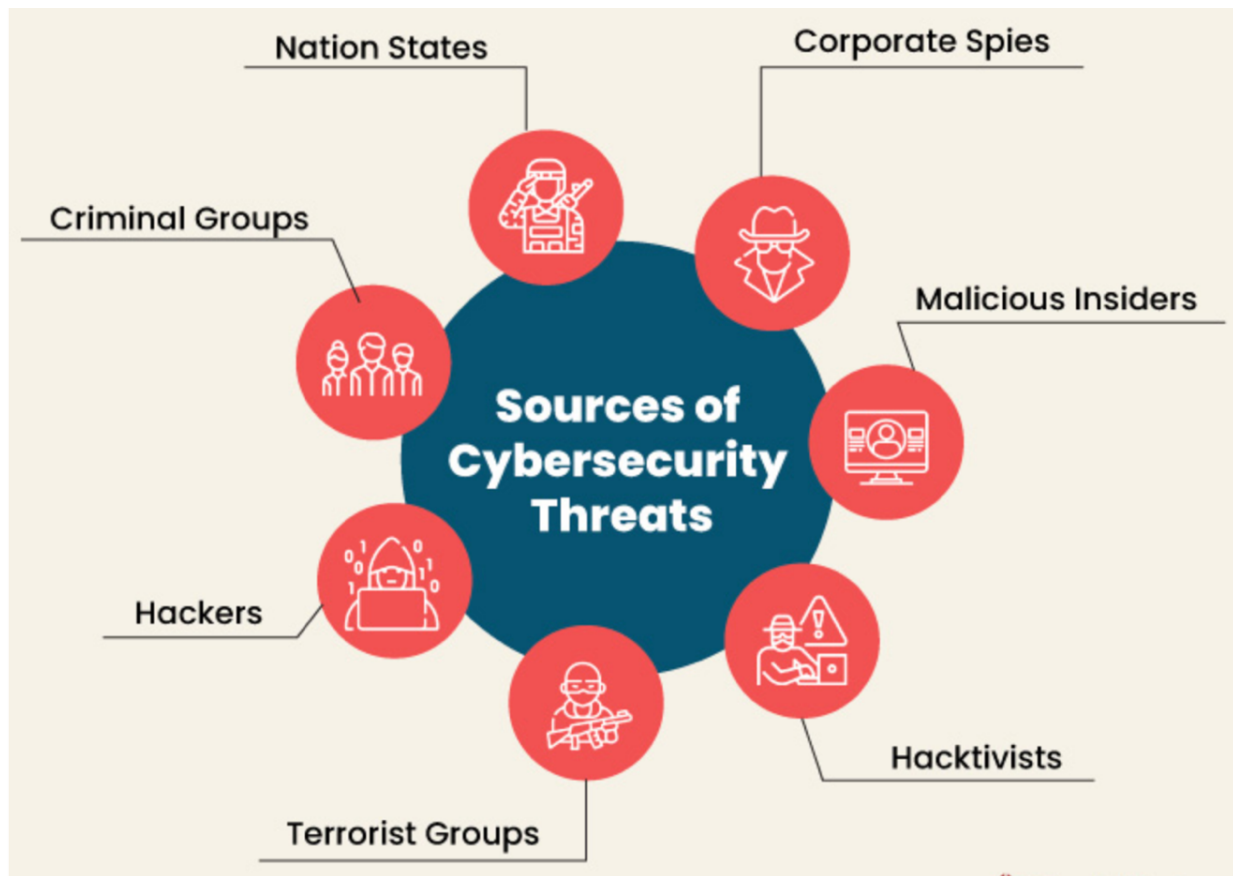
Cybersecurity is the most important and central for all organizations to securely operate and protect critical information assets. Therefore, enterprises worldwide, mainly in Australia, have been constantly exposed to cyber threats due to the increased digitization leveraging public cloud technologies. Under the shared responsibility model, customers are responsible for configuring and managing their respective services and resources properly. Therefore, protecting an organization's IT assets and data is the most crucial demand among the stakeholders Australia's 2023 Global Digital Trust Insights Survey finding reflects that the organization's leadership have placed their cyber security and protection of organization critical information from cyber threats as the top priority. The following figure provides insights into how disparate cyber threat actors significantly affect organizations globally and within Australia. Cyber threat actors expect to significantly affect organization in 2023 compared to 2022. Which is expected to be around 67% in 2023



Evolution of cyber threat actors and motive

Due to evolving and constantly changing cyber-threat landscape, new cyber threats, and new strains of malware threats, including ransomware, are on the rise. Organization's critical data and infrastructure are continually at risk even though considerable cyber risk assessment and mitigation strategies have been deployed. It is vital that organizations practice CSA to protect and recover, including ability and capabilities, and are kept operational and ready for a rapid response to incidents.

