BRISSEC

AISA
Cyber | smart · safe · secure

Can on-screen cues activate risk recognition? A criminological perspective

With traditional crimes, an offender and their victim must converge in a physical time and space for the crime to occur. However, technology has created a virtual environment which easily connects one motivated offender to numerous potential victims; this has placed an increased onus on individuals to engage in protective behaviours when online. This presentation takes a human factor focus and will consist of two parts: 1) a criminological overview of theories on victimisation, crime prevention, and behavioural responses; and 2) an examination of the results from a pilot study that uses eye-tracking software to measure how people interpret, and respond to, phishing emails containing different situational cues.

The first part of this presentation examines key criminological and behavioural theories, and how they relate to both physical and cyber crime. In a virtual environment, situational cues may be lacking or users may be less aware of threat indicators. This may impact our ability to protect ourselves against cyber threats.

The second part of the presentation examines the preliminary results of a randomised-control cyber victimisation pilot study. The study uses eye-tracking technology to better understand where people look to determine the validity of an email and seeks to measure the impact embedded situational cues have on threat recognition and protective behaviours. The results of the study indicate disparities between physical and cyber threat responses. This has implications for several tactics currently used to target phishing.

Presenter:
KELSY LUENGEN

HUMAN FACTORS
10:45 AM – 11:25 AM
BALLROOM A

BRISSEC

AISA
Cyber | smart · safe · secure

Brain Machine Interfaces: New vectors for cyber attack

Brain Machine Interfaces (BMIs) are devices that act as intermediaries between human thought and machine action. While research has traditionally focused on enabling patients with spinal cord injury to communicate or control a prosthetic limb, over the last decade many companies have been investing in BMI technology for a much broader range of applications. BMIs employ a pipeline that traverses hardware, software and machine learning layers, each of these introducing vulnerabilities that could be exploited by an adversary.

Like many other computing and IoT devices, emphasis of BMI development has been on improving accuracy and efficiency, and less on the security of the device or its algorithms. Specifically, adversarial machine learning is a field growing in prominence that represents the ability to 'hack' machine learning algorithms by poisoning data sets imperceptibly before training, by evading classification, or by hijacking the model's function to make it do something it wasn't intended to. Potential attacks in the BMI domain could include a prosthetic limb making an action that wasn't intended, a drone changing course or crashing itself, or sensitive information being breached.

This presentation outlines the presenter's PhD research on cyber security in BMIs, specifically on their vulnerability to adversarial machine learning attacks.

Presenter:
HARRIET FARLOW

TECHNICAL: RED, BLUE – WHAT COLOUR ARE YOU?
10:45 AM – 11:25 AM
REDLANDS ROOM

BRISSEC

AISA
Cyber | smart · safe · secure

Bringing down public infrastructure to cripple a nation

In this session, Ashwin Ram will shed light on cyber attacks against a nation, with the sole purpose of bringing its public infrastructure to its knees. This attack campaign successfully crippled Iran's Railway Network, then destroyed computer systems of Iran's Ministry of Roads and Urbanization, disrupted Gas Stations across the country, breached Prison Security Cameras, hacked Airline and hijacked the country's broadcast signals.

The attacks were conducted not by another nation state, but a relatively unknown and not so well funded hacktivist group. The key message is that these attacks could have just as easily been against public infrastructure in Australia, U.K, the U.S or any other part of the world. Ashwin will share what the threat actor did, and how you can take steps to prevent this type of attack or at least minimize the damage.

The Check Point Research team, focused on reverse engineering nation state cyber attacks, conducted this research.

Presenter:
ASHWIN RAM

COPS AND ROBBERS: GRC & CYBER CRIME
10:45 AM – 11:25 AM
BALLROOM C

BRISSEC

AISA
Cyber | smart · safe · secure

Positioning your cyber security program for success

Frustrated by trying to get a security program off the ground, or re-energising a stalled program?

In this presentation, Chris will share critical factors to position a security program for success. Chris will draw on his experience in establishing and leading security programs to provide practical examples to help you succeed in the corporate environment.

Chris will discuss the following:
- How to communicate a strong vision in business terms
- How to generate sponsorship and buy-in
- How to work the ‘corporate machine’
- How to maintain focus in a noisy corporate world

The session is not technical in nature and is focused on the discipline of security management.

