2A - Hacked
The Anatomy of a Cyber Attack

William Makdessi
Cyber Risk Lead

InConsult
risk advisory | audit | assurance

The Institute of Internal Auditors
Australia

Discussion Topics

Improve your awareness of the current cyber threat landscape threatening Australian businesses.

We will cover:

- Understanding strategies that hackers use to gain entry into systems
- Assessing your cyber incident prevention, detection, and response program
- Using penetration testing to understand your cyber risk vulnerabilities
- Understanding the role of internal audit and independent assurance

STRATEGIES USED BY HACKERS

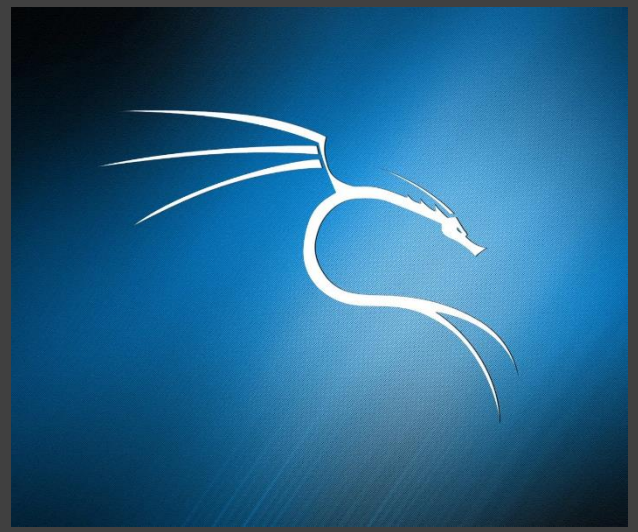
Cyber Threat Stats in 2022

- The cost of scams in 2022 has already exceeded the total value in 2021 in only 9 months
- Primary victims are greater than 35 years old
- The financial sector is the second largest victim behind healthcare
- 93% of all corporate networks in Australia are penetrable
- There is an attack on a small to medium enterprise every 10 minutes
- In the month following the Optus breach there were more than 50 attacks on other organisations
- Threat actors are using techniques that are commensurate with our vulnerability landscape

Common Issues We Observe

- Email security in Australia is poorly managed with the majority of organisations easily penetrable.
- Mobile devices are a silent killer. Mobile phones accounted for the highest number of malware attacks in Australia.
- Ransomware attacks are no longer just about money. Data is king on the dark web.
- Poor upkeep of security configurations and basic or no information security framework in place.
- Many IT teams are not educated on the latest threats and what tools are available to them.

How Attackers Gain Entry



External mapping

Persistence

Timing

Advancements in Ransomware

- Delivery of macro payloads without engaging content.
- Extensive reconnaissance on organisations, social media, understanding staff and infrastructure.
- Time-based ransom increases and critical service attacks to increase pressure and the likelihood of payment.
- Offering decryption of a file or portions to infer trust in the attacker.
- Encryption combined with immediate exfiltration to leverage public release or harming clients or staff. All ransomware is a data breach.
- Advertising the compromise to stakeholders, staff and more.
- Ransomware as a Service (RaaS)

AlphV/Blackcat Ransomware

- Completely customisable command-line ransomware built on new-era code (Rust).
- Innovative approaches including tokenised negotiation portal with victims.
- Dormancy capability to avoid detection.
- Flexibility in complexity: worm option, avoid servers, four types of encryption, desktop editing, network share access and lateral movement.
- Blackcat User-friendly search engine to find out if you have been compromised.

