PERTHSEC

AISA
Cyber | smart · safe · secure

Cyber lessons in the wake of Russia's invasion of Ukraine

More than 75 days after Russia invaded Ukraine, what cyber security lessons should security leaders be learning from the conflict?

This presentation details the cyber activity Microsoft has observed as part of the war in Ukraine, and the work we have done in collaboration with Ukrainian cyber security officials and private sector enterprises to defend against cyber attacks. Microsoft's ongoing, daily engagement establishes that the cyber component of Russia's assault on Ukraine has been destructive and relentless.

The purpose of this presentation is to provide insights into the scope, scale, and methods of Russia's use of cyber capabilities as part of the largescale "hybrid" war in Ukraine, to acknowledge the work of organisations in Ukraine defending against persistent adversaries, and to provide strategic recommendations to organisations worldwide.

Presenter:
MICHAEL RICHARDS

CYBER CRIME, INTELLIGENCE AND POLICING
10:45 AM – 11:25 AM
NORTH BALLROOM

PERTHSEC

AISA
Cyber | smart · safe · secure

Cyber security resilience: Playing an infinite game requires preparation, adaptation and endurance

It is surprising how many organisations do not have an incident response plan or have a plan that's underdeveloped. According to a survey by Ponemon, 77 percent of respondents say they lack a formal incident response plan applied consistently across their organisation, and nearly half say their plan is informal or non-existent. Among those that do have plans, only 32 percent describe their initiatives as mature.

What's clear is this, what is ahead of us is an ever evolving threatscape with no clear end, continued investment in people, technology and process is involved to stay ahead. IBM's 2022 Cost of a Data Breach Report, based on its analysis of data breaches experienced by 550 organisations globally between March 2021 and March 2022, found the average cost of a data breach reached a record $4.35 million. Organisations who had tested Incident reponse plans were able to reduce the total cost and breach time.

This session will explore:

- Why are we "hardwired" to avoid planning for a cyber crisis? and how do we overcome the blindspots?
- How do we build a team to lead in a crisis?
- How do we use technolgy to protect, defend and respond?
- How do we build personal resilence for the inevitable?

This session will provide tactical tips and stories to prepare, respond and recover.

Presenter:
VANNESSA VAN BEEK

CYBER SECURITY, INCIDENTS AND TECHNOLOGY
10:45 AM – 11:25 AM
SOUTH BALLROOM

PERTHSEC

AISA
Cyber | smart · safe · secure

Securing your IaC with automated governance and policies

Infrastructure as code (IaC) is the managing and provisioning of infrastructure through code instead of through manual processes and seems scary because it's an automated process that creates, updates or edits infrastructure. Things can go wrong making the worst case scenario of deleting infrastructure but consider the alternative - a human manually managing your infrastructure, which is a time consuming and costly manual process.

When you take the human element out of the equation, then we can ensure a number of checks which can be deployed and never be skipped. So how do we govern IaC and make it more secure? Firstly, we need to take into consideration that we are not looking for security vulnerabilities but misconfiguration of IaC. We want to check the configuration for mistakes and stop anything that should be allow to happen, like using a specific region in the cloud.

What else can we do to ensure the end user can safely create infrastructure without creating issues, it's all about code and automation! So how can it help, by following an automated process such as: Code -> PR -> CI -> Review -> deploy to development/non-prod/staging. In this presentation we will discuss the management of securing IaC with an automated process which is governed by policies and procedures.

Presenter:
SIMON GRZEBIETA

GOVERNANCE, RISK AND STRATEGY
10:45 AM – 11:25 AM
CENTRAL BALLROOM

PERTHSEC

AISA
Cyber | smart · safe · secure

The Cyber Avengers

Did you know that:

1. Australians report cyber security incidents to cyber.gov.au every 10 minutes
2. 84% of Australian small businesses have adopted online services and rely on up to 30 separate technologies
3. 19% of small businesses spent $0 on cyber security over the past 12 months
4. Less than 15% of small businesses have paid for outside cyber security help in the past 12 months AND
5. Two-thirds of respondents (61.5%) reported that they had not experienced, or are unaware of, any cyber security incident occurring in their business!

While these stats are alarming, most organisations already have the staff who can help protect against cyber attacks, just not the know how! In this presentation we unveil the new superhero - The Cyber Avengers and discuss the following:

- Who are the Cyber Avengers? (any technical or non-tech staff/employee in an organisation)
- What role cyber avengers play in any cyber incident response process of any organisation (vigilance, following the cyber standards, reporting, lessons learnt etc.)
- Crafting your Cyber Incident Response Plan
- Using the Optus incident as an example we explore:
  - What has been stolen
  - What happens to the stolen information?
  - How that stolen data could be used against us
  - What we can do and government recommendations

Presenter:
SHEAVY KAUR

CYBER CRIME, INTELLIGENCE AND POLICING
11:30 AM – 12:10 PM
NORTH BALLROOM

PERTHSEC

AISA
Cyber | smart · safe · secure

Either you run the day, or the day runs you: Incident Response Plan recommendations from the front lines

It’s Friday afternoon and your Security Operations Centre identifies a backdoor beaconing to an unknown IP address from your server environment. It is up to your team to execute on your Incident Response Plan to investigate and remediate the threat.

