Canadian Home Builders' Association

CHBA Member Webinar

CYBER SECURITY: EFFECTIVE STRATEGIES TO PROTECT YOUR BUSINESS

Derek Browne, CISO
March 2021

YOUR HOSTS

KEVIN LEE

CEO, CHBA

DEREK BROWNE

Chief Information Security Officer
for Northbridge Financial &
Federated Insurance

ABOUT ME

Derek Browne

- 30 years of security experience
- Lots of security credentials (CISSP, ISSAP, PCI-QSA, PA-QSA, CRISC, CISA, CIPP/IT, ISO27001 Lead Auditor)
- Experience both as backroom technical geek and in consulting and advisory roles
- Chief Information Security Officer for Northbridge Financial & Federated Insurance

AGENDA AND OBJECTIVES

- Brief status of the threat landscape
- Impacts of ransomware
- Overview of risks
- Protecting your company
- Partner security
- Some options for assessments
- Certifications of interest

STATE OF THE WORLD

It's been a busy year…

STATE OF THE WORLD

It's been a busy year…

Vulnerability known to be exploited in the wild

Common solution often white labeled

Triggers survey of partners

Triggers a hunt for alternatives and patching

STATE OF THE WORLD

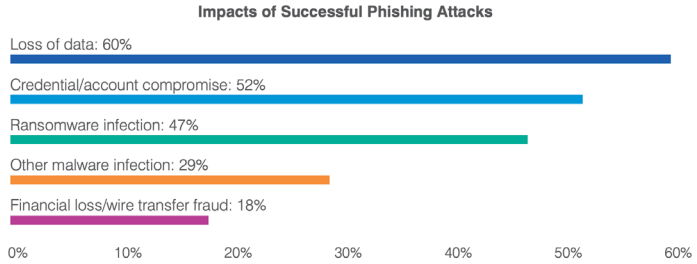
It's been a busy year…

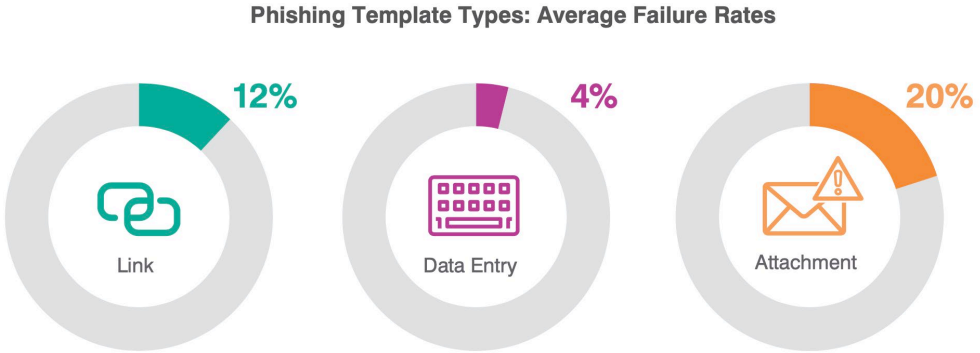
4 critical vulnerabilities in MS Exchange

So severe it justified release of patches a week ahead of schedule

Released tools to investigate compromise

The required architecture resulted in 20,000 customers in the USA compromised





The failure rate for COVID-19 related phishing simulations was almost 100% early in 2020

