Cyber security Master Class.

Understanding and Managing cyber and digital risk

Hilary Walton, CISO Kordia, @hilswalton


10 REASONS WHY
400+
IN-HOUSE
TECH EXPERTS
65-YEAR+
HISTORY IN NZ
DEDICATED
CYBER SECURITY
& CLOUD DIVISIONS
24/7
NETWORK & SECURITY
MONITORING
LEADING
BUSINESS
ONLY
TELCO
CRITICAL
COMMUNICATIONS
TRUSTED
BY 1000+
CUSTOMERS
WE CARE:
NPS +60
AT THE FOREFRONT OF
CUTTING EDGE
TECHNOLOGY
BEST
CONNECTED
TO AWS & AZURE

@HilsWalton's Cyber Security Master Class

- Exploring the developing trends in cyber and ransomware attacks **(a.k.a understanding cyber security and why it's a big deal)**
- What role should risk professionals play in the managing cyber risk? **(a.k.a ever noticed it how difficult it can be to get assurance on an enterprise cyber security programme)**
- Understanding information management risk - delivering effective information governance **(a.k.a you can't have security without thinking about information/data)**
- What risk lessons can be learned from major recent breaches **(a.k.a best to learn from others than suffer them yourself)**
- Digital and cyber resiliency – preparing for the loss of digital systems and cyber attacks **(a.k.a an unpracticed plan ain't a plan)**

Understanding cyber security made easy


WORLD ECONOMIES (BY SIZE)
1 US
2 CHINA
3 CYBERCRIME
4 JAPAN
5 GERMANY
6 INDIA
THE RISING COST OF CYBERCRIME
$3 TRILLION
2015
$6 TRILLION
2021
$10.5 TRILLION!
2025
SPONSORED BY: INTRUSION
CYBERCRIME
MORE PROFITABLE THAN
GLOBAL DRUG TRADE
CYBERCRIME COSTS MORE PER YEAR THAN ALL NATURAL DISASTERS
RESEARCH BY
CYBERSECURITY VENTURES
CYBERSECURITYVENTURES.COM

Key Findings: Top 10 Risk List

Respondents have selected and rated 10 top risks that their organizations face today:

1 Cyber Attacks/ Data Breach	2 Business Interruption	3 Economic Slowdown/ Slow Recovery	4 Commodity Price Risk/Scarcity of Materials	5 Damage to Reputation/ Brand
6 Regulatory/ Legislative Changes	7 Pandemic Risk/ Health Crises	8 Supply Chain or Distribution Failure	9 Increasing Competition	10 Failure to Innovate/Meet Customer Needs

https://www.aon.com/2021-global-risk-management-survey/index.html

Australia,
May 2022

Company fined for inadequate Cyber Security risk management

by admin@extreme | May 13, 2022 | Security | 0 Comments

The role of company directors

1. Directors need to understand and approach cybersecurity as an enterprise-wide risk management issue, not just an IT issue.
2. Directors should understand the legal implications of cyber risks as they relate to their company's specific circumstances.
3. Boards should have adequate access to cybersecurity expertise, and discussions about cyber-risk management should be given regular and adequate time on board meeting agendas.
4. Directors should set the expectation that management will establish an enterprise-wide cyber-risk management framework with adequate staffing and budget.

Discuss in your tables for 5 mins:

- What role should risk professionals play in managing cyber risk?
- What are some of the challenges in doing so?
- What are some solutions?

Are we doing well? Or are we just lucky?

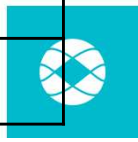
Table of Contents

Key Move #1: Get the business clear on the highest level of security Policy.

