“Anatomy of a Cyber Attack”

with Forensic IT

All attendees will be on mute for the duration of the webinar.

Throughout the webinar, please ask questions using the chat function.

The recording and slides for this webinar will be made available on our website.

Enjoy the webinar!

For more information:

hello@dspanz.org

www.dspanz.org

dspanz.
digital service providers
australia new zealand

forensic it

Acknowledgement of Country

Belinda Stewart

DSPANZ Director & GNGB Director

Leveraging a wealth of leadership experience in compliance and data security, specialising in scoping, project management, consultation, and customised solutions. Bringing a unique perspective to the optimisation of Payroll, Time & Attendance, and HR processes. Recognised for the ability to devise innovative solutions, driving efficiency and ensuring compliance in business operations.

dspanz.
digital service providers
australia new zealand

forensic it

Charles Gillman

CISO - SuperChoice & DSPANZ Security Committee Co-Chair

With over two decades of expertise in Information Security, specialising in financial services. Led security teams at major institutions and held CISO roles in diverse settings, offering a comprehensive perspective from a background as a penetration tester. Provides practical solutions for current and emerging cybersecurity threats.

dspanz.
digital service providers
australia new zealand

forensic it

Jordan Hunt

Director of Cyber & Incident Response - Forensic IT

Drawing on extensive expertise in cyber incident response and forensic data analysis, Jordan is proficient in threat detection, digital forensics, and mobile device investigations. He brings a distinctive approach to cybersecurity challenges, adept at managing intricate cyber incidents and formulating effective strategies. Celebrated for his capability to improve cybersecurity defenses and establish resilient incident response frameworks.

dspanz.
digital service providers
australia new zealand

forensic it

“Anatomy of a Cyber Attack”

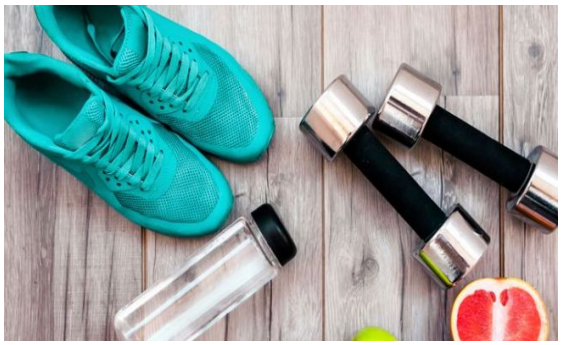
Jordan Hunt

dspanz.
digital service providers
australia new zealand

forensic it

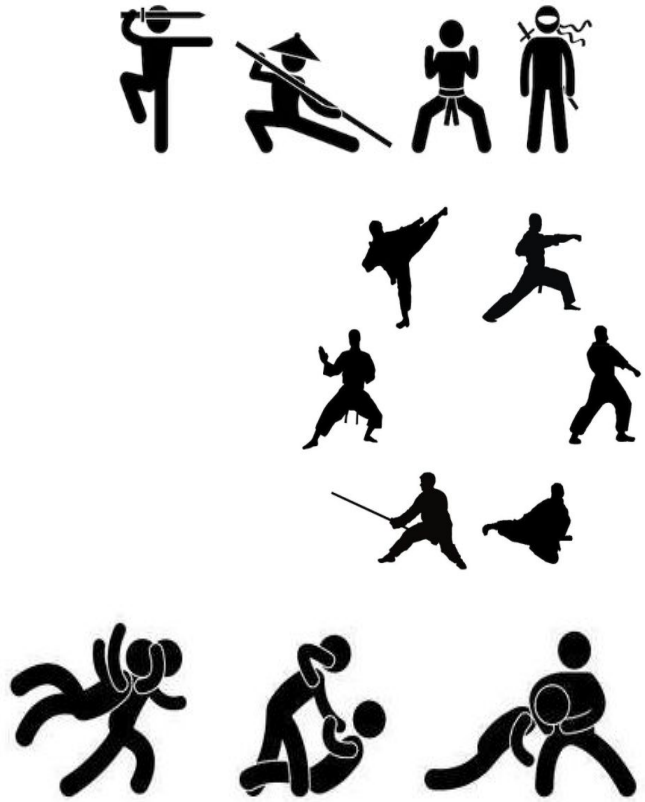
//_Anatomy of a Cyber Attack

//_What's the difference



IT Security

Cyber Security



Lockheed Martin – Cyber Kill Chain.

//_What's the difference

Risk Management

Asset, Change, Patch / Vulnerability & Configuration Management

Cybersecurity Program Management

Information Security Policies

Staff doing their part in keeping applications and operating systems up to date.

IT Security

Cyber Security

Threat Management

Situational Awareness

Event and Incident Response, Continuity of Operations

Take note of communications from Cyber Security advisors

Know, how and when to report an issue.