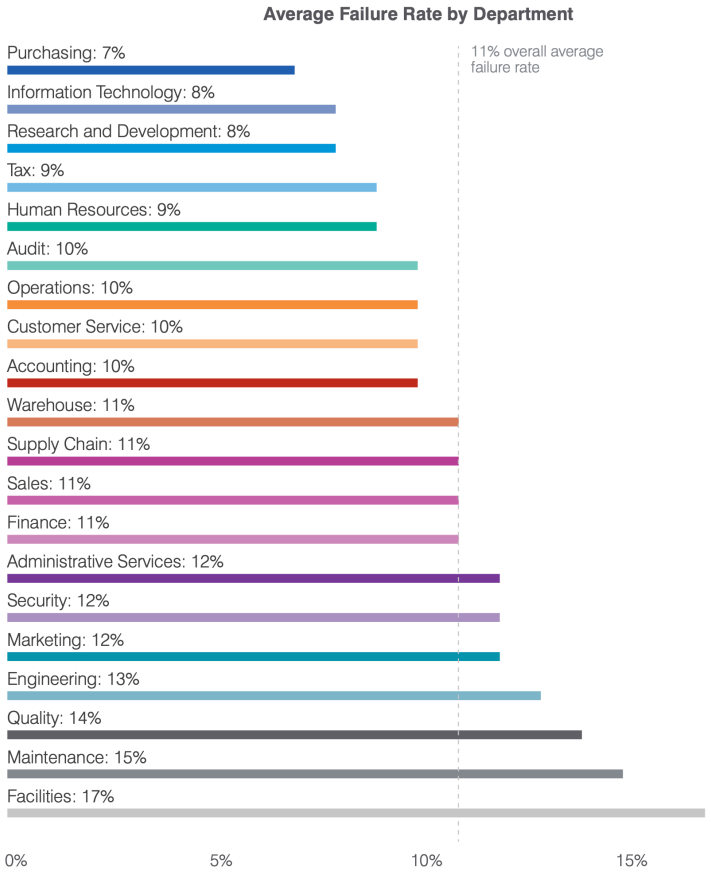
SOCIAL ENGINEERING THREATS

Social engineering is an attempt to convince a recipient to do something they would not normally do - an attack on trust.

- Click on a link
- Open an attachment
- Provide sensitive information

Overall the phishing failure rate appears to be 11%

Who is failing most?

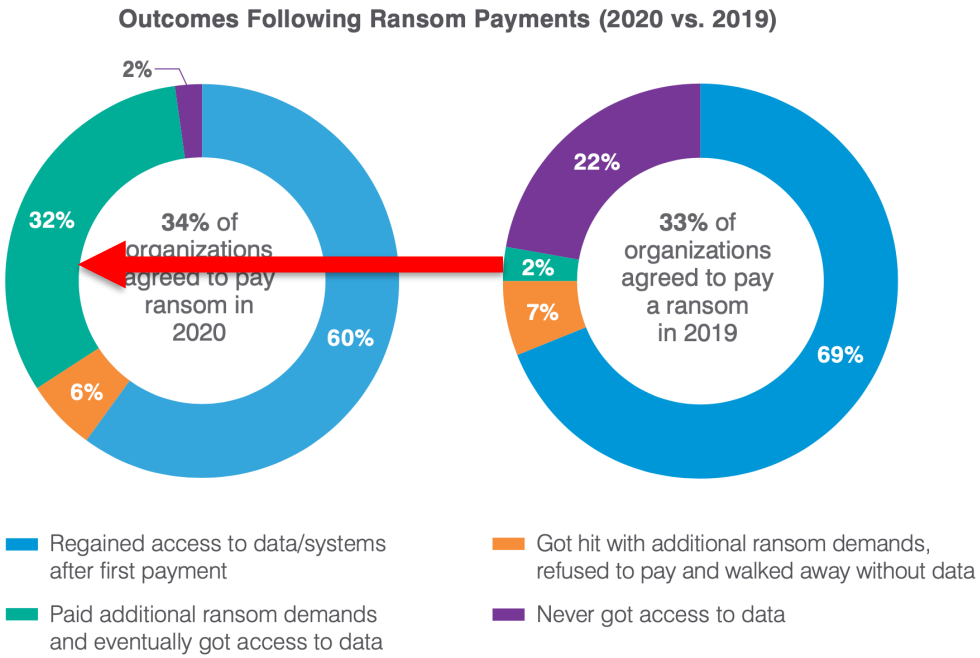


SOCIAL ENGINEERING THREATS

Social engineering is an attempt to convince a recipient to do something they would not normally do - an attack on trust.

