TEG7

PULSE CONFERENCES

Cyber Attacks – The Risk and the Fix

25-26 April 2018
Dubai, United Arab Emirates

North Cyber advises that this course is suitable for any officials in government, business, critical infrastructure, banking, transportation, energy, shipping and ports, retail, leisure, police, intelligence and security operations whether government or private sector. The case studies and work will be drawn from Europe, Africa, Middle East and South Asia depending on the persons attending and the region where the course is delivered.

Over two days, delegates are shown the reality of just how easy real cyberattacks can be - even those with the most devastating effects - and the implementation of simple measures to avoid catastrophic risk. The course is suitable for entirely non-technical officers as well as cyber managers and administrators who wish to develop a sound understanding of just how easy and low-tech the efforts of an attacker can be, and how to implement mitigation or who wish to upgrade their existing skills to become more cost effective for their organisation. The practical elements are comprehensively taught in a walk-through manner to demonstrate the vulnerabilities in realistic targets. A key theme running through the course is that of workforce vulnerability – no matter how well defended the organisation's intellectual property is, the staff are the way in.

Day One - The Risk

Focuses on the mindset and techniques of the attacker, whether a cybercriminal, a state actor, a corporate spy or frivolous hacker. Students are equipped with tools and techniques to perform investigations of targets in the preparation for a notional attack, essentially becoming the hacker to demonstrate just how easy those attacks often are due to the visibility of staff and corporate data online.

Introduction to Cyber Risk

- "It's not about the tech" - why the attackers' techniques are surprisingly low-tech, and why the information security risk lies with the human workforce, not their computers.
- Real world examples of catastrophic attacks and the vulnerabilities in every organisation.
- One size fits all - the common vulnerabilities used by any attacker against any target: corporate, government and personal.

Attacker Methodology

Part One – reconnaissance

Scoping a target. A practical module demonstrating to delegates how an attacker uses OSINT (open source intelligence) to obtain corporate data and personal details using nothing more than search engines and free, legal tools.

Part Two – Attack

- Compare and contrast of 'technical' attacks with low tech and no-tech hacking by social engineering.
- Teach a man to phish. Understanding the myriad ways an attacker uses the freely obtained data to quickly penetrate an organisation through simple influence.

The Persistent Threat of Leaked Data

The permanent threat to corporations that arises from leaks of staff data from breaches such as Yahoo - even when non-corporate in nature, and even when many years old. Delegates are show the surprising amount of leaked data online and what to do about it.

Wi-Fi - the Corporate and Personal Risk

The largely unknown risks of wi-fi, not only as a vehicle for corporate intrusion by attackers but also for tracking the physical movement of individuals and identifying their homes. A practical module in which students are walked through the steps of an attacker breaking into corporate wi-fi and tracking of staff members using freely available tools.

Day Two - The Fix

Focuses on mitigating the identified risks. Real world examples of damaging attacks are dissected, with particular emphasis on correct implementation of cyber incident response. Delegates are presented with the most effective measures to mitigate an attack to bring a business back online at minimum expense.

Exercise: Attack the Corporation

WHAT HAPPENS NOW? - The reality of an attack, and the art of incident response.

The Devastation

Lessons learned from a vast number of cyber incident responses, where basic lack of security procedures and response plans allow simple attacks to have catastrophic effect.

Mitigation

From lessons learned in the 'attack methodology' modules and further illustrated in 'What happens now?' we explore the steps to secure the company. Again, the technical aspect is secondary to the information and 'human' security.

- The technical penetration test - learning why most companies waste time and money with incomplete or ineffective testing.
- Cyberattack response plan - The blueprints of the towering inferno. Why you must engage with your incident responders BEFORE an attack, and why incident response should cost thousands not millions.
- Staff data - reducing the target surface by educating the workforce in simple, effective ways that require no technical knowledge.
- Threat intelligence - the utility and strengths of currently available threat intelligence systems.
- 'Convenience is an attack vector. ' Overcoming perceptions of inconvenience by removing certain technical privileges to maximise information security and aiming to become hack-proof.

About the instructor:

North Cyber Limited

North Cyber are team of former intelligence officers with expertise in covert online operations and digital forensics. The company teaches government and corporate clients how find and fix the unseen holes in their security. They specialise in all levels of capability including low-tech and no-tech hacking, using freely available information to circumvent vastly expensive but ineffective security systems. The teaching draws on many and varied real-world examples from the private and government sectors, from the perspectives of the attacker and incident responder. Participants in these courses will evaluate their own experience on the course in gaining additional skills and understanding of the threats to their organisation and they will gain confidence in tackling these catastrophic risks to the comparate or government operation.

Key information and registration

Course name: Cyber Attacks – The Risk and the Fix
Date: 25-26 April 2018
Location: Dubai, United Arab Emirates
Course length: Two days
Price: £1,500

Register for this course:

To register or find out more about this course please

email:sanna.lindstrom@pulseconferences.com