Risk = threat x Vulnerability +/- Controls

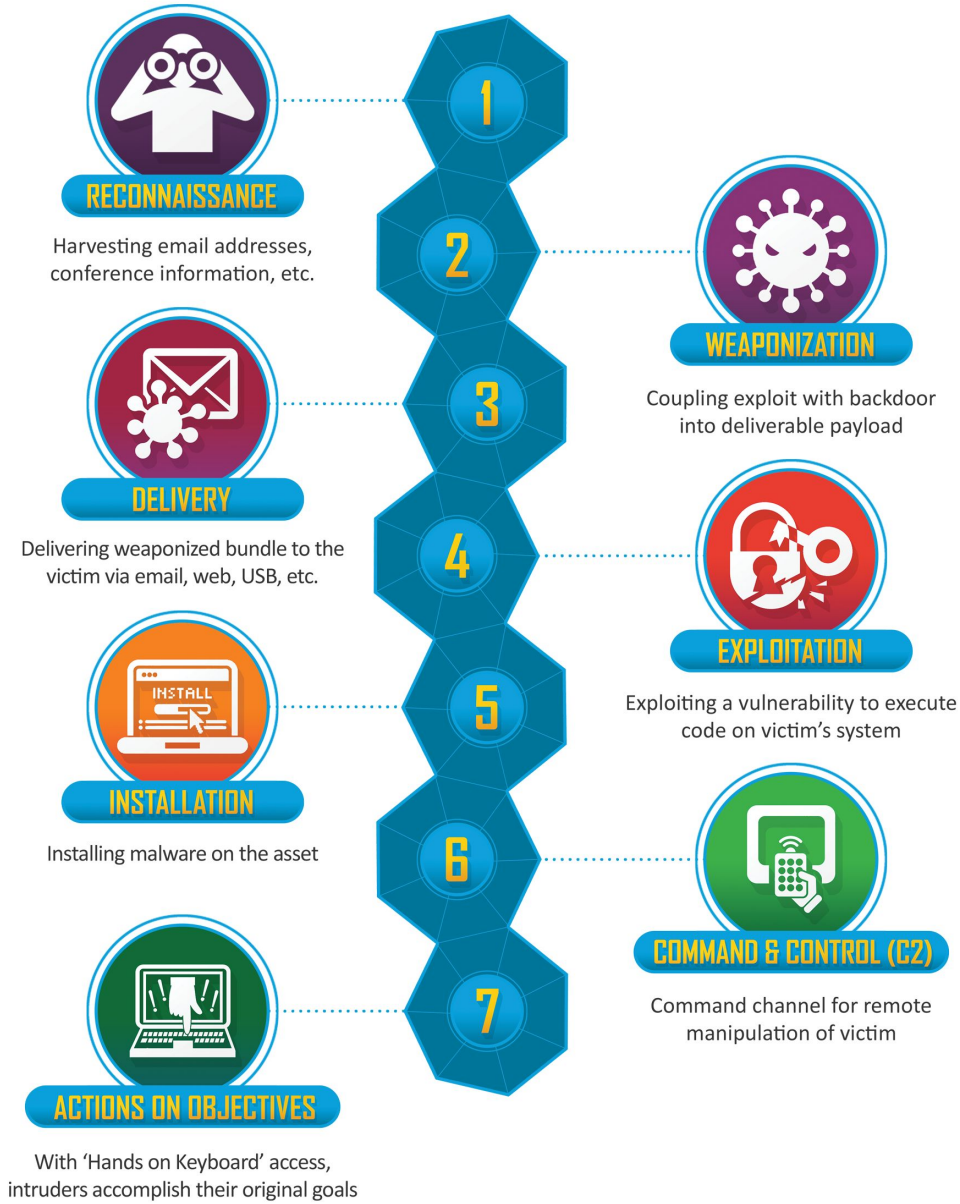
Risk = Threat x Vulnerability +/- Action

//_Some Context

Cyber Kill Chain

Cyber attacks don't materializese out of thin air.

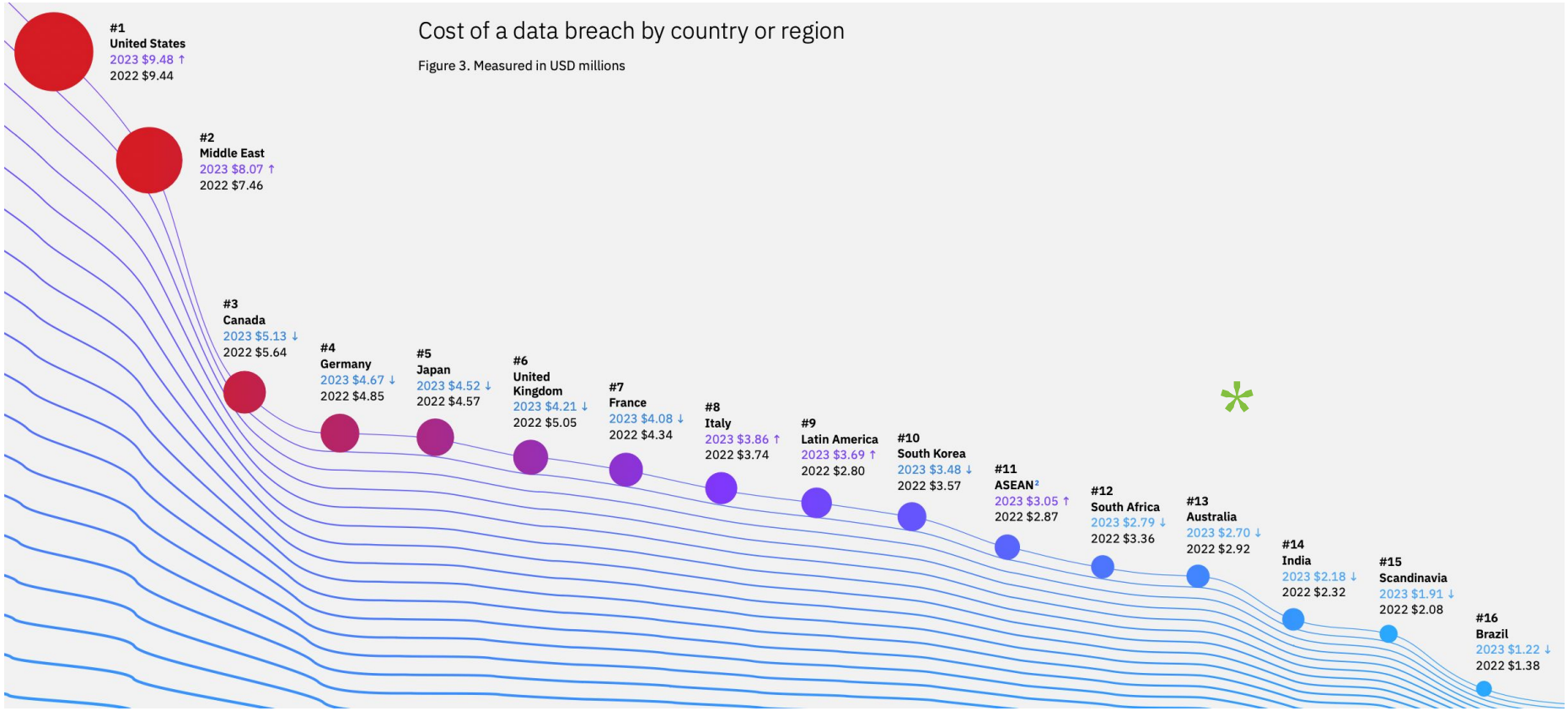
There is always a motive behind threat actors, and a process they MUST follow to achieve their objectives.



Lockheed Martin – Cyber Kill Chain.

//_Some Context

The 2022/2023 AEP of 7.40% represents a 2.15% increase in the likelihood of a cyber incident impacting Australian organisations over the 2021/2022 figure of 5.25%.



IBM Cost of a Data Breach Report 2023

* Average cost is $2,110,164 AUD when outliers US and UAE removed.