- Click on a link
- Open an attachment
- Provide sensitive information

COSTS OF **RANSOMWARE**



RANSOMWARE

Ransomware is an extortion attack in which the victims computing resources are disrupted and only returned if ransom is paid

- Often results from social engineering
- Recently accompanied by data theft as well

LOST BUSINESS OPERATIONS

- Unplanned work
- Emotional stress
- Decrypting is typically slow and may overheat underpowered systems

MONETARY COSTS

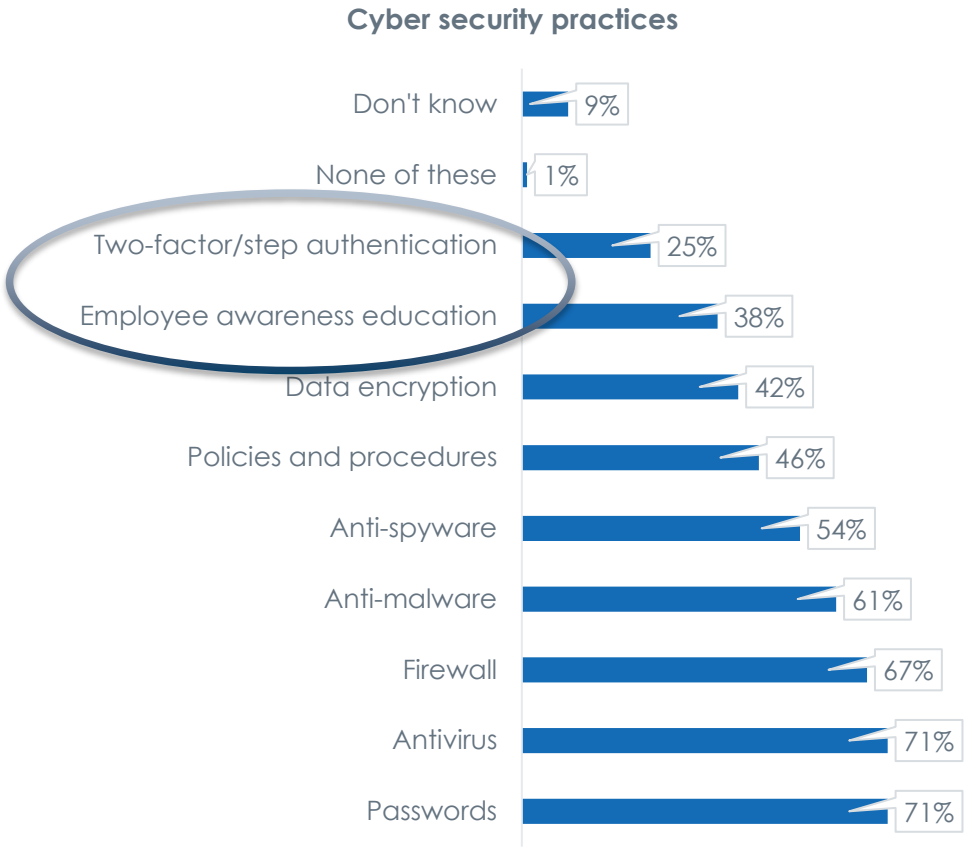
- Physical hardware damage
- Backup recovery
- Incident response and forensic partners
- Media communications preparation
- Breach of partner contracts
- Legal expenses
- Cyber insurance deductibles
- Ransom

DAMAGE TO CUSTOMERS

- Notification and communication
- Call centre set-up, staffing and scripting
- Credit and ID theft protection offers
- Reputational harm

COMMON CYBER SECURITY PRACTICES

- Due to smaller budgets, limited time or lack of guidance and awareness, SMEs engage in remedies that temporarily mitigate cyber threat
- Security is a moving target – there is constant evolution and a need to adapt accordingly



Canada - Ipsos, ESET North America, ID 828625

OVERVIEW OF **RISKS**

ROOT CAUSES

Technical risks

- Misconfigurations
- Vulnerabilities
- Malware – Ransomware, RATs and Bots

Non-technical risks

- Insiders
- Partner risk
- Social engineering

TECHNICAL RISKS

Vectors of attack & attack surfaces

- Connectivity via wireless/cellular and OTA updates
- Untrusted or loosely configured network connections
- End-of-life operating systems and migrating data to new systems