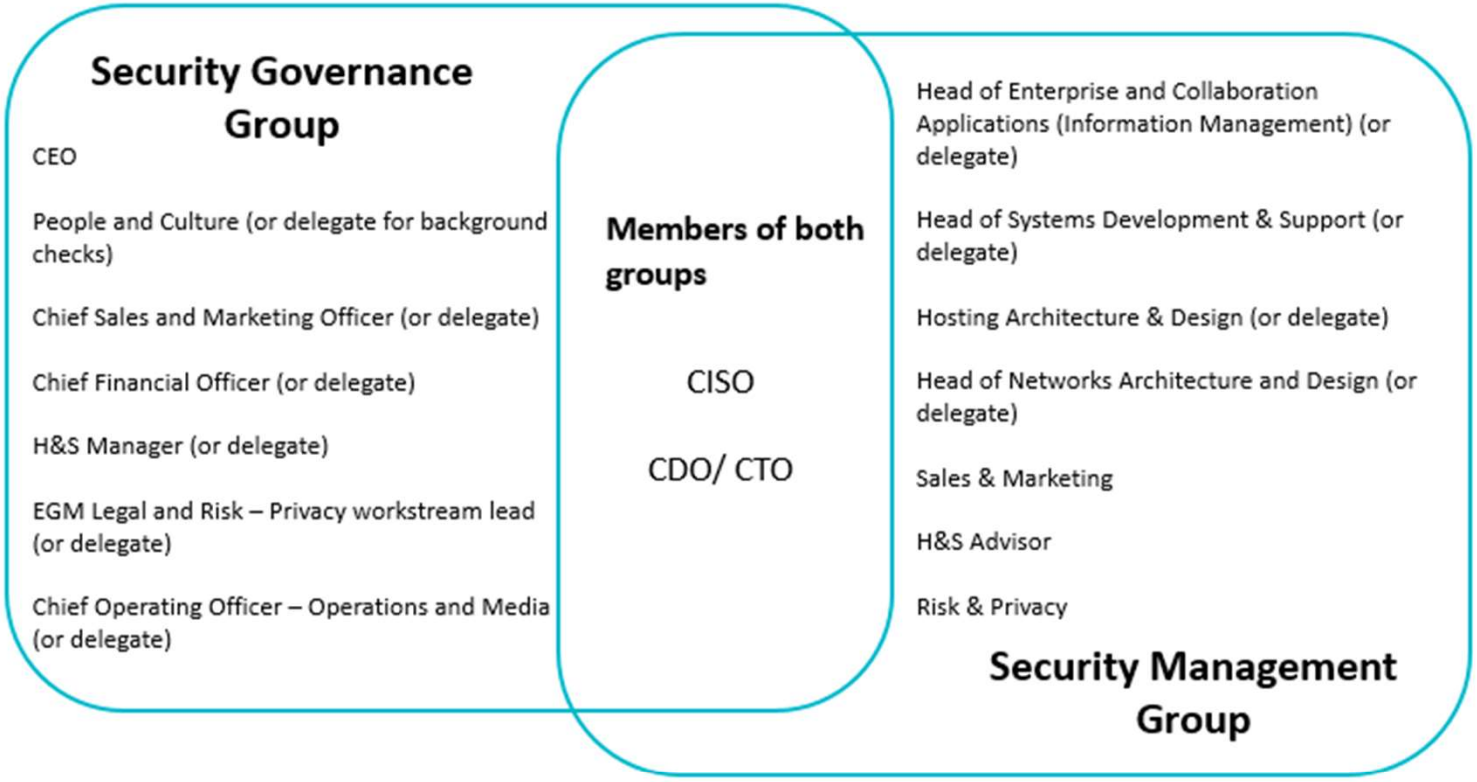
Enshrine in policy:
- security objective
- security principles
- roles and responsibilities

Security is everyone's responsibility, but it helps to be super clear on what that means

Roles	Responsibilities
All staff and contractors	
Managers and Leaders	
HR Team (Personnel security implementation)	
Property Management (Physical security implementation)	
Project Managers and other People who manage projects	
Legal	
Information Asset Owners	
Information Technology Security Managers	
Executive	
Board	
Risk team	