//_Some Context

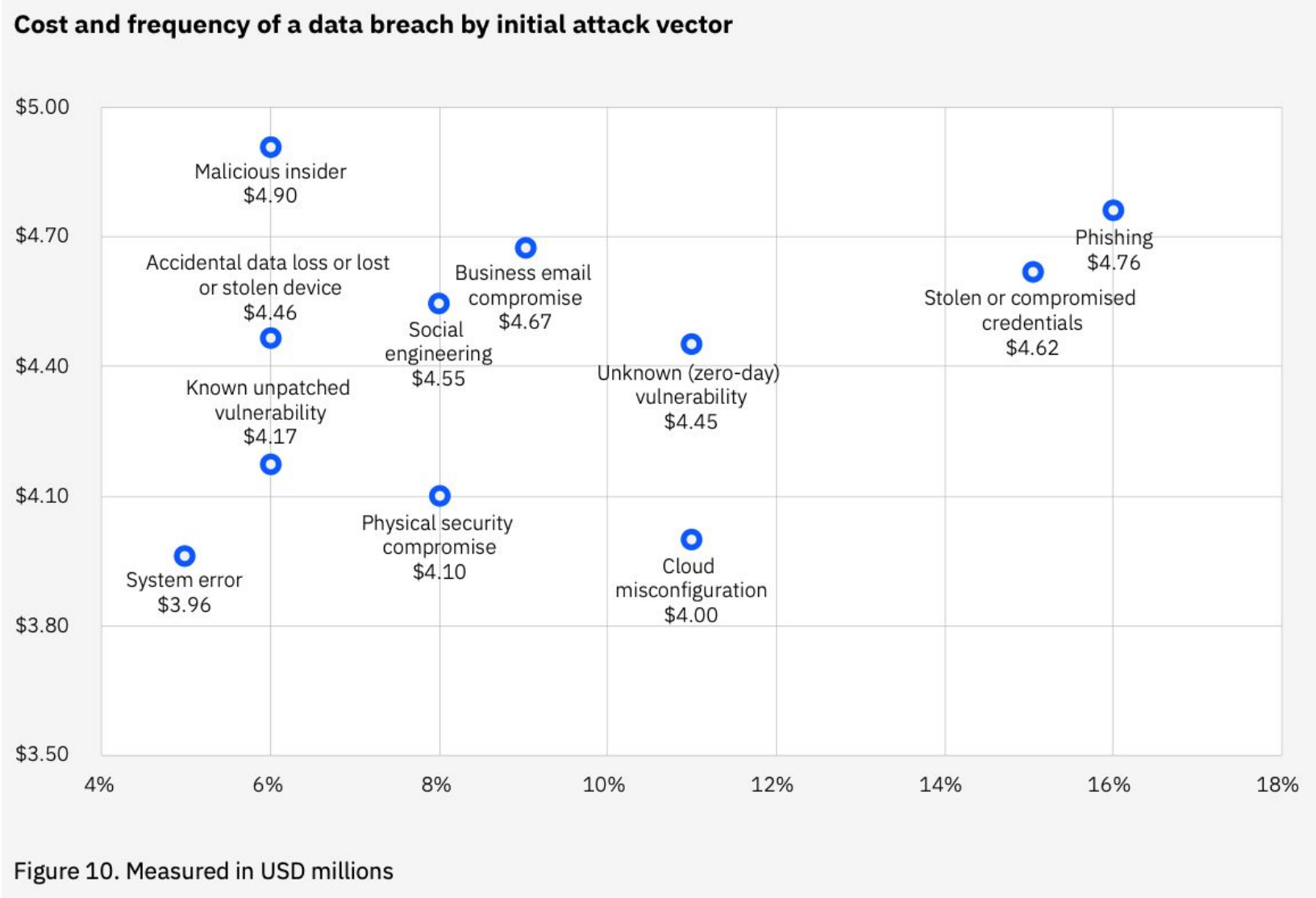
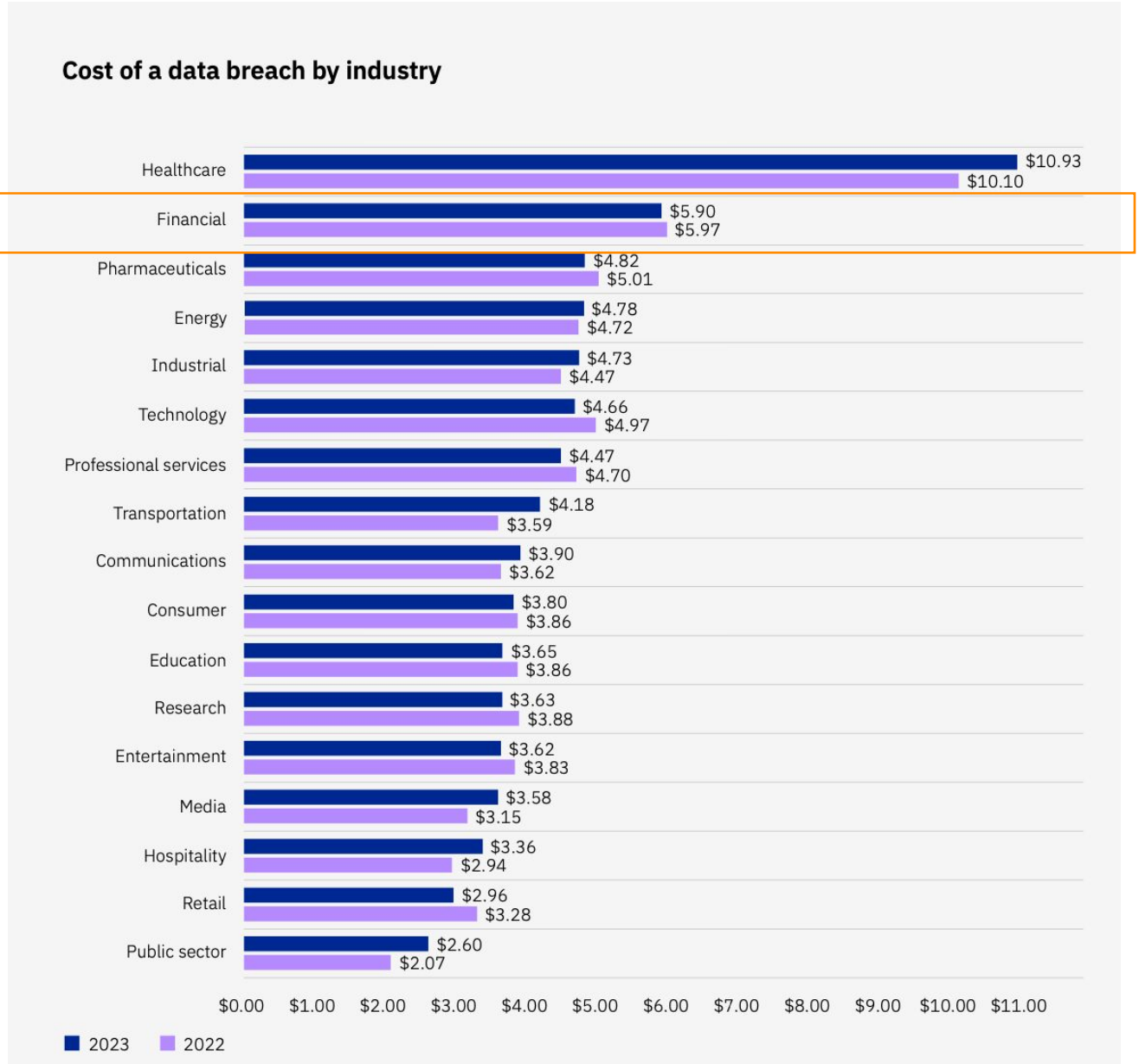


