PERTHSEC

AISA
Cyber | smart · safe · secure

The essential 8 - A light hearted review of the controls and why you didn't implement them

The Australian Cyber Security Centre (ACSC) describes the essential 8 as "a series of baseline mitigation strategies taken from the Strategies to Mitigate Cyber Security Incidents recommended for organisations. Implementing these strategies as a minimum makes it much harder for adversaries to compromise systems."

The statement is true, yet this baseline often feels aspirational to many organisations. This session will provide a brief view on each control and reasons why they are not implemented. What looks like an easy win can often require major organisational change, and even worse, impact businesses potentially worse than the supposed risk being mitigated.

Attending this session will leave you a little more informed, likely a little more concerned, and hopefully a lot more motivated to manage the risk in your organisation, adopting mitigation strategies appropriate to your environment and helping to meet your GRC obligations.

Presenter:
GEORGE COLDHAM

MAIN STREAM
10:45 AM – 11:25 AM
CENTRAL BALLROOM

PERTHSEC

AISA
Cyber | smart · safe · secure

Cyber espionage reloaded

Last year Check Point Research published evidence of an ongoing cyber espionage operation against several national and state government entities in the Asia Pacific (APAC) region, including a state government in Australia. This operation, which we were able to attribute to the Naikon APT group, used a new backdoor named Aria-body, in order to take control of the victims' networks.

Aria-body is what is known as a backdoor, a tool that is used to gain access to a computer or server without using the traditional access points. They can give unauthorized users access to sensitive information, or even allow that person to control the system. Backdoor tools can do different things, but in the specific case of Aria-body, they are designed, to gather data on the victim's machine, including: Host-name, computer-name, username, domain name, windows version, processor ~MHz, MachineGuid, 64bit or not, and public IP.

In this presentation, Ashwin will describe the tactics, techniques, procedures and infrastructure used by the Naikon APT group over the five years since the last reports, and offer some insight into how they were able to remain under the radar. We also discuss and shed light on countries that are currently being targeted by this threat actor.

Presenter:
ASHWIN RAM

TECHNICAL STREAM
10:45 AM – 11:25 AM
NORTH BALLROOM (VIRTUAL PRESENTER)

PERTHSEC

AISA
Cyber | smart · safe · secure

Risk benefit analysis of cyber security programs and change initiatives to measure return on investment for value at risk

Cost and financial risk are frequently measured in return on investment (ROI), risk adjusted cost of capital (RACOC) and risk adjusted return on capital (RAROC). These quantitative measures are dependent on the organisation having the ability quantify the value of assets, known as value at risk (VaR). In some organisations these values are explicit, such as banking, while in other industries, some have quantifiable value, such as the price of a hospital but others, such as how a patient feels as they leave the hospital, do not.

Those organisations which can demonstrate meaningful benefit in financial risk and cost from cyber security change initiatives are the most likely to gain the required internal and external financial support. Vendors of cyber security technologies and consulting services focus on those industries with readily quantifiable VaR as these have consistently proven to be most fertile markets. Is cyber security ROI as feasible in qualitative outcome focussed industries such as government and health?

Many of the cyber security ROI arguments are specious and focussed on selling a particular vendor's technologies or services. A new firewall may reduce the volume of unsolicited network events but this does not actually address the question of whether risk is reduced. An annual click-through online awareness course may make all feel that they are doing something about cyber security but probably does nothing to reduce the probability of cyber attacks such as ransomware. In this presentation, we will discuss how can cyber security initiatives be measured by how they reduce risk.

Presenter:
LUKE FORSYTH

MAIN STREAM
11:30 AM – 12:10 PM
CENTRAL BALLROOM

PERTHSEC

AISA
Cyber | smart · safe · secure

My war stories - hacking some of the worlds' biggest brands

In a world where threats and threat-actors operate at scale, how do you protect and defend your business 'at scale'?

Over the past few years, Michael has worked as a crowd-sourced bug bounty hunter in his spare time. Somehow through this experience, he has managed to end up ranking in the top 1% of bug hunters on the Bugcrowd platform globally and was subsequently recognised by Bugcrowd for "tremendous impact".

In this presentation, Michael will walk you through some of his hacking exploits and tell the story of how he has been able to get a small edge over the global crowd of white-hat hackers.