Controls to implement and test

- *1-10-60 Rule:* Detect in 1 minute, qualify in 10 minutes, react in 60 minutes

NON-TECHNICAL RISK

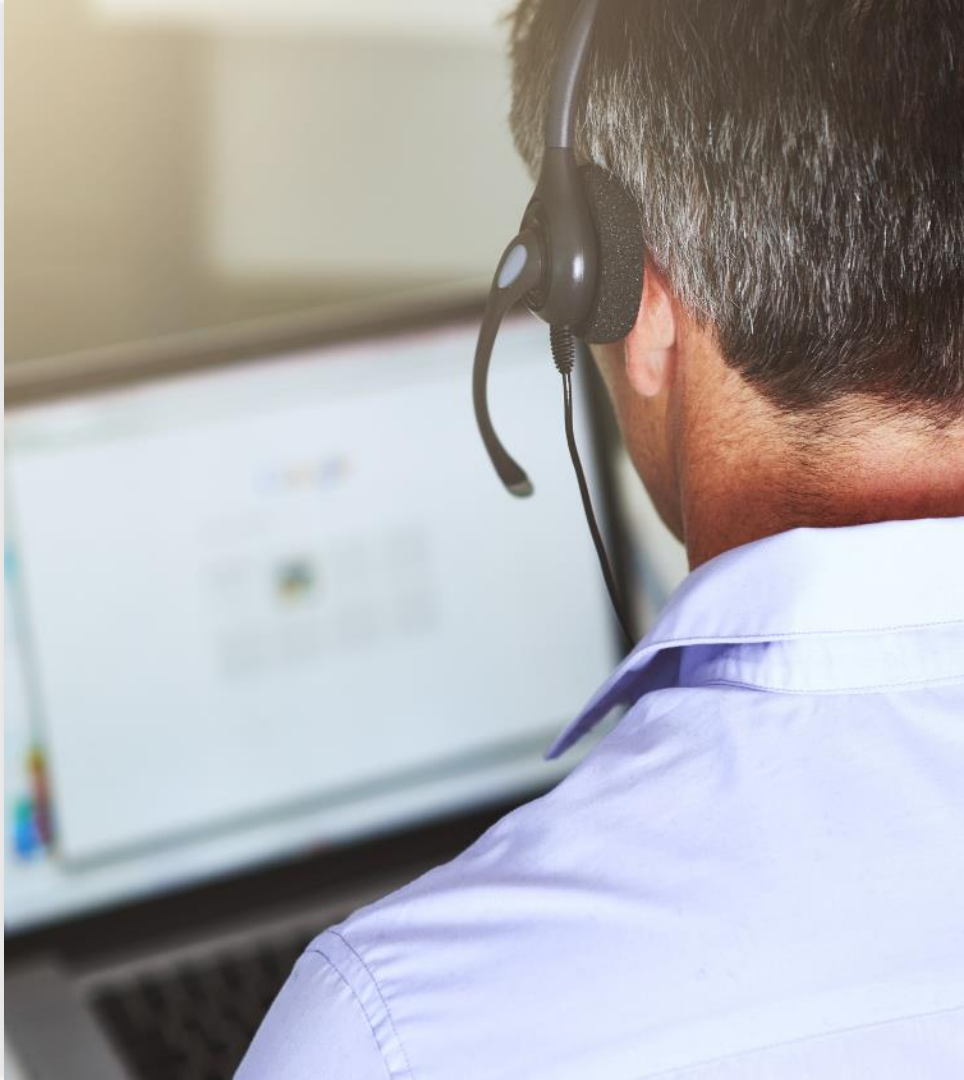
Insider Examples: Capital One & AWS

- Monitor who has access to what and regularly challenge that assumption
- Send people on vacation or temporarily rotate them to a new role
- Remove access and see what people actually need

NON-TECHNICAL RISK

Partner Email Compromise

- Partner compromised and their email system taken over
- We received well-crafted emails with invoices and new banking details
- AP clerk detected suspicious behavior and called the partner to validate