Figure 10. Measured in USD millions

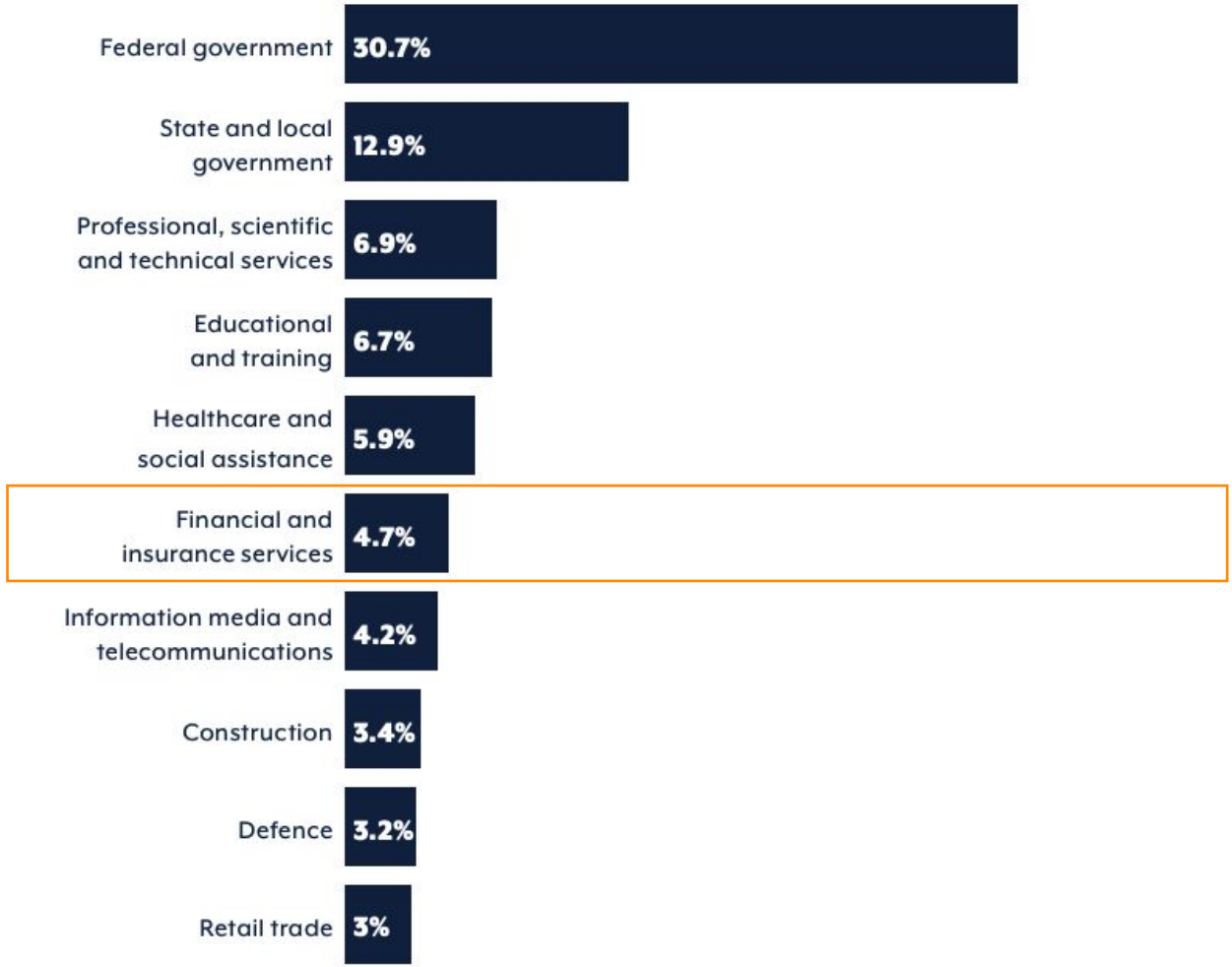
IBM Cost of a Data Breach Report 2023

//_ Industry Impact by Cost



IBM Cost of a Data Breach Report 2023

//_ Incident by Sector



Top 10 industry sector cyber security incidents to which the ACSC responded in financial year 2022–23.