Key Move #2: Security Governance Arrangements

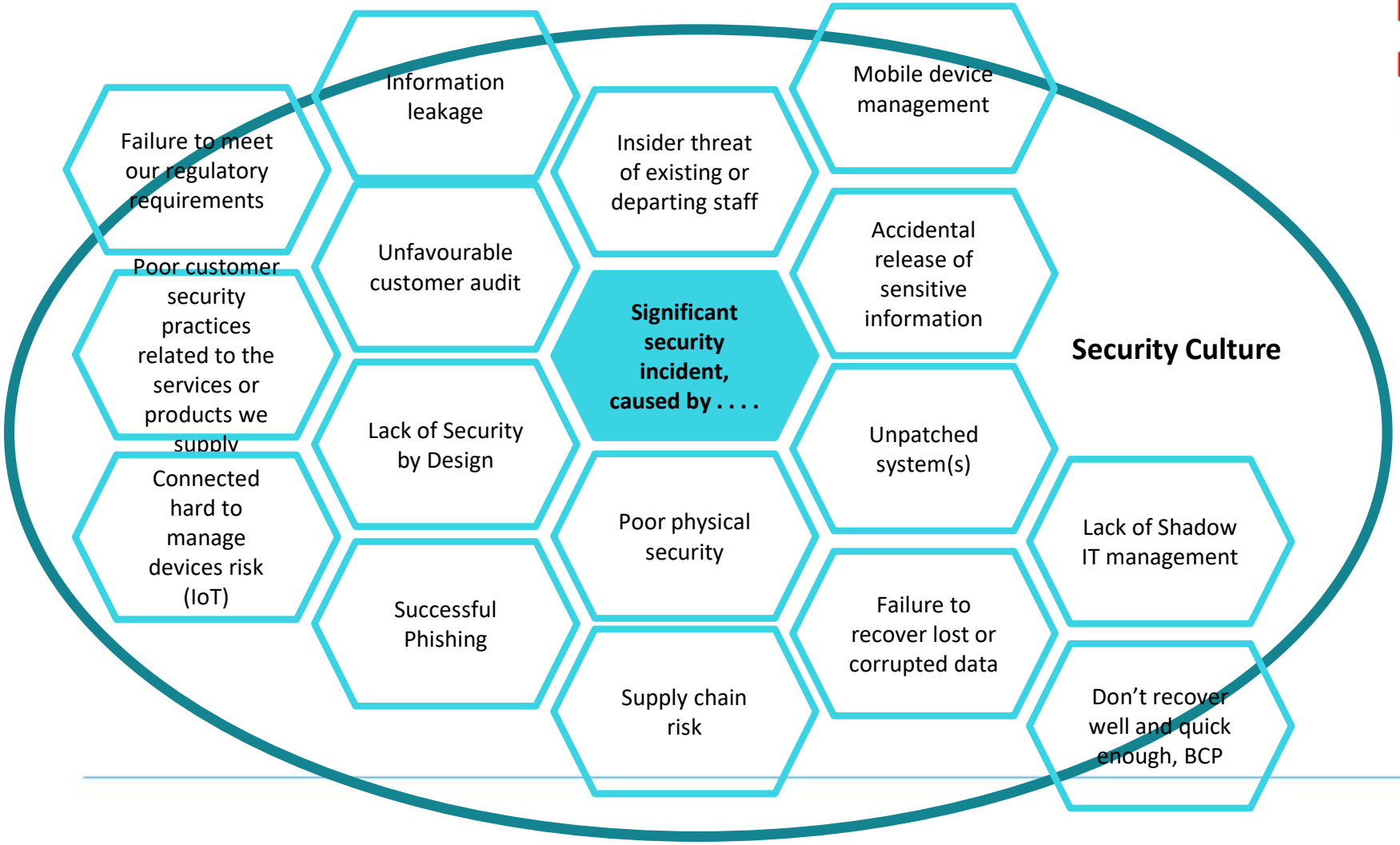


of all dimensions of Security Programme, including Information Security, Physical Security, Personnel Security, Privacy, Information Management, Disaster Recovery and Business Continuity.