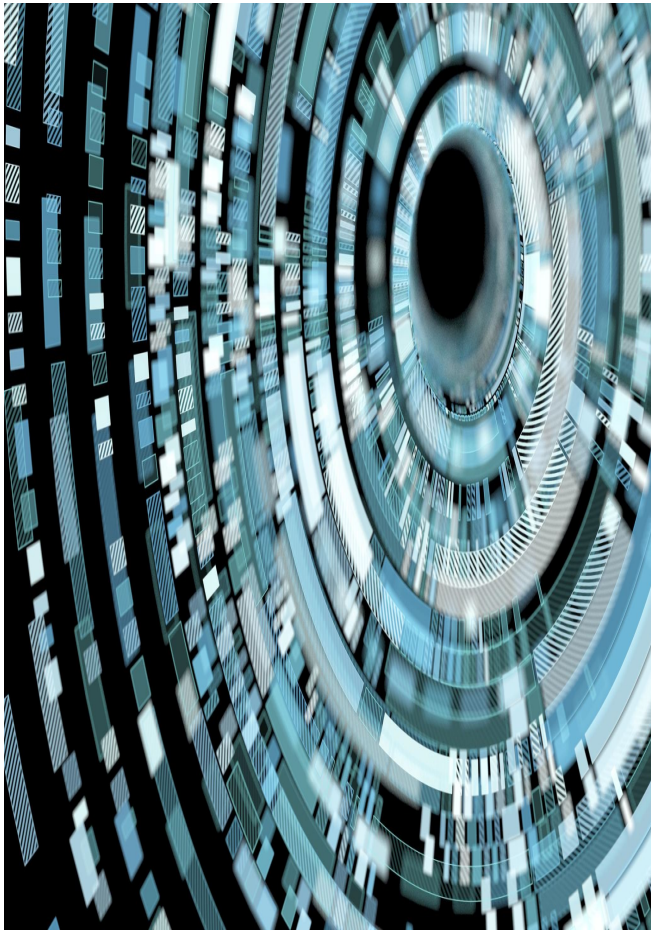
NON-TECHNICAL RISK

Partner Compromise

- Partner has provided their services manually since December when they were hit with ransomware
- Still attempting to recover one application server
- Ensure you're doing partner security assessments

SOCIAL ENGINEERING AND PHISHING ATTACKS

- If something seems off, verify with sender without using email
- Question and examine every email
    - Does sender's email address match what you expected?
    - Do URLs and links match expected destination?
    - Is logo colour and placement correct?
    - Is spelling, grammar and formatting professional?
- Don't open attachments until you're sure they're legitimate
- Don't pull emails from your junk mail and trust them
- https://youtu.be/l7alNPcudgg -- Classic phishing attack



PROTECTING YOUR COMPANY

Know what you have

Prioritize the risks

Good security hygiene

Know what you need to do when the crisis occurs

KNOW WHAT YOU HAVE

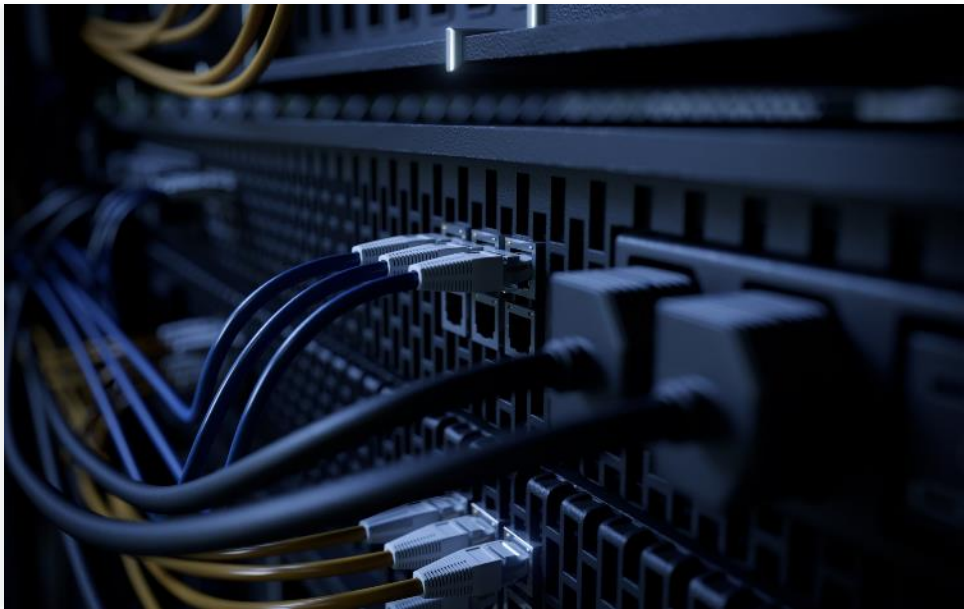
- Document your assets
- Get independent security assessments
    - Technical penetration tests
    - Non-technical security controls
- Monitor threat feeds for emerging risks

PRIORITIZE YOUR RISKS

- What's likely to happen?
- What are the impacts?