Note: The reporting frequency of government agencies is in part due to their obligations to report significant cyber security incidents to the ACSC, and may not necessarily reflect a greater susceptibility to cyber security incidents. https://www.cyber.gov.au/sites/default/files/2023-11/asd-cyber-threat-report-2023.pdfq

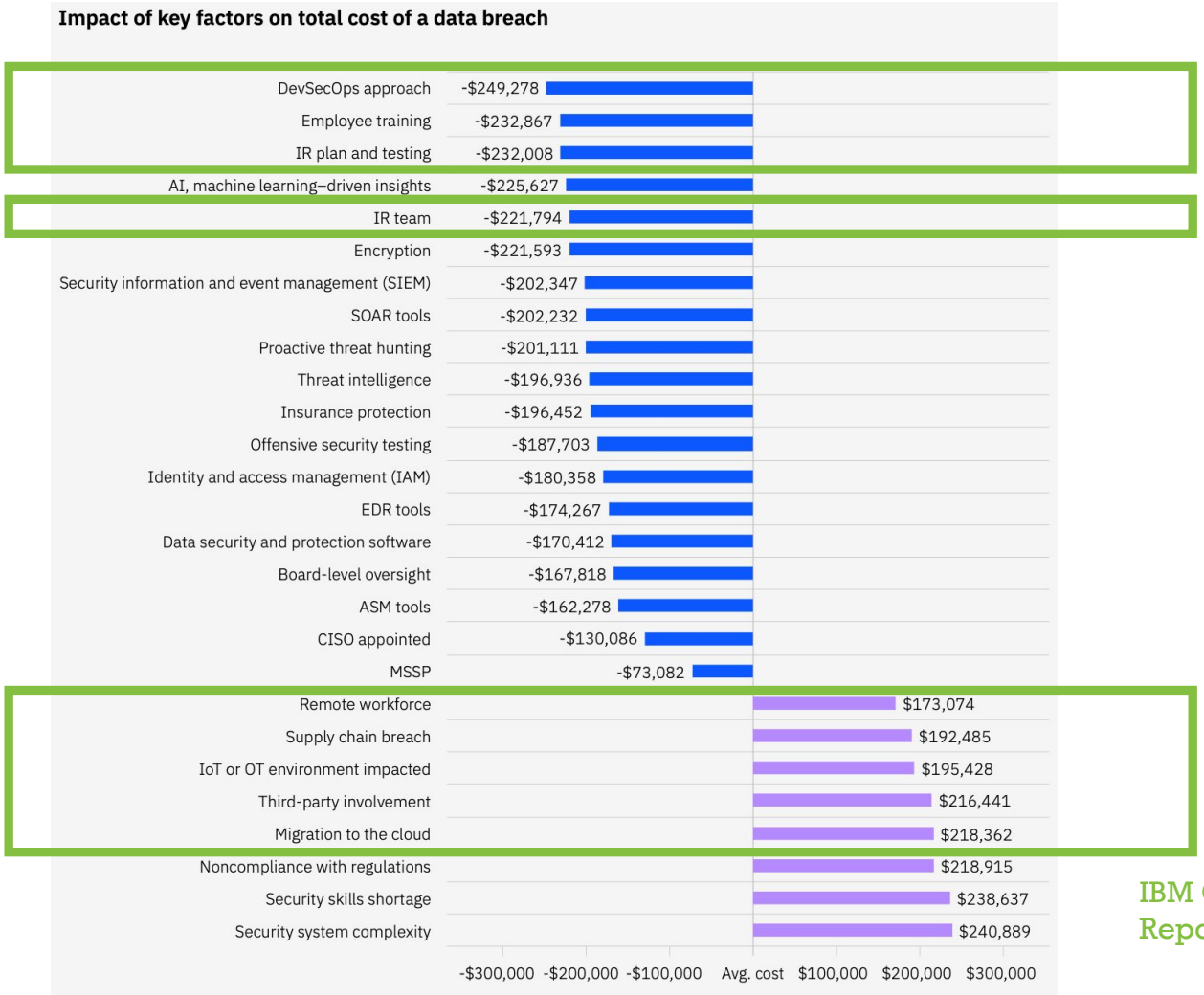
//_ Incident Severity Category

	Member(s) of the public	Small organisation(s) Sole traders	Medium-sized organisation(s) Schools Local government	State government Academia/R&D Large organisation(s) Supply chain	Federal government Government shared services Regulated critical infrastructure	National security Systems of National Significance
Sustained disruption of essential systems and associated services	C6	C5	C4	C3	C1	C1
Extensive compromise	C6	C6 15	C4 23	C3 17	C2 3	C1
Isolated compromise	C6	C5 38	C5 57	C3 63	C3 35	C2 2
Coordinated low-level malicious attack	C6	C6 7	C5 14	C4 32	C3 46	C3 1
Low-level malicious attack	C6 1	C6 73	C5 72	C4 88	C4 90	C3 9
Unsuccessful low-level malicious attack	C6	C6 19	C6 21	C6 73	C6 292	C6 43

Table 1: Cyber security incidents by severity category for FY 2022–23 (total 1,134)