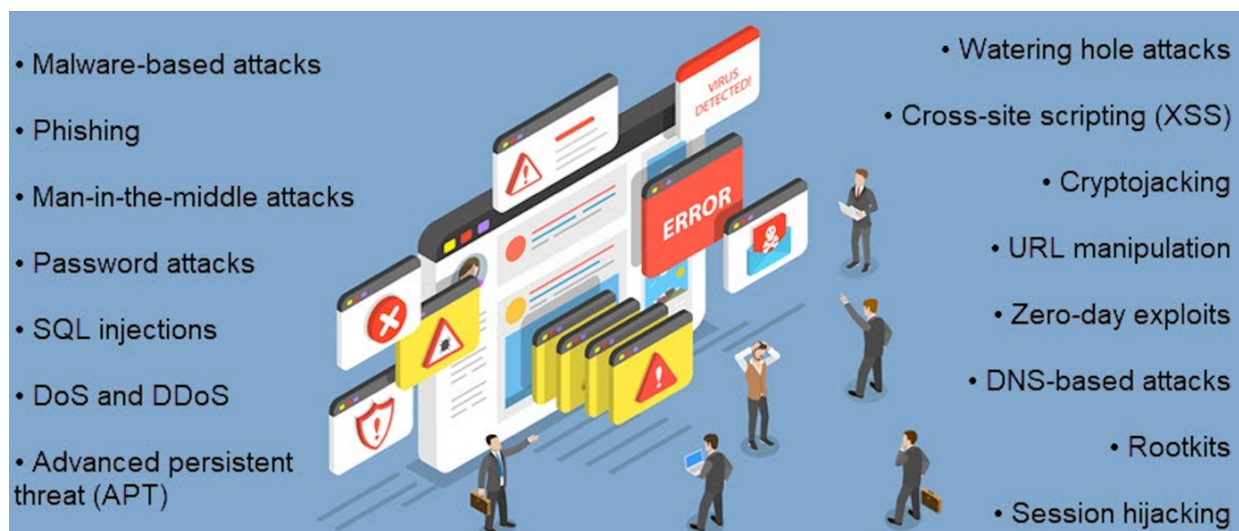
We must understand the constantly changing cyber threat landscape, its origins, types, and evolution and how CSA plays a vital role in developing and practicing CSA for a rapid response to incidents. To respond effectively to a cyberattack, it is crucial to know the threat actors and understand their tactics, techniques, and procedures.



- Personal gain
- Personal challenge
- Form of vandalism
- Theft & extortion for financial gain
- Trusted insiders steal or extort for personal, financial, & ideological reasons. Increasingly targeted because of privileged access to systems
- Corporate or Nation-state actors steal valuable data
- Advance political or social causes
- Sabotage & destruction to instill fear
- Nation-state actors with destructive cyber weapons (Not Petya)

Common types of cyber threats

	Cyber threat type	Description
1	Data theft or data exfiltration	Or data exfiltration, an offender gains access to files or data with sensitive information such as personal identifiable information (PII), credit card numbers, bank account information, health records, and social security numbers.
2	Malicious insiders	Malicious insiders can be employees, former employees, contractors, or business associates who have legitimate access to your systems and data, but use that access to destroy data, steal data, or sabotage your systems. It does not include well-meaning staff who accidentally put your cyber security at risk or spill data.
3	Distributed Denial of service attack	(DDoS) Make an online service unavailable by overwhelming it with excessive traffic from many locations and sources.
4	Malware	Also known as malicious code or malicious software. Malware is a program inserted into a system to compromise data confidentiality, integrity, or availability. It is done secretly and can affect your data, applications, or operating system.
5	Phishing	A form of social engineering, including attempts to get sensitive information. Phishing attempts will appear to be from a trustworthy person or business.
6	Ransomware	Prevents or limits users from accessing their system via malware. Ransomware asks you to pay a ransom using online payment methods to regain your system or data access.
7	Viruses and Worms	A piece of malicious code that is installed without the user's knowledge. Viruses can replicate and spread to other computers by attaching themselves to other computer files. Worms are like viruses in that they are self-replicating. However, they do not need to attach themselves to another program to do so.
8	Zero-Day Exploit	Is the method hackers use to attack systems with a previously unknown vulnerability.



How can we prevent cyber attacks?