#3

Identify your key assets – people, information, technology, facilities

Critical Security Risks – if we don't manage these risks, we have a problem

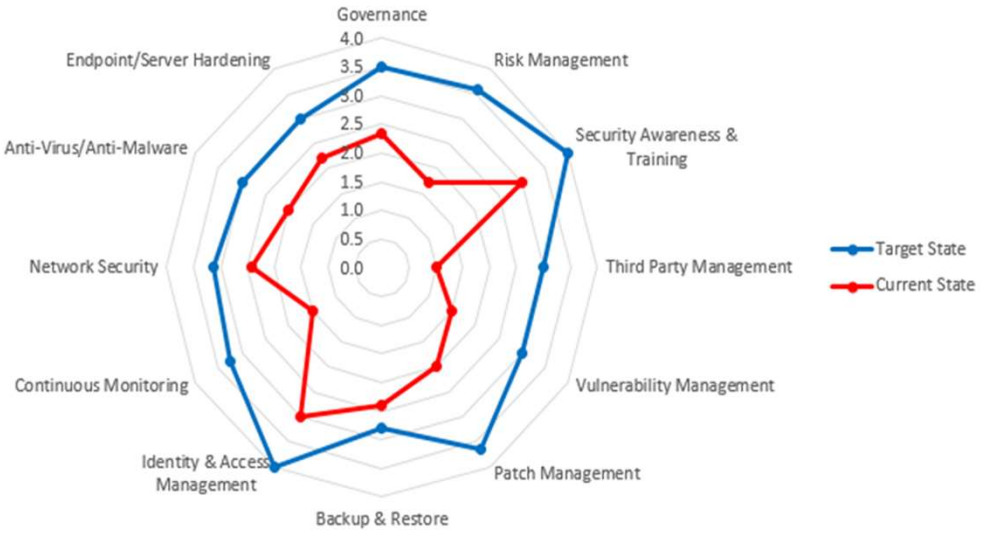


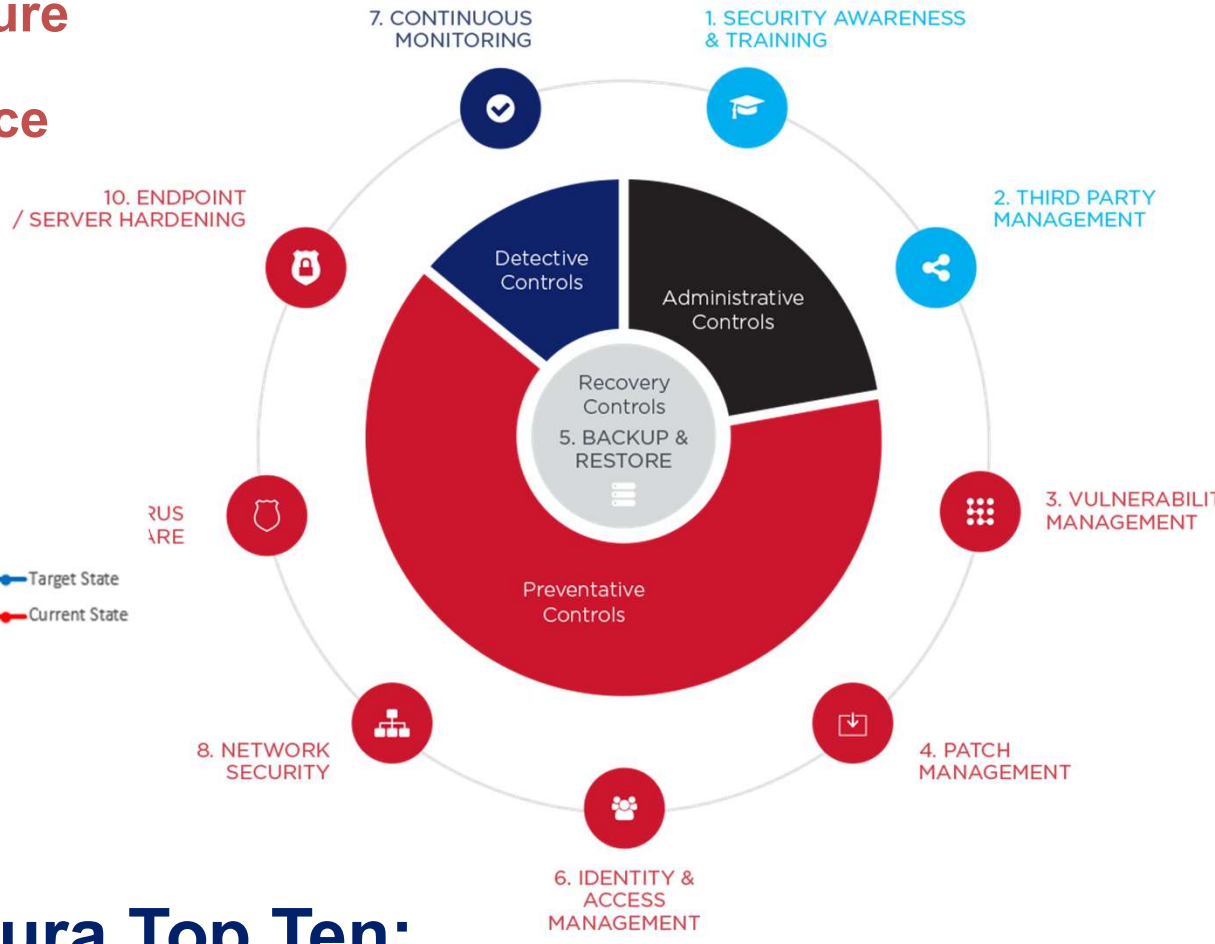
#4

- What risks are we missing?
- Anything else keeping you up at night?