ASSESSING YOUR CYBER SECURITY PROGRAM

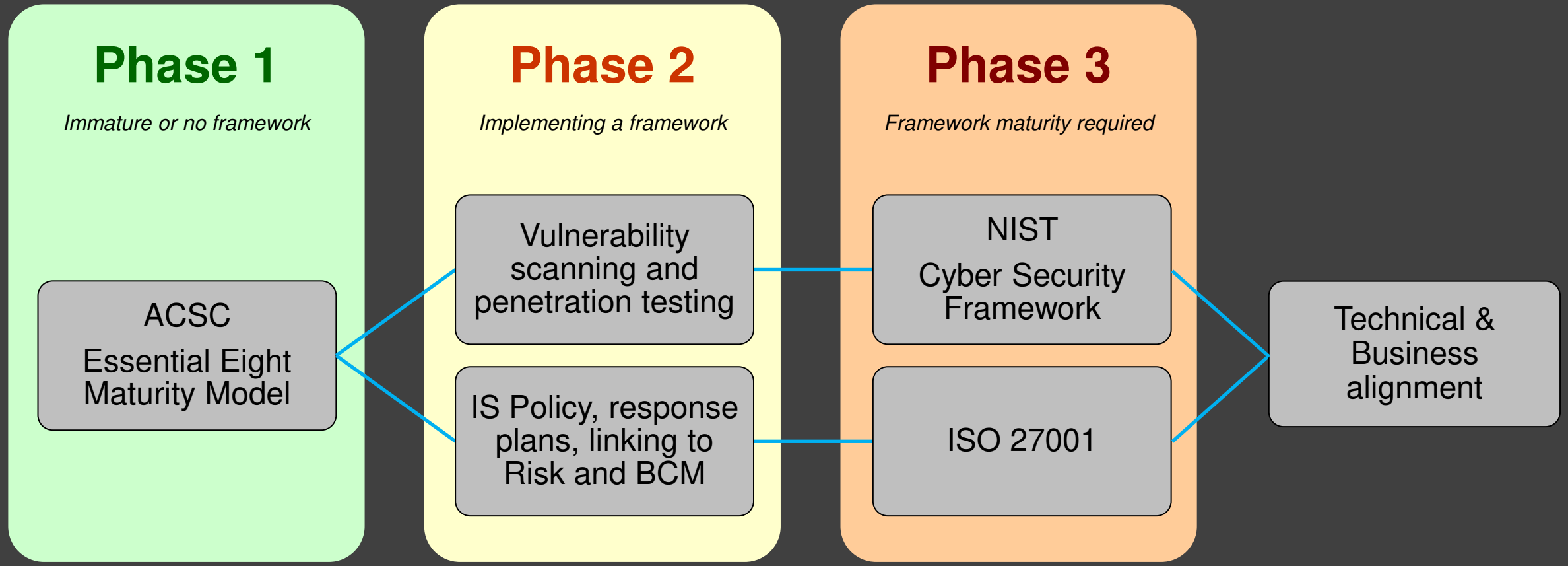
The Institute of Internal Auditors Australia

InConsult risk advisory | audit | assurance

How Mature is Your Program

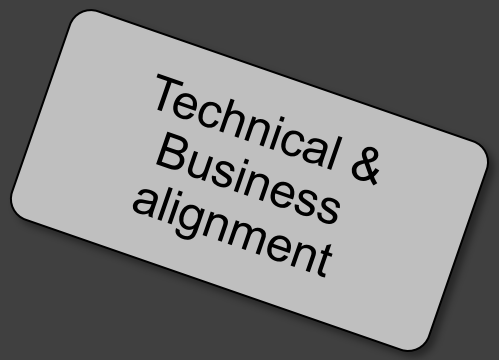
- Is your cyber security program based on a better practice framework – NIST, ISO, ACSC, APRA
- How does your organisation fair against the ACSC Essential Eight Maturity Model
- Understand the difference between technical and business-oriented frameworks
- Is there a roadmap for maturity development
- What were the results of an independent assessment
- IT are not responsible and they never were