This presentation will hopefully be a fun way to highlight:

- To organisations, the value of crowdsourced security in a world where threat actors are operating at scale
- To beginners in security, how to get a competitive edge in a world where cyber security roles are hot.

Presenter:

MICHAEL HYNDMAN

TECHNICAL STREAM

11:30 AM – 12:10 PM

NORTH BALLROOM

PERTHSEC

AISA
Cyber | smart · safe · secure

Shift left: Cyber pilgrimage, culture odyssey and coffee addiction

There has been much talk about the need for cyber security practitioners to “shift left” to cultivate a robust cyber aware practice in recent years. However, what does it mean to be shifting left? Is it DevOps or DevSecOps? Or is it implementing TOGAF (The Open Group Architectural Framework) or SABSA (Sherwood Applied Business Security Architecture) for the whole organisation?

In this presentation, Joshua will provide some learnings and reflections drawing from personal experiences and attempts to “shift left” and why creating a “culture” can be so challenging and even counter-productive if not done well.

The presentation will also challenge some of the commonly held beliefs and practices within the cyber community, with the intent to incite meaningful soul searching and robust conversations.

Presenter:
JOSHUA QWEK

MAIN STREAM
1:15 PM – 1:55 PM
CENTRAL BALLROOM

PERTHSEC

AISA
Cyber | smart · safe · secure

Setting yourself up for success - Logging and monitoring

- How did they gain access to our environment?
- How long have we been compromised?
- Did they steal any data?

These questions have been asked in every intrusion Barnaby has worked as an incident response lead for Mandiant. The ability to quickly answer these questions is often limited by gaps in the default logging configuration of enterprise products which overlook critical details needed to support incident response investigation.

In this presentation, Barnaby will discuss critical logging configurations and monitoring practices which fill commonly overlooked gaps and set you up for success in your next investigation.

Presenter:
BARNABY SKEGGS

TECHNICAL STREAM
1:15 PM – 1:55 PM
NORTH BALLROOM

PERTHSEC

AISA
Cyber | smart · safe · secure

The role of Boards and Executives in cyber strategy: Key insights to delivering real cyber resilience

In June 2021, the Avertro team spoke with a number of board members, business executives, CISOs, and cyber security leaders to gain an understanding of how organisations manage cyber security.

This presentation will report on the learnings from this study and provide key insights on the challenges and solutions around managing the business of cyber, and how organisations are elevating their game to meet the ever-increasing demand for improved cyber resilience.

Some of key questions that will be covered are:

- Where are the biggest misalignments between leadership and cyber security teams and what are the key strategies that help connect them
- What makes an effective cyber security strategy and why it's crucial the board/ leaders need to play their part in developing it
- Cyber security problem statement trends (specifically focusing on strategy and business alignment)
- Potential AI/ML use-cases for better data-driven decision making in cyber
- Learnings from cyber leaders in the finance, federal government, and education sectors

Presenter:
FARRELL TIRTADINATA

MAIN STREAM
2:00 PM – 2:40 PM
CENTRAL BALLROOM

PERTHSEC

AISA
Cyber | smart · safe · secure

13,000 incidents: A study of global healthcare data breaches, staff attitudes and what any industry can learn

Healthcare data can contain sensitive, personal, and confidential information that should remain secure. Despite the efforts to protect patient data, security breaches occur and may result in fraud, identity theft, and other damages.

The recent IBM Security Data Breach Report, found that healthcare breach costs have surged. Industries that faced huge operational changes during the pandemic (healthcare, retail, hospitality, and consumer manufacturing/distribution) also experienced a substantial increase in data breach costs year over year. The global study found that healthcare breaches cost the most by far, at $9.23 million per incident – a $2 million increase over the previous year.

In this presentation, Martin will summarise a three year PhD study that has collated and reviewed over 13,000 cyber security healthcare data breaches in the UK, USA, Australia and New Zealand. Also presented for the first time are the findings from a national healthcare staff survey that reveals some clues as to why this paticular industry has the dubious title of being ‘most breached’, and what any sector can learn and implement within their own systems.

Presenter:
MARTIN DART

TECHNICAL STREAM
2:00 PM – 2:40 PM
NORTH BALLROOM