5

Key Move #5: Measure Security Performance





Aura Top Ten:

Critical Controls & Mitigation Strategies

Aura Top Ten: Critical Controls & Mitigation Strategies

1. SECURITY AWARENESS TRAINING

Security education, training, and awareness for staff is a crucial activity. Often it needs to be tailored to suit the needs of an organisation, and further tailored to suit specific sub-sets of staff and IT users.

2. THIRD PARTY MANAGEMENT

In today's environment most organisations have many suppliers who have access to their systems and data. It is important to understand who they are, what they have access to, and what risk they pose to the organisation.

3. VULNERABILITY MANAGEMENT

Many compromises occur due to an organisation not knowing that they have an unpatched system in their environment. It is vital to continually scan all critical and boundary systems to understand if they contain known vulnerabilities.

4. PATCH MANAGEMENT

Closely tied to Vulnerability Management, all vulnerabilities and regular updates require updating , or 'patching', as soon as possible.

5. BACKUP & RESTORE

It is important for organisations to consider what they need to backup, how often they do so and where they store it. They then need to understand how to restore those backups in the event of ransomware attacks, deletions and disasters.

6. IDENTITY & ACCESS MANAGEMENT

It's vital that organisations ensure the correct people get the right amount of access to the right data. There are many processes to managing identities as people join, move and leave an organisation.

7. CONTINUOUS MONITORING

There is no way to know if you are under attack, or have been compromised, if you are not looking at the logs from your systems in a real-time fashion.

8. NETWORK SECURITY

Network security involves splitting up a computer network into smaller subnets. Granular controls can then be placed at these subnet boundaries to achieve greater control of any inter-VLAN traffic. It also involves using security tools to analyse the traffic for improper or unusual behaviour.

9. ANTI-VIRUS / ANTI-MALWARE

It's important to use software that makes use of heuristic analysis – this has the potential to detect previously unseen malware and, not just known threats. Other endpoint solutions can also augment security by preventing data loss, detecting intrusions or providing analytics and indicators of compromise.

10. ENDPOINT / SERVER HARDENING

Hardening is the process of securing systems by attempting to reduce the attack surface. This is achieved by removing unnecessary software and functions.

Key Move #6: Develop your security strategy

Security Strategy

- Co-developed with the business
- 3 year strategy
- Detailed roadmap for FY
- 1 pager PowerPoint for communication and business plan

Security 3 Year Plan on a Page – Execution View

		FY20/21 Strategic Initiatives	FY21/22 Strategic Initiatives	FY22/23 Strategic Initiatives
	Security Culture & Governance	• Secure senior level engagement • Develop and communicate clear roles and responsibilities • Review INFOSEC polices and standards, particularly Info Asset Management and Physical Security. • Further develop Secure By Design framework to ensure it is implemented, practiced and effective	• Include formal responsibilities in position descriptions • Continue review of INFOSEC polices and standards, particularly Supply Chain • Mature Secure By Design framework • Develop security risk management framework aligned to the Kordia Group Risk Management • Develop third party risk management strategy	• Include security objectives in senior managers at risk performance plans • Continue review of INFOSEC polices and standards • Secure By Design aligned to standard • Re-run Security culture survey every 2 years • Implement third party risk management strategy (into general contractor management processes) • Integrating security risk management with the Kordia Group Risk Management
	Educate	• Increase security policy awareness, train high risk groups, e.g. those dealing with Personally Identifiable Information (PII) • Enterprise use of a Password Manager • Formalise Security Champions	• Continue programme of training for high risk groups • Develop eLearning for general security policy awareness • Embed Security Champions • Embed security mindset into day to day life, not just work	• Develop and include security training in Kordia 'Digital Academy'
	Protect	• Develop policy and strategy for patching and security of equipment, products and services (IT and OT) • Implement key components of Information Asset Management • MFA everything	• Develop physical security baseline standard and increase levels based on risk profile of sites • Implement data classification controls and data loss prevention • Implement Privileged Access Management (PAM)	• Implement physical security baseline standard and increase levels based on risk profile of sites • Physical security centralized access control system
	Detect	• Develop event detection strategy • Implement phased USM Anywhere capability	• Implement event detection strategy • Further implement phased USM Anywhere capability • Develop or acquire tools to improve proactive and reactive threat detection	• Review event detection strategy • Further develop or acquire tools to improve proactive and reactive threat detection • Network access based on MDM compliance
	Respond & Recover	• Develop log retention strategy • Develop security incident exercise programme • Develop post incident analysis framework • Develop testing of backups programme, especially for KN • Prepare for mandatory privacy breach reporting	• Implement logging strategy • Implemented security incident exercises programme • Post incident analysis framework implemented • Increased testing of backups, especially for KN • Backup cloud environments • Implement mandatory privacy breach reporting	• Ongoing security incident exercises programme • Post incident analysis framework embedded