Presenter:
CHRIS PENNYCUICK

HUMAN FACTORS
11:30 AM – 12:10 PM
BALLROOM A

BRISSEC

AISA
Cyber | smart · safe · secure

Rethinking the purpose of cyber defense: What are we doing wrong and how we can be more effective

In the military, the doctrine is that the purpose of defense is not just to protect assets, but to destroy the enemy on the ground of our choosing. The traditional approach to information security only thinks about manning the barricades and has no plan to win the cyber-battle.

In this presentation, Duncan will challenge long-held orthodoxies about what good cyber security looks like, and how new approaches such as active defense need to be central of how an organisation thinks about their security architecture. He will develop a concept about how we can fight the battle against hackers where the end result is not the defeat of an organisations defenses and the loss of key assets. He will then look at what this means in terms of cyber security capabilities and architecture.

Presenter:
DUNCAN UNWIN

TECHNICAL: RED, BLUE – WHAT COLOUR ARE YOU?
11:30 AM – 12:10 PM
REDLANDS ROOM

BRISSEC

AISA
Cyber | smart · safe · secure

Protecting people, processes and technology

We read about security breaches on a daily basis, but what do we actually know about these cyber crime groups? How do they conduct their attacks and what are the best practices to protect ourselves and our businesses against them? Understanding the threats your organisation faces may make the difference between preventing or mitigating breaches and suffering a worst case scenario.

In this session, we will review security issues with people, process and technology, examine how threat intelligence can be used to identify social engineering attacks, and review some of the latest attacks seen in the wild. The session will close with how to operationalise threat intelligence using security frameworks such as MITRE ATT&CK framework in conjunction with cyber threat intelligence best practices.

Key takeaways for the audience:

- Real-world examples of how threat intelligence can help you reduce risk and improve your incident detection capabilities
- How to create or transform your threat intelligence program with the simple Intelligence Cycle
- Tips for integrating threat intelligence into your day-to-day detection, response, and overall risk management operations

Presenter:
RICHARD STOCKS

COPS AND ROBBERS: GRC & CYBER CRIME
11:30 AM – 12:10 PM
BALLROOM C

BRISSEC

AISA
Cyber | smart · safe · secure

Human impacts of ransomware attacks

The impact the internet has on our daily lives is unquestionable. It provides a platform for communication, e-commerce and interactions between individuals and organisations around the world. As cyber space grows in prominence, the number of cyber attacks also increase each year. In particular, the number of ransomware attacks, whereby cyber criminals use sophisticated methods to attack organisations' networks and encrypted data, are also reaching a record high.

Organisations and governments are often keen to examine the financial loss and disruption to services caused by ransomware attacks. However, the significant and wide-ranging short and long-term social and psychological impacts on victims are often overlooked. In this presentation, Joseph will explore the psychosocial impacts of ransomware attacks. As well as discuss the importance and need for further studies, in developing a standardised measurement tool to provide a comprehensive understanding of the damage caused by ransomware attacks on the government, organisations, society and individuals.

Presenter:
JOSEPH CHENG

HUMAN FACTORS
1:15 PM – 1:55 PM
BALLROOM A

BRISSEC

AISA
Cyber | smart · safe · secure

Scanning millions of domains and compromising the email supply chain for hundreds of Australian organisations

Curious to find out what happens when you perform OSINT at-scale? In this presentation we will discuss how a seemingly innocuous scan of 1.8 million Australian domains resulted in the email supply chain of 264 Australian organisations being compromised. We will then discuss how the migration of email infrastructure from private to public cloud environments has significantly elevated the risks associated to IP takeover attacks and how these attacks are practically performed.

The following topics will be discussed:

- What phishing is, how it has evolved and how an overlooked technique can be exploited to tip the table in favour of attackers
- How email sender authentication is performed, how public cloud environments are ephemeral in nature and how trusted but unused IP addresses can be taken by threat actors with malicious intent
- Methods used to collate a target list that includes millions of domains
- What's involved in extracting the full IP supply chain of an SPF record and the infrastructure necessary to scan millions of targets
- What's involved in cycling through tens of thousands of IP addresses
- Process for cross referencing scanned AWS IPs against a repository of known SPF IPs
- How each of the affected organisations and their downstream customers are significantly more susceptible to business email compromise and phishing-related attacks

Presenter:
SEBASTIAN SALLA

TECHNICAL: RED, BLUE – WHAT COLOUR ARE YOU?
1:15 PM – 1:55 PM
REDLANDS ROOM

BRISSEC

AISA
Cyber | smart · safe · secure

Enhancing incident response in the Cloud with a real-time understanding of cyber risk

The seismic shift to the cloud continues at an ever accelerating pace across the globe. The benefits are unquestionable – infinite scalability, lower capital costs and rapid access to game-changing technology. Mature adopters of cloud-based DEVOPS are already performing thousands of 'go-lives' every week, and many businesses have publicly reported double digit decreases in IT infrastructure spend. However, just as benefits realisation requires planning and focus, so too does the mitigation of cyber risk in the cloud. One peril to avoid is not utilising the rich data from your multi-cloud instances to enhance your security posture.