The top two cyber threat actors expected to impact Australian organizations significantly were cyber criminals and insider threats. Nowadays, ransomware attacks have evolved to be highly targeted attacks and have spread through systems with unpatched vulnerabilities, including an organization's critical infrastructure and data systems.

- Define framework and general principles to improve and practice CSA

- Employing ACSC E8, NIST and other industry standards to build maturity and capability models
- Ransomware protection
- Cyber recovery
- End-user trainings
- Edge security posture and protection
- Client antivirus, anti malware, and firewalls
- Operating system (OS) patches
- Identity and key management
- Security Operations (SOC) and CERT
- Review incident response plan including RACI matrix
- Assess and mitigate cyber security risks
- Isolate, lock, and harden data from changes
- Monitor and find anomalous threats
- Threat and fraud intelligence
- Threat and vulnerability management
- Security defects and security testing, leveraging emerging technologies and tools
- Analyze data and automate actions
- Data and service recovery from a complete service loss scenario

AWS and Compliance

AWS compliance empowers customers to understand the robust controls in place at AWS to maintain security and data protection in the AWS cloud. AWS's approach in security and data protection is not only proven, but it enables continuous compliance controls across the entire AWS Cloud. AWS services are in compliance with GDPR and additionally SOC 1/SSAE 16/ISAE 3402 (formerly SAS 70), SOC 2, SOC 3, ISO 9001 / ISO 27001, FedRAMP, DoD SRG, and PCI DSS Level 1 certifications are continuously audited in AWS computing environments. Amazon also has assurance programs that provide templates and control mappings for customers to achieve compliance in their AWS-hosted environments. Finally, resources such as whitepapers, reports, accreditation, certifications, and third-party attestations are available for customers to learn more about compliance controls and implement them.

AWS Cloud Security Best Practices

Cloud security at AWS is the highest priority, the security of AWS cloud depends on how the customer configure and manage it. Here are some of the most important best practices that customers can follow to ensure the security of your data in the AWS cloud:

Understand Customer Responsibilities

While AWS provides a plenitude of security tools to secure customer cloud environment, it follows the shared responsibility model when it comes to security. Under this model, AWS is responsible for the security of the cloud infrastructure and its customers are responsible for configuring and managing their respective AWS services and resources properly. Essentially meaning that Amazon is responsible for the security of the cloud and customers are responsible for security in the cloud.

Encryption and Backups

Data encryption is key to maintaining security in the cloud. By default, AWS offers AES256 encryption for all data stored in the Amazon S3 buckets. In addition, customers can take advantage of Amazon Key Management Service to create your own encryption keys and encrypt your data.

Backup cloud data in multiple copies and 2 different locations, one of which is in a different physical location - either a different service or a different region. Also ensure that keep one of the backups is on a cloud service other than AWS.

Implement Strong Cloud Security Controls

Include strong cloud security controls in security strategy. This includes clearly defining user roles, conducting regular privilege audits and implementing privilege access control that means removing privileges when the user no longer needs them, implementing a strong password policy, and multi-factor authentication and permission time-outs.

Leverage AWS Security Tools

It is advised to use the AWS Advisor tool that helps customers to identify potential security vulnerabilities and provides recommendations for mitigating them. It provides recommendations for improving system performance and optimizing your infrastructure in accordance with AWS standards. In addition, customers can use built-in AWS security tools such as Amazon CloudFront, AWS Shield, Guard Duty, and Cloud Watch that can assist you in securing your cloud environment.

Test Infrastructure Regularly

Regularly carry out security assessments and penetration tests against AWS infrastructure to ensure that the security controls are effective and also to identify vulnerabilities or potential weaknesses.

Use a Cloud-Native Security Solution

To fulfill the compliance and requirements of the cloud, use a cloud native security solution that can provide the visibility and controls that are required to secure cloud infrastructure. Cloud-native solutions enable continuous delivery, and protect customer data from external threats. Moreover, some of them also help you with meeting compliance requirements.

Integrate Customer Security Products

Customers can use numerous tools that are available within AWS and third-party providers to secure the cloud data. Some tools will present their findings in their own formats. Security Hub uses a unified format to integrate and present findings from various tools, eliminating the need for security teams to do so.

Keep AWS Security Best Practices Up to Date

As a leader in cloud computing, AWS is constantly improving its cloud infrastructure and security services to better serve its customers. Stay informed about the latest security updates and keep updating your AWS security best practices and store these policies on a shared drive accessible by all of your users so that everyone is on the same page. Customer can patch their AWS servers using a variety of third-party tools. They can also use AWS Systems Manager Patch Manager, which allows automates the process of patching managed nodes with both security related and other types of updates.