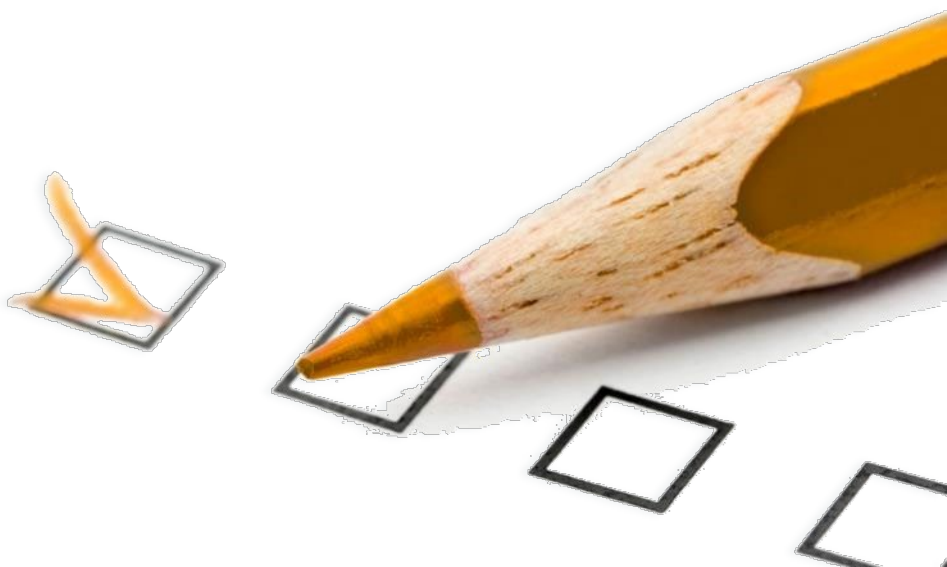
PRACTICE GOOD SECURITY HYGIENE

- Patch everything regularly
- Configure for security – harden and review
- Back up mission critical systems
- Test for validity



KNOW WHAT TO DO IN A CRISIS

- Create an incident response plan
- Make sure you know who to call
    - IR/forensics partners
    - Police service
    - Lawyers
- Plan your communications strategy