ASCS Cyber security incidents by incident category for financial year 2022–23

//_Factors to Reduce the Cost



IBM Cost of a Data Breach Report 2023

//_Cyber Response Incident Phases

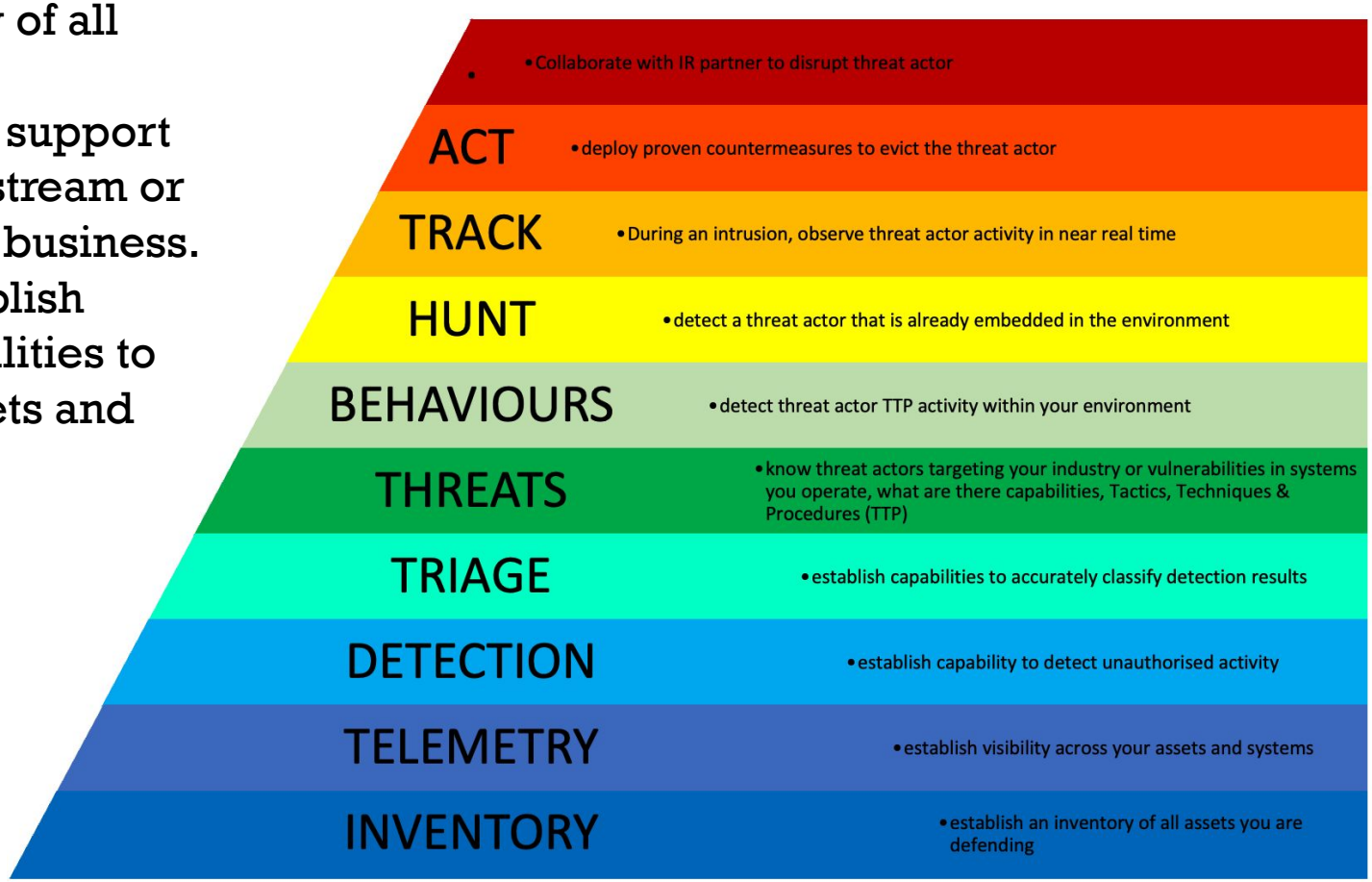
1

Preparation

Incident response methodologies emphasize preparation. This is achieved through establishing an internal response capability supplemented by an IR Partner, so the organisation is ready to respond to incidents, while also preventing incidents by ensuring that systems, networks, and applications are secure.

//_Preparation

Beginning with a solid inventory of all assets within the environment, understanding the systems they support and where they fit within the upstream or downstream supply chain of the business. Your organisation can then establish Telemetry and Detection capabilities to increase overall visibility of assets and systems.



//_Preparation

Profile Networks and Systems - Allows for measuring the characteristics of expected activity so that changes to your organisation's environment can be more easily identified. Organisations should run file integrity checking software on hosts to derive checksums for critical files and monitoring network bandwidth usage to determine what the average and peak usage levels are on various days and times.

Understand Normal Behaviours – Your organisation should study networks, systems and applications to understand what their normal behaviour is, so that abnormal behaviour can be more readily recognised. No staff member will have a comprehensive knowledge of all behaviour throughout the organisation's environment but should know which experts could fill in the gaps.

//_Preparation

Enable PowerShell Script Block Logging - PowerShell Module, Script Block, and Transaction logs, can be enabled via group policy. The default log size should also be increased to capture appropriate log time frames.

Log Retention Processes - Information regarding a cyber security incident may be recorded in several places, such as firewall and application logs. Creating and implementing a log retention process that specifies how long log data should be maintained will be extremely helpful in analysis because older log entries may show reconnaissance activity or previous instances of similar attacks. The length of time to maintain log data will depend on several factors, including your organisation's data retention policies and the volume of data.

//_Preparation

Keep All Host Clocks Synchronised - Protocols such as the Network Time Protocol (NTP) synchronise clocks among hosts. Event correlation will be more complicated if the devices reporting events have inconsistent clock settings. From an evidentiary standpoint, it is essential to have consistent timestamps in logs.

Maintain and Use a Knowledge Base of Information – Your organisation's ICT knowledge base should include information that the IMT need for referencing quickly during cyber security incident analysis. A simple approach to system documentation will be most effective. Text documents, spreadsheets, and relatively simple databases provide effective, flexible and searchable mechanisms for sharing data among IMT members.

//_Preparation

Ensure Volume Shadow Copy Snapshots are enabled – All systems critical to the delivery of the organisation's services should have Volume Shadow copy snapshots enabled, with the "scope snapshots" functionality disabled to ensure all critical data is protected. In addition to this, increasing the reserved size for snapshots and the frequency (using scheduled tasks) should be considered for critical systems.

Increase NTFS Journal file size – The Microsoft Windows NT File System (NTFS) maintains multiple files that are critical to the successful investigation of cyber incidents. The $Logfile and $USNJRNL record file and folder metadata for each individual NTFS volume. The file size of these two NTFS artifacts can be increased to ensure the potential attack time window is retained .

//_Case Study

On Saturday the 9th of September 2023, Forensic IT were engaged by the client to investigate the potential compromise of their cloud infrastructure and systems. The client had identified that on the 4th of September 2023 between 10:49PM and 11:48PM (AEST) **a total of 36 unauthorised cryptocurrency transactions** consisting of a mix of Ethereum and Ethereum Tokens on Ethereum-compatible blockchains occurred from a web platform developed and operated by the client.

The unauthorised transactions collectively withdrew almost all available digital assets from one of the "hot" wallets supporting the web platform production environment. The total amount of the digital assets stolen was almost limited by the available funds within the wallet, except that the **transaction service crashed just prior to that occurring**.

The total amount of Ethereum / Ethereum Tokens stolen from the hot wallet at the time of the incident was estimated at approximately **$62 Million AUD**.

//_Cyber Response Incident Phases

2

Identification & Scoping

Identification is triggered by a suspicious event. This can be an alert from Security monitoring systems, a call logged with the IT helpdesk, or the result of findings from a pro-active threat hunt. Event validation should occur before a cyber incident is declared, classified, and the formal incident response process has begun.

This phase is used to better understand the findings and begin scoping the network for additional compromised systems.

//_Case Study

Initial access to the client's web platform / environment was obtained through a sophisticated **social engineering campaign** that has been identified and reported on by multiple cyber intelligence organisations. Over the previous few months **5 cyber incidents resulting in the theft of large sums of cryptocurrency have been attributed to the Lazarus Group** (AKA Labyrinth Chollima, Hidden Cobra, APT37, APT38 or Jade Sleet), a hacking group with links to the North Korean Government (Democratic People's Republic of Korea). **The cyber incident impacting the client was part of this Lazarus Group campaign.**

//_Cyber Response Incident Phases

3

Containment & Intelligence Development

In this phase of the incident response process, the goal is to rapidly understand the threat actor and begin developing a containment strategy. The IMT must identify the:

- initial vulnerability or exploit used (Initial Attack Vector);
- how the attackers are maintaining persistence;
- how the attackers are laterally moving through the network; and
- how command and control or data exfiltration is being accomplished.