T

FY20/21 Strategic Theme 1: Security Culture & Governance

Key aspect to solve	Rationale (why do we need to solve this/ what is the value unlocked)	What needs to be done to deliver	How will we measure it
Secure senior level engagement	• The greatest influences on individual performance are the expectations of leaders to secure prioritisation and funding of the plan. • Security is most effective when leaders continually demonstrate their commitment and support for security through their words and actions.	• Develop, agree and publish security strategy in Business Plan • Develop, agree and publish overarching security policy/ charter • Define and formalise governance arrangements for security for Corporate and Customer operations	• Security culture survey results • Published overarching Security Policy • Formalised security governance arrangements through TOR implemented
Develop and communicate clear roles and responsibilities	• Clarity of roles and responsibilities helps people know what is required and what they are expected to do	• Develop, agree and publish roles and responsibilities. • Communicate via appropriate comms channels.	• Published overarching Security Policy containing roles and responsibilities. • Campaign delivered on this topic via different comms channels.
Review INFOSEC polices and standards, particularly Info Asset Management &, Physical Security.	• To ensure INFOSEC policy and standards reflect risk levels change • Policy/ standards should reflect practice in the organisation or are not effective.	• Review INFOSEC policy and standards one by one, consult and communicate when complete. • Info Asset Management, Classification, Supply Chain and Physical Security as priorities.	• Published INFOSEC policy and standards for: Info Asset Management Info Classification Supply Chain Physical Security Customer Operations
Further embed Secure- By-Design framework, to ensure it is implemented, practiced and effective	• To ensure security designed from the start and included throughout product, system or service lifecycle. • To avoid costly rework, errors, vulnerabilities, the right people engaged at the right time	• Review good practice Secure-By-Design frameworks, Aura to input • Identify and implement improvements to existing framework • Educate IT and OT people to ensure the right people are engaged, with the right capability to design	• Published Secure-By Design framework • Demonstrate it being in use

Lesson’s learned from cyber attacks

BBC Sign in | News | Sport | Reel | Worklife | Travel | Future | M

NEWS

Home | Video | World | Asia | UK | Business | Tech | Science | Stories | Entertainment &

Business | Market Data | Global Trade | Companies | Entrepreneurship | Technology of Busi

Travelex: Banks halt currency service after cyber-attack

By Joe Tidy
Cyber security reporter, BBC News

8 hours ago

Share

A number of High Street banks have stopped customers ordering foreign currency, following a ransomware cyber-attack on Travelex.

RNZ Home | News | Radio | Podcasts & Series | Topics | Pacific

New Zealand | World | Politics | Pacific | Te Ao Māori | Sport | Business | Country | Local Democracy Reporting

NEW ZEALAND / BUSINESS

LPM breach could have revealed thousands of people's data

4:57 pm on 16 July 2020

Share this

A design flaw in a property management firm's website meant potentially thousands of images of private customer information was publicly available.

NEW ZEALAND

Worldwide ransomware attack: St Peter's College and 10 other schools hit by US cyber attack

4 Jul, 2021 06:00 PM

3 minutes to read

SECURITY ALERT: Apache Log4j "Log4Shell" Remote Code Execution 0-Day Vulnerability (CVE-2021-44228, CVE-2021-45046 and CVE-2021-45105)

Product/Version includes:TippingPoint Digital Vaccine , Cloud One - Application Security 1.0, Cloud One - Open Source Security by Snyk Not Applicable, View More

Update Date: 2022/03/11 | Article Number: 000289940

Category: Remove a Malware / Virus | Rating: 1

Summary

Updated on 12/29/2021 @ 2:00PM GMT with updated information about Trend Micro Log4Shell Vulnerability Assessment Tool and new CVE-2021-44832.