Over the coming weeks of incident response, there are critical decisions that must be made which will impact the time to scope and remediate the intrusion. Some of these decisions are not considered in many organisation’s Incident Response Plans (IRP).

Barnaby Skeggs has been a lead incident responder at Mandiant for 4 years, in which time he has responded to the infiltration of bank ATM networks and SWIFT foreign transaction systems, nation state backed espionage, intellectual property theft and ransomware attacks where millions of dollars are lost in downtime every day. In this non-technical presentation Barnaby will share many of the roadblocks that have impeded an organisation’s ability to respond by days or weeks whilst under targeted cyber attack or ransomware.

You will leave this presentation with ideas to improve your IRP.

Presenter:
BARNABY SKEGGS

CYBER SECURITY, INCIDENTS AND TECHNOLOGY
11:30 AM – 12:10 PM
SOUTH BALLROOM

PERTHSEC

AISA
Cyber | smart · safe · secure

Five Critical Controls: Pragmatic advice for resilient OT systems

Join Rowan as he introduces the Dragos ‘5 critical controls for world class OT cyber security’. He’ll draw on a wealth of operational experience to provide practical examples of how each control can be implemented safely and effectively.

Each year, Dragos analyst conduct hundreds of assessments against critical infrastructure assets around the world. Despite the industry changing rapidly through new regulation, technology, and threats, there are a few key issues which appear and re-appear across the world. In the ‘2021 Year in Review’, Dragos identified 5 critical controls to address these issues, establish world class cybersecurity, and improve operational environment resiliency.

While knowing where to focus is half the battle, knowing how and when to change can be just as challenging for operational environments. Rowan will pragmatically dissect each of the five controls, and provide practical examples of basic, good, and advanced application in real world environments. This won’t be a collection of anecdotes or war stories, bring a notepad and your best questions for someone who has ‘been there, tripped that’!

Finally, each of the controls will be considered against the changing Australian critical infrastructure regulations (SOCI) and Australian Energy Sector Cyber Security Framework (AESCSF) for commonality and pitfalls.

Presenter:

ROWAN MACFARLANE

GOVERNANCE, RISK AND STRATEGY

11:30 AM – 12:10 PM

CENTRAL BALLROOM

PERTHSEC

AISA
Cyber | smart · safe · secure

Cyber-CPTED: Addressing new crime forms beyond conventional cyber security and physical security

There is widespread emergence of new crime forms combining cyber and physical attacks that are outside conventional cyber security and physical security. Many of these crime use legitimate digital processes, and even use the implemented cyber security measures, alongside physical strategies to commit them.

In this presentation, Dr Terence Love outlines why this new area of criminality and security is significant in both urban and rural societies. He describes 6 examples of such cyber physical crime methods and outlines practical strategies to address them. The presentation concludes with a pointer to a new, novel and more generic cyber security approach.

Presenter:
DR TERENCE LOVE

CYBER CRIME, INTELLIGENCE AND POLICING
1:15 PM – 1:55 PM
NORTH BALLROOM

PERTHSEC

AISA
Cyber | smart · safe · secure

Cyber exercising: Strengthens resiliency in the face of increasing cyber threats

Just having a cyber resilience strategy in place is not enough. With constantly evolving business risk landscape, an effective exercising program can be a critical success factor in developing and enhancing preparedness for a cyber attack.

Organisations need to be able to detect and respond quickly and effectively to a cyber incident to reduce the financial, operational and reputational harm it can cause. Having effective cyber security and robust incident response plans and procedures in place is therefore crucial, as is the team's ability to follow them.

Cyber incident exercising helps organisations to establish how resilient they are to a cyber attack, and practice their response in a safe environment. Exercising also helps create a culture of learning within an organisation, and provides an opportunity for relevant teams and individuals to maximise their effectiveness during an incident.

This session is all about why, what and how to test your organisation's cyber resilience.

Presenter:
VIDHU BHARDWAJ

CYBER SECURITY, INCIDENTS AND TECHNOLOGY
1:15 PM – 1:55 PM
SOUTH BALLROOM

PERTHSEC

AISA
Cyber | smart · safe · secure

Kubernetes security - A layered approach to securing production runtime

Today, many organisations are greatly simplifying their code-to-customer journey by building internal technology platforms powered by Kubernetes. Folks are adopting modern DevOps practises like GitOps, IaC, CI/CD to deliver customer value often and at a fast pace. But Kubernetes is not secure by default and more often than not the vanilla installation can drastically compromise the risk and security posture resulting in increased risk of exposure.

In this presentation, we will look at a layered security model for Kubernetes and touch on native must have k8s objects and configuration, eBPF based open-source tooling and finally cover off the recent developments in supply chain security that can apply to Kubernetes.