In conjunction with phase-2 the IMT will work to develop a complete picture of the attack, while implementing changes to increase host and network visibility. Threat Intelligence is one of the key components of this phase.

//_Case Study

An internal developer (e.g. John Smith) confirmed he has been **undergoing a recruitment process.** The recruitment agency reached out initially to him **via LinkedIn (and subsequently Telegram)**. As part of the interview process, John Smith has been **tasked to download and work with a given GitHub repository and solve certain challenge as a test of his technical skillset**.

John further confirmed he **undertook the test task on his personal laptop, on which in the past he had used legitimate credentials to access various corporate / development environments and systems.**

On noticing certain irregularities on his device, John conducted a full factory reset his laptop in the morning prior to crypto theft occurring.

It was confirmed that John had been part of a sophisticated social engineering campaign targeted at the organisation's development team, where the threat actor were able to compromise John's personal laptop **to harvest his credentials (with AWS administrative rights) to carry out the subsequent attack.**

//_Case Study

GitHub / Docker Hub Analysis

A preliminary review of GitHub logs confirmed the compromise and **use of the John Smith account to access GitHub / Docker Hub with suspicious user agents recorded** between 4 August 2023 14:29 and 2 September 2023 00:45:

- Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit / 537.36 (KHTML, like Gecko) Chrome /116.0.0.0 Safari/ 537.36
- Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/115.0.0.0 Safari/537.36

Through discussions with client staff and analysis of logs, it was identified that **the compromised version of the docker image was created by the threat actor within the clients private Docker Hub account** on 31 August 2023 and subsequently **tagged as "production", initiating the attack and theft of crypto currency.**

//_Cyber Response Incident Phases

4

Eradication & Remediation

The most important phase of the incident response process, eradication aims to remove the threat and restore normal business operations. Successful eradication cannot occur until the full scope of the incident is understood, this is why phase-2 and phase-3 operate as a cycle until the incident is fully scoped and containment is complete. Remediation plans are developed, with immediate tactical recommendations implemented in a controller manner. Examples include:

- block malicious IP address and domain names
- rebuild compromised systems
- enterprise wide password reset
- changes to cloud or on-premis systems

5

Recovery

Recovery from a cyber incident enables to organisation to return to day-to-day operations. The organisation will have learned alot from the incident investigation and will have many recommendations to implement to improve its cyber resilience. Recovery plans should be divided into relief and early recovery, medium-term recovery and long term recovery objectives. The goal is to improve the overall cyber security to prevent reinfection. Some examples of recovery recommendations include:

- improvements in authentication, password management
- enhance network visibility (SIEM implementation for centralised logging)
- comprehensive patch management processs

//_Cyber Response Incident Phases

6

Lessons Learned / Post Incident Activity

Use the lessons learned as a chance to achieve closure with respect to an incident by reviewing what occurred, what was done to intervene, and how well intervention worked. Some questions to answer during a post incident review include:

- exactly what happened, and at what time?
- what information was needed sooner?
- were any actions or steps taken that might have inhibited phases of the IR process?
- what IoC or precursors should be watched for in the future to detect similar incidents?

//_Log Management & Retention

Since event logs can contribute to investigations following cyber security incidents, they should ideally be retained for the life of a system, and potentially longer. However, the minimum retention requirement for these records under the Public Record Office Victoria (PROV) Common Administrative Functions Retention and Disposal Authority (RDA) publication is seven years. The governing body will likely change depend on the state in which your organization and clients are operating.

The following list of events can assist in monitoring the security posture of systems, detecting malicious behaviour, and contributing to investigations following cyber security incidents in the future.

For any system requiring authentication, successful logon, failed logon and logoff events are logged.

//_Log Management & Retention

The following events are logged for operating systems:

- access to important data and processes
- application crashes and any error messages
- attempts to use special privileges
- changes to accounts
- changes to security policy
- changes to system configurations
- Domain Name System (DNS) and Hypertext Transfer Protocol requests
- failed attempts to access data and system resources
- service failures and restarts
- system start-up and shutdown
- transfer of data to external media
- user or group management
- use of special privileges.
- Command line execution

//_Log Management & Retention

The following events are logged for web applications:

- authenticated user access
- attempted access that is denied
- crashes and any error messages
- search queries initiated by users.
- user agents connecting
- IP addresses and associated port of connection
- access to sensitive information

//_Log Management & Retention

The following events are logged for databases:

- access to particularly important information
- addition of new users, especially privileged users
- any query containing comments
- any query containing multiple embedded queries
- any query or database alerts or failures
- attempts to elevate privileges
- attempted access that is successful or unsuccessful
- changes to the database structure
- changes to user roles or database permissions
- database administrator actions
- database logons and logoffs
- modifications to data
- use of executable commands.

//_Change the Context

You can reduce the risk of cyber attacks by:

- Thinking before you act;
- being aware of the Delivery methods;
- play your role in keeping Systems up to date; and
- maintaining good password hygiene.