In this presentation, Dirk and Adam will discuss the ways to maximise your readiness for incident response when a cyber-attack happens. Dirk and Adam will use a case study of a recent attack on a US cloud services provider (Cloudstar, July 2021), as well as some of the other prominent cyber incidents from 2021 to explore how incidents in the cloud are different to those that occur on-premise. They will also apply the SANS incident response framework to zero in on what response organisations need to do differently in each phase of an incident to get the best results in the cloud. In particular, the need to invest time upfront, and on an ongoing basis, in the 'preparation' phase will be covered in some detail, including techniques to identify and minimise cloud supply chain risks to avoid them ever becoming incidents.

Presenters:

DIRK HODGSON & ADAM GREEN

COPS AND ROBBERS: GRC & CYBER CRIME

1:15 PM – 1:55 PM

BALLROOM C

BRISSEC

AISA
Cyber | smart · safe · secure

Threat hunting: A human solution to a human problem

In the face of ever-increasing cyber security attacks, technology alone is not enough to identify and disrupt adversary behaviour. Humans play a pivotal role in the hunt for these threats; identifying and analysing malicious artefacts or events that may have otherwise bypassed traditional security tooling. In this presentation, we will explore the anatomy of a real campaign, identifying how the human factor played a fundamental role in the fight against a highly motivated adversary.

Topics covered include:

- Threat hunting fundamentals, methodologies and misconceptions
- What makes human driven threat hunting successful, and why the human factor is important
- The anatomy of a hands-on intrusion campaign being run and executed by human actors
- Case study: how human threat hunters uncovered and prevented an attack by a state-nexus (or eCrime) adversary

Audience learnings and takeaways:

- Understand the importance of a human-led threat hunting capability
- Demonstrate how human expertise plays a fundamental role in the identification and disruption of adversary behaviour, and why it must augment technological solutions (or, why we can't rely on technology alone)
- Understand why speed is important in the face of increasing adversary capability

Presenter:
KERAYOF BENJAMIN

HUMAN FACTORS
2:00 PM – 2:40 PM
BALLROOM A

BRISSEC

AISA
Cyber | smart · safe · secure

What the CVSS is EPSS?

Patching vulnerabilities with limited resources requires a risk-based approach. The less resources available, the riskier a patch management program will be to run. Vulnerabilities, have industry tags to assist in telling the impact of a vulnerability. The Common Vulnerability Scoring System (CVSS) does assist, but does not answer the other side of the risk equation, being the probability of an exploitation of the vulnerability. The Exploit Prediction Scoring System (EPSS) tries to answer this.

In this presentation, we will discuss how EPSS is calculated, where can you get the score, how you can verify the EPSS score and whether CVSS combined with EPSS provides a timely picture to coordinate a risk-based patch management program.

Presenters:
GEOFFROY THONON & MARCUS SCHULL

TECHNICAL: RED, BLUE – WHAT COLOUR ARE YOU?
2:00 PM – 2:40 PM
REDLANDS ROOM

BRISSEC

AISA
Cyber | smart · safe · secure

The Integrated Security Model: Security beyond just cyber

In today's hyper-connected and digital world, organisations must think broadly about their security operating model and how they can best use the data across all security related functions to ensure that their customers are protected and that thier organisation is cyber resilient.

In this presentation, we will explore the evolution of the integrated secuirty model which brings togther multiple security related functions, including but not limited to, cyber security, fraud, physcial security and crisis management.

The following topics will be discussed:
- The benefits of the integrated security model
- Operatiing model considerations
- What role does the Fusion Centre play?
- How should organisations start their journey?

Presenter:
DAVID FAIRMAN

COPS AND ROBBERS: GRC & CYBER CRIME
2:00 PM – 2:40 PM
BALLROOM C