Presenter:
PRATEEK NAYAK

GOVERNANCE, RISK AND STRATEGY
1:15 PM – 1:55 PM
CENTRAL BALLROOM

PERTHSEC

AISA
Cyber | smart · safe · secure

Nobody: The collection, use and sharing of data both lawfully, unlawfully, and everything in between!

In this presentation, we will discuss the collection, use, sharing and storage of data both lawfully, unlawfully, and everything in between! The title (nobody) is a trifecta approach. The first is the collection of data that identifies everyone but nobody in particular. The second is the discussion of law that focuses on social policy but nobody in particular. And last is the cyber criminal who is nobody but someone of interest.

We will cover some common tools used in data collection, discuss the type of data collected, highlight the risks associated with data collection and talk about current law, together with gaps, around data collection.

The objective of the discussion is to raise awareness about data protection and law while educating the audience on applicable steps they can take for themselves and the company they represent. After all, what would happen if you did not delete inessential data on Tuesday?

Presenter:
BRENDA VAN RENSBURG

CYBER CRIME, INTELLIGENCE AND POLICING
2:00 PM – 2:40 PM
NORTH BALLROOM

PERTHSEC

AISA
Cyber | smart · safe · secure

Beyond vulnerability and threat management - Is your business truly managing its risks?

The emergence of two key cyber security management domains in Critical Infrastructure and Operational Technology has provided a significant increase in the ability to plan, detect and respond to threats. These are Vulnerability Management and Threat Management. However, the story can’t stop there. The job isn’t done.

Senior management who make the business decisions still suffer from the context gap and lack of visibility of what is truly happening in their business and on their terms. How do we bridge that gap and connect the parts of the business together, top to bottom, from technology to the actual real physical business operations? So that cyber security actions and reactions are quantified with common business language and aligned with business risk management principles.

Presenter:
MARK STEVENS

CYBER SECURITY, INCIDENTS AND TECHNOLOGY
2:00 PM – 2:40 PM
SOUTH BALLROOM

PERTHSEC

AISA
Cyber | smart · safe · secure

Hell in a sell - Wrestling for Executive buy-in

In this presentation, we will cover how cyber security teams can effectively gain better buy-in from the executive and gain more funding for their programs. It will explain how the importance of security awareness and training programs can be communicated as well as why your team needs the money and resources it needs in order to prevent cyber attacks.

We will covering the following:

- The importance of driving cultural change in organisations as a way to instill better cyber security practices and policies
- Executive buy-in can only be accomplished by effective communication and driving the narrative behind the WHY of cyber

Presenter:
SIMON CARABETTA

GOVERNANCE, RISK AND STRATEGY
2:00 PM – 2:40 PM
CENTRAL BALLROOM

PERTHSEC

AISA
Cyber | smart · safe · secure

Application control is hard lessons learned from the trenches

Many organisations have been given a mandate to adhere to the Essential Eight, often with little to no understanding of what is required to achieve even the first level of maturity.

Attend this session to learn from my mistakes in implementing Application Control in a large government environment with many stakeholders, requirements and PROBLEMS.

Windows Defender Application Control was chosen due to it being included with Windows 10 Enterprise and due to guidance from the Digital Transformation Agency Blueprint, integration with existing security products, and inclusion with the Windows license.

Learn through sharing my story of this project how you can avoid issues, plan appropriately, and evaluate whether your environment is mature enough to enable a successful Application Control project.

Presenter:
GEORGE COLDHAM

CYBER CRIME, INTELLIGENCE AND POLICING
2:45 PM – 3:25 PM
NORTH BALLROOM

PERTHSEC

AISA
Cyber | smart · safe · secure

Mastering the must-dos to operationalize data protection

Building trust with customers doesn't have to be difficult, but it has to be a deliberate and sustained focus. To address today's key security challenges, meet compliance regulations, and accelerate digital transformation initiatives, enterprises need to learn how to operationalize enterprise data privacy programs and build an enterprise data protection framework.

Join this session where we'll discuss today's challenges in operationalizing data protection and how to overcome them:

- Protecting corporate and consumer data
- Meeting compliance mandates like GDPR, PSD2, KYC, etc.
- Securing virtualized and cloud infrastructure
- Enabling a secure, productive workforce



Presenters:
DOROTHY PRAGA, REBECCA VINCENT & TARYN EARNSHAW

CYBER SECURITY, INCIDENTS AND TECHNOLOGY
2:45 PM – 3:25 PM
SOUTH BALLROOM

PERTHSEC

AISA
Cyber | smart · safe · secure

Post pandemic risk - Managing the ever increasing cyber risk landscape, when it's dwarfed by other global risks

For many years, cyber security has been the largest man made risk. It still is, but in the 2022 World Economic Forum Risk Report it's the first time this risk hasn't made the top 10.

In this presentation, we will look at the impact of the rise of global social risks on cyber security, explore the strategies to manage these risks and lastly how to communicate to an executive audience who is bombarded by new global risks daily.

Presenter:
ANDREW PHILP

GOVERNANCE, RISK AND STRATEGY
2:45 PM – 3:25 PM
CENTRAL BALLROOM