Thank you for listening

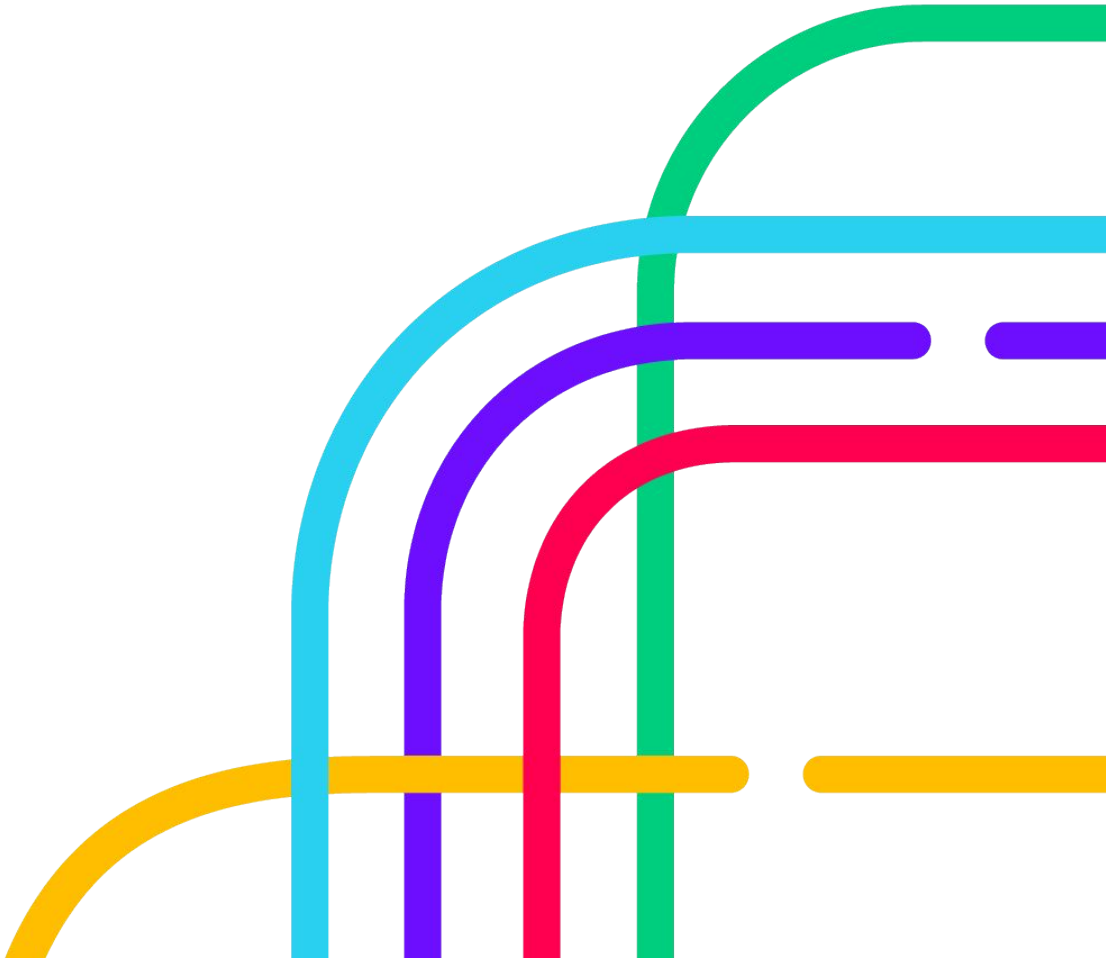
//_CONTACT

Jordan Hunt – Principal Analyst, Cyber Incident Response

+61 437 979 163

Jordan.hunt@forensicit.com.au

Group Q&A



dspanz.
digital service providers
australia new zealand

forensic it

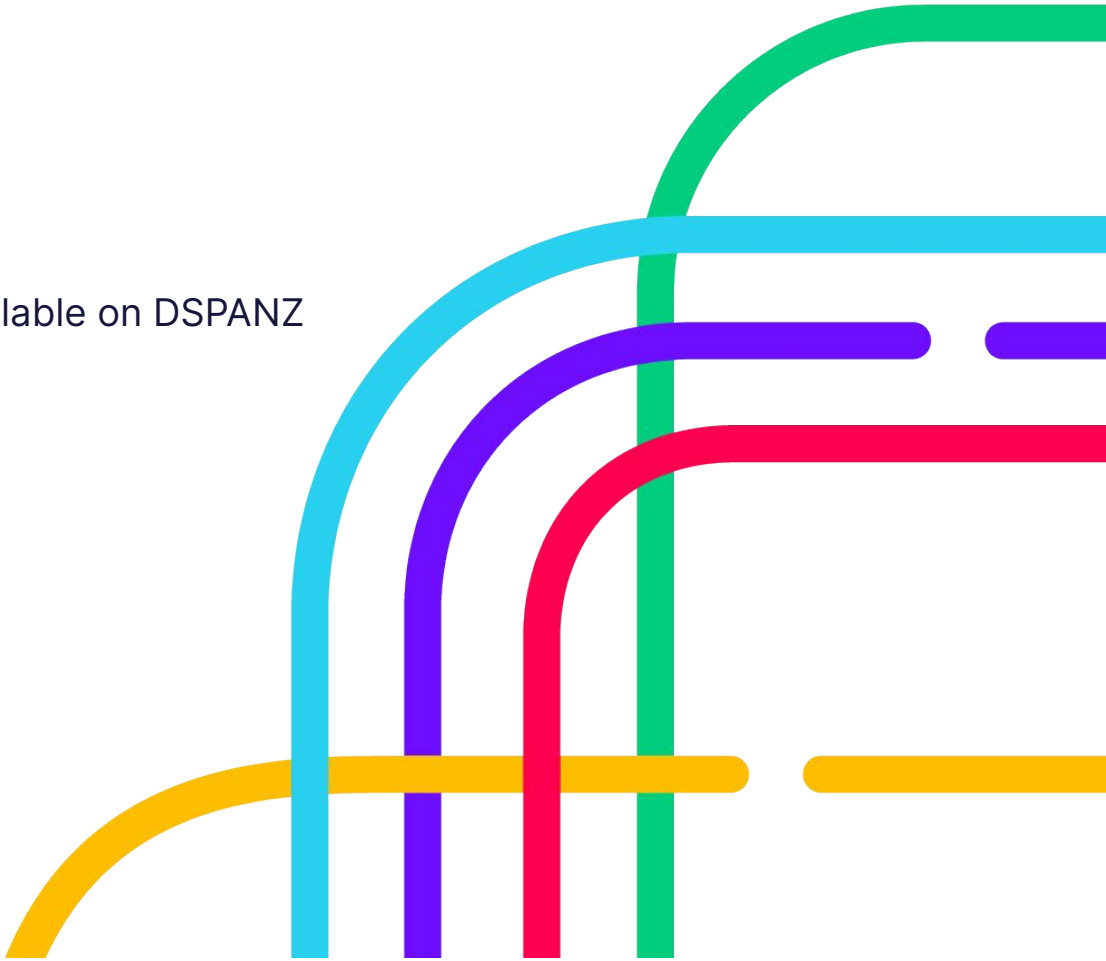
Thank you for joining us

The recording and slides for this webinar will be made available on DSPANZ website.

For more information:

hello@dspanz.org

www.dspanz.org



dspanz.
digital service providers
australia new zealand

forensicit