Jump directly to information on affected/not-affected Trend Micro Products

On December 9, 2021, a new critical 0-day vulnerability impacting multiple versions of the popular Apache Log4j 2 logging library was publicly disclosed that, if exploited, could result in Remote Code Execution (RCE) by logging a certain string on affected installations.

This specific vulnerability has been assigned CVE-2021-44228 and is also being commonly referred to as "Log4Shell" in various blogs and reports. Versions of the library said to be affected are versions 2.0-beta 9 to 2.14.1.https://repo1.maven.org/maven2/org/apache/logging/log4j/log4j-core/2.15.0/.

Lessons learnt from cyber attacks

- The number one thing to worry about is your people.
- Plans drafted, but not put into place, are really bad.
- A checklist in place before the crisis hits, that you routinely practice the response plan, really good.
- Your company should pick a cyber security framework (e.g. Aura Top 10 Critical Controls, NIST Cyber Security Framework), and follow up with a maturity and effectiveness assessment, which drives a roadmap and investment.
- Don’t wait for the crisis to hit to start looking for outside help – legal, public relations, business continuity, ahead of time and sign them up.
- Key is engagement. You have to learn enough to ask smart questions and make sure that you are getting the complete and clear information you need to effectively oversee cyber security risk.
- Practice – learn – improve, practice – learn – improve, repeat

“Only one third of organisations surveyed by the NCSC possessed and tested an incident response plan in the previous year.

Only 41% of organisations were either ‘mildly confident’ or ‘not confident’ in their ability to detect a cyber intrusion.”

How to connect

HILARY WALTON

Email: hilary.Walton@Kordia.co.nz

LinkedIn: linkedin.com/in/HilsWalton/

Twitter @HilsWalton

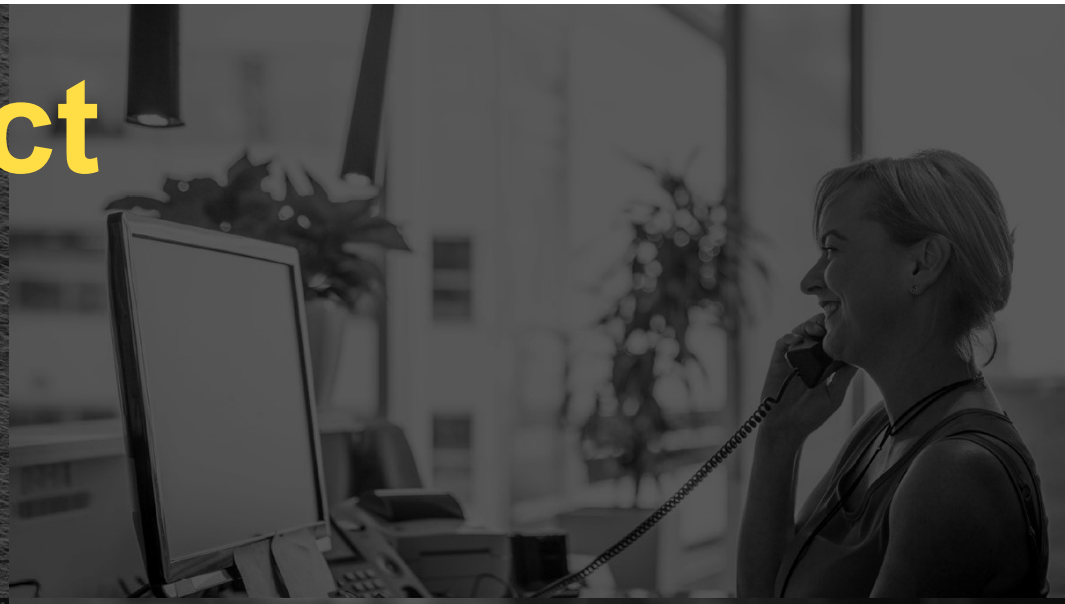
Instagram @HilsWalton

Facebook facebook.com/HilsWalton

TikTok @HilsWalton

YouTube: Digital Culture Ideas with Hilary Walton

Podcast: Digital Culture Ideas with Hilary Walton



kordia®

Q & A