General Assessment Tiering



Technical and Business Alignment

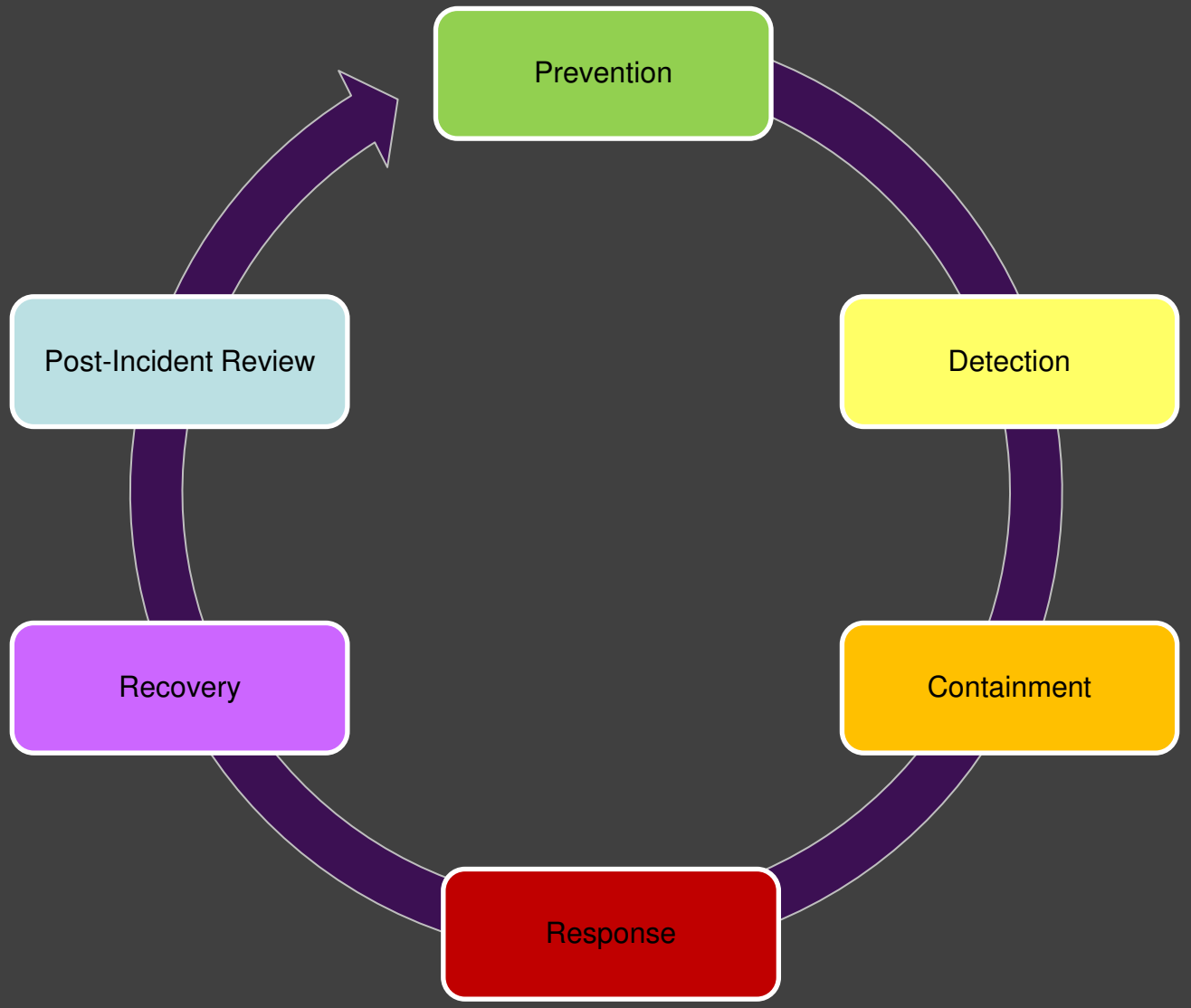
- The key role of the Risk Management and Business Continuity Management frameworks
- IT should understand Risk, and Risk should understand IT – IT Governance as a mediator
- Information assets are owned and/or supported by the entire organisation
- Poor asset management can result in data breaches
- Success is the operation and recovery of critical systems to meet both technical and business requirements



Education & Testing

- Start early
- Experiential learning is the best way to prepare for an incident
- Baselines allow for rapid identification and resolution
- Always challenge ordinary thinking. Is this really a critical system, how long can we last, what will we do if we cannot recover
- Cyber risk awareness training is cheap and tremendously effective
- Independent assessments cut away the fairy tale