References:

- [1] A. Ahmad, S. B. Maynard, K. C. Desouza, J. Kotsias, M. T. Whitty, and R. L. Baskerville, "How can organizations develop situation awareness for incident response: A case study of management practice," *Computers & Security*, vol. 101, p. 102122, 2021/02/01/ 2021, doi: <https://doi.org/10.1016/j.cose.2020.102122>.
- [2] U. Franke and J. Brynielsson, "Cyber situational awareness - A systematic review of the literature," (in English), *Comput Secur, Review* vol. 46, pp. 18-31, 2014, doi: 10.1016/j.cose.2014.06.008.
- [3] M. R. Endsley, Toward a theory of situation awareness in dynamic systems, *Human Factors* (32-64). March, 1995.
- [4] A. Evesti, T. Kanstrén, and T. Frantti, "Cybersecurity situational awareness taxonomy," in 2017 International Conference On Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA), 19-20 June 2017 2017, pp. 1-8, doi: 10.1109/CyberSA.2017.8073386.
- [5] H. Tianfield, "Cyber Security Situational Awareness," in 2016 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), 15-18 Dec. 2016 2016, pp. 782-787, doi: 10.1109/iThings-GreenCom-CPSCom-SmartData.2016.165.
- [6] S. Varga, J. Brynielsson, and U. Franke, "Information requirements for national level cyber situational awareness," presented at the Proceedings of the 2018 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining, Barcelona, Spain, 2020.
- [7] (2022). Annual Cyber Threat Report. [Online] Available: <https://www.cyber.gov.au/>
- [8] Commvault, "IT Security – Cyber Threats " 2022. [Online]. Available: <https://www.commvault.com/it-security>.
- [9] p.-P. D. T. I. Survey. "Business complexity and supply chain cyber risks, a magnet for security breaches - PwC Digital Trust Insights Survey." (accessed).
- [10] K. M, H. S, H. M, and O. A, "Exploring the Dark Web for Cyber Threat Intelligence using Machine Learning," in 2019 IEEE International Conference on Intelligence and Security Informatics (ISI), 1-3 July 2019 2019, pp. 200-202, doi: 10.1109/ISI.2019.8823360.
- [11] R. Crethar, "Cybersecurity risks outrank COVID-19 as Australia's top threat to business growth in PwC Australia's 25th CEO Survey," <https://www.pwc.com.au/ceo-agenda/ceo-survey/cyber-top-risk-to-business-growth.html>, 2022. [Online]. Available: <https://www.pwc.com.au/ceo-agenda/ceo-survey/cyber-top-risk-to-business-growth.html>.
- [12] K. Denney et al., "A Novel Approach to Cyber Situational Awareness in Embedded Systems," 2021: Institute of Electrical and Electronics Engineers Inc., doi: 10.1109/HPEC49654.2021.9622800. [Online]. Available: <https://www.scopus.com/inward/record.uri?eid=2-s2.0-85123480103&doi=10.1109%2fHPEC49654.2021.9622800&partnerID=40&md5=a246757f21d2269a0d90bd397683b1a0>
- [13] E.-i.-C. Morgan. (Oct. 21, 2019) Global Ransomware Damage Costs Predicted To Reach \$20 Billion (USD) By 2021. *Cyber Magazine*.
- [14] Anupama Mukherjee, AWS security best practices you need to know, Blog on Threat Intelligence, <https://www.threatintelligence.com/blog/aws-cloud-security>
- [15] R. Gutzwiller, J. Dykstra, and B. Payne, "Gaps and Opportunities in Situational Awareness for Cybersecurity," *Digital Threats*, vol. 1, no. 3, p. Article 18, 2020, doi: 10.1145/3384471.
- [16] M. Bada and J. R. C. Nurse, "Profiling the Cybercriminal: A Systematic Review of Research," 2021: Institute of

Electrical and Electronics Engineers Inc., doi: 10.1109/CyberSA52016.2021.9478246. [Online].

Available: [https://www.scopus.com/inward/record.uri?eid=2-s2.0-](https://www.scopus.com/inward/record.uri?eid=2-s2.0-85114213912&doi=10.1109%2fCyberSA52016.2021.9478246&partnerID=40&md5=d2c26f5a01dbbe9e42650cd070260339)

[85114213912&doi=10.1109%2fCyberSA52016.2021.9478246&partnerID=40&md5=d2c26f5a01dbbe9e42650cd070260339](https://www.scopus.com/inward/record.uri?eid=2-s2.0-85114213912&doi=10.1109%2fCyberSA52016.2021.9478246&partnerID=40&md5=d2c26f5a01dbbe9e42650cd070260339)