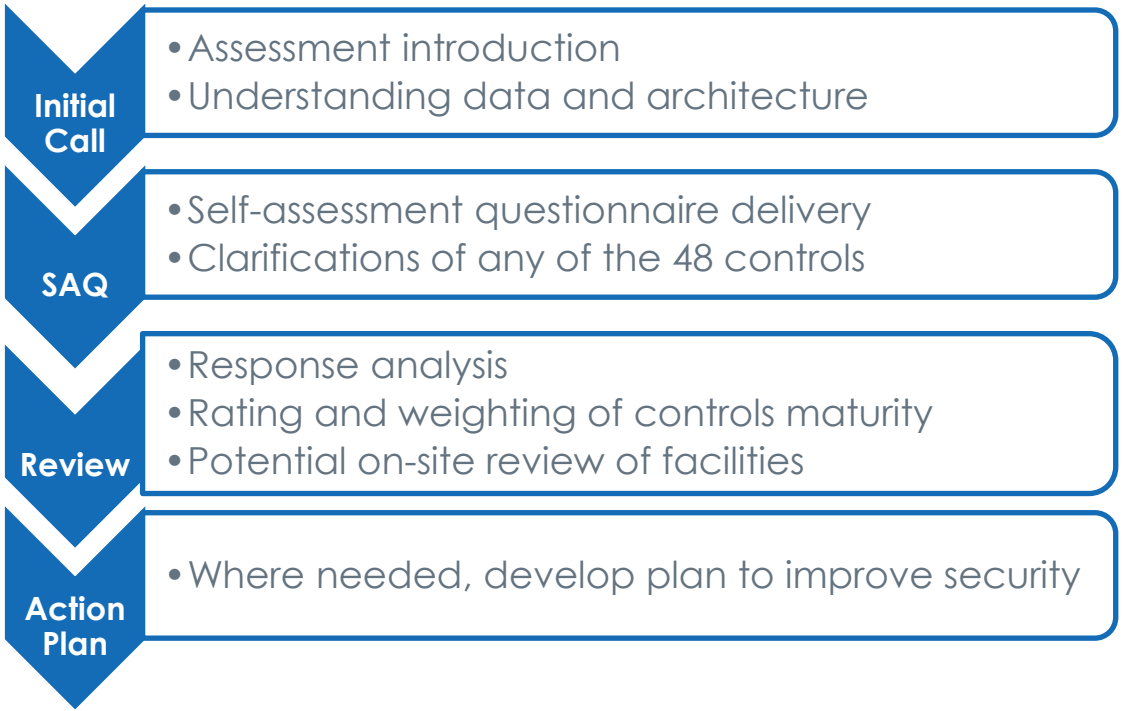


PARTNER RISKS

MANAGING PARTNER RISK

- What does partner risk look like?
    - Prevention measures
    - Technical control and products
    - Building a program
- Making it business as usual

PARTNER SECURITY RISK PROCESS



ASSESSMENT FRAMEWORKS

THE ESSENTIAL EIGHT
THE AUSTRALIAN SIGNALS DIRECTORATE

1. Do you only permit known good applications to run?
2. Do you Patch Applications
3. Do you block Microsoft Office Macros?
4. Are users applications 'Hardened'?
5. Do you control who can act as Administrator?
6. Do you Patch Operating Systems?
7. Do you use Multi-Factor Authentications?
8. Do you do Daily Backups?

Three tiers of Maturity:

- Partly
- Mostly
- Fully Aligned

https://www.cyber.gov.au/acsc/view-all-content/essential-eight

CIS TOP 20

- Tiered approach to a smaller set of controls
  - Three Implementation Groups
- Understandable by mere mortals
- Deals with processes not just technologies
  - e.g. 3.1 and 3.6 - Automate Vuln Scanning & Compare scans
- Provides something that can be audited

https://www.cisecurity.org/controls/cis-controls-list/

CIS Top 20 Security Controls

1. Inventory hardware assets
2. Inventory software assets
3. Continuous Vulnerability Management
4. Control Admin privileges
5. Securely configure all devices
6. Maintenance & Monitoring of Audit Logs
7. Email and Web Browser Protection
8. Malware Defences
9. Limit Network ports and services
10. Data Recovery Capabilities
11. Securely configure all network devices
12. Boundary Defenses
13. Data Protections
14. Control Access – Need to Know
15. Wireless Access Control
16. Account Monitoring and Control
17. Security Awareness Training
18. Application Software Security
19. Incident Response Capabilities
20. Penetration Testing and Red Team exercises

RESOURCING CERTIFICATIONS

NORTHBRIDGE

SECURITY CERTIFICATIONS

Cert	Focus	Pre-Reqs
CISSP (ISC2)	General information security domains 8 Domains of focus Has Separate concentrations 3 year cycle of CPEs & AMFs	5 years Experience Background check 6 hours exam Sponsor to vouch
CRISC (ISACA)	General Risk Management Professional 4 Domains of Risk Management Looks at Finding, Assessing, mitigating and reporting risk	3 years experience Demonstrated work in some domains 3 hour exam
CISA (ISACA)	Info Systems Audit Focus 5 Domains of Audit and Governance	5 years experience in Audit 6 hour exam

NORTHBRIDGE

SECURITY CERTIFICATIONS

	CISSP	CISM	CISA	CRISC
Experience	5 years	5 years	5 years	3 years
Number of exams	1	1	1	1
Exam fee	$699	$575/Member $760/Non-member	$575/Member $760/Non-member	$575/Member $760/Non-member
Annual fee	$85	$45 members; $85 non-members	$45 members; $85 non-members	$45 members; $85 non-members
Valid for	3 years	3 years	3 years	3 years
CPEs for recertification	120 total; at least 40 each year	120 total; at least 20 per year	120 total; at least 20 per year	120 total; at least 20 per year
Average salary *	$109,965	$105,926	$97,117	$107,968

OVERVIEW

- Social Engineering
- Ransomware Impacts

- Partner Risk

- Using a framework to guide your security journey
- Who to work with to assist you with the security journey.
    - Skills to look for

Content provided in this webinar is provided by our specialists and is intended to augment your internal safety, compliance and risk management practices, and are not a substitute for professional or legal advice.
Services are not an insurance policy, contact us for details.

Federated Insurance

Derek Browne
Derek.Browne@nbfc.com
416-350-4400