The Typical Information Security Framework



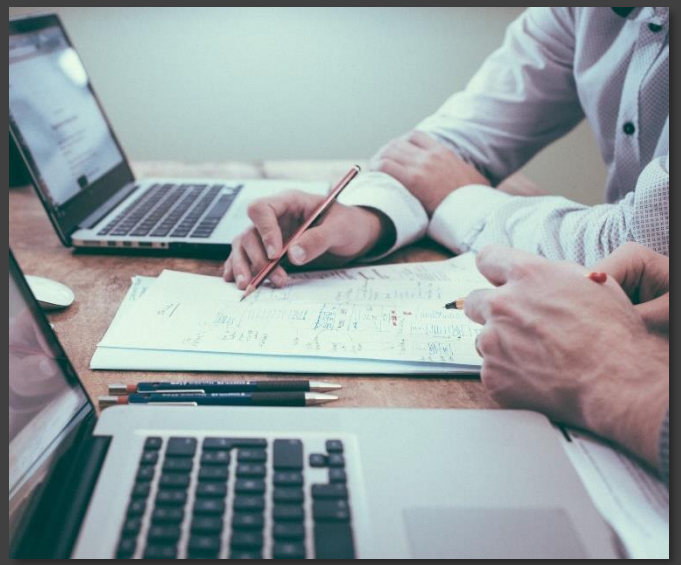
Pen Testing to Identify Vulnerabilities

The Great Misconception

- Penetration testing or “pen testing” involves internal and external testing of systems. Always both for good reason.
- External pen testing alone is not really pen testing.
- Vulnerability scanning is highly value but completely different.

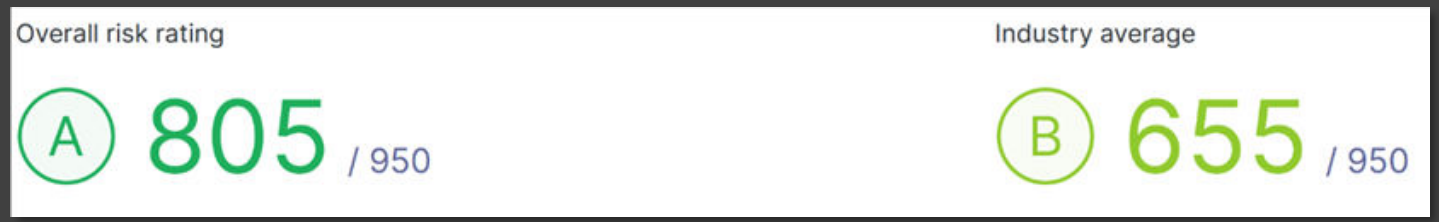
Understand Your Scope

- Pen testing can become costly fast
- Typically, testing charges per application, website or API. A flat rate charge is also an indicator of inexperience
- A single application pen test can range from $3k to $15k
- Testing can take a few weeks to a few months
- Almost all testers provide free checking after remediating critical issues
- With cost easily multiplying, focus on critical systems



Ongoing Vulnerability Scanning

- Much cheaper and provides similar coverage to external pen testing
- Live updates on vulnerability changes represented by a Cyber Security Rating mapped against the Common Vulnerabilities and Exploits (CVE) database
- Takes a maximum of 48 hours to identify issues by way of propagation
- Also helps with information asset mapping and identifying unsafe rogue assets
- Can be used to provide assurance to stakeholders and partners at any point in time



Internal Audit and Independent Assurance

The Institute of Internal Auditors Australia

InConsult risk advisory | audit | assurance

Frameworks & Internal Audit

- Almost all well-known frameworks require an internal audit function to test the suitability and operational effectiveness of information security controls
  - Suitability: The appropriate allocation of a control based on the risk statement
  - Operational Effectiveness: The adequate performance of a control in the last 12 months of implementation
- Control testing should be performed annually and be used as the foundation for budget allocation and maturation of the information security framework
- Control testing is great preparation for external audits and assurance

The Value of Independent Assurance

- Completely external viewpoint, much like that of a threat actor
- Offset costs of vulnerability tools and monitoring to a vendor that has an arsenal of valuable tools
- Much like Internal Audit, most frameworks require independent assessment to validate testing and the Internal Audit program itself
- Getting setup for accreditation, reviews, regulator audits
- Independent assurance holds high value

Summary

- *Attackers* – There is and always will be easy ways for attackers to gain access due to our dependence on technology and constant evolution
- *IS Frameworks* – Contextualise your framework and constantly work to better it. Maturity should be an every day ongoing activity
- *Pen Testing* – Vulnerability scanning and pen testing are two different things. Work out your scope and have the critical system assessed annually
- *IA & Independent Assurance* – Internal Audit and Independent Assurance are not only required, they provide a great means of gap analysis and assuring stakeholders of your cyber security capability

Thank You

William Makdessi

0416 090 893

williamm@inconsult.com.au

www.inconsult.com.au

InConsult

risk advisory | audit | assurance