Asia Pacific Risk Symposium 2020

Cybersecurity: Recent trends in a changing cyber risk landscape

26 August 2020

pwc

Agenda

1. Introduction
2. Cyber threats to Asia Pacific – An incident response retrospect & demo
3. Demo
4. Panel discussion –The challenges ahead
5. Q&A and wrap up

1

Introduction

Session 2 | Cybersecurity – Recent trends in a changing cyber risk landscape

Kenneth Wong
Cybersecurity and Privacy Leader,
Risk Assurance,
PwC Asia Pacific and
Mainland China/Hong Kong

Andrew Gordon
Partner, Cyber
PwC Australia

Shong Ye Tan
Digital Trust Leader
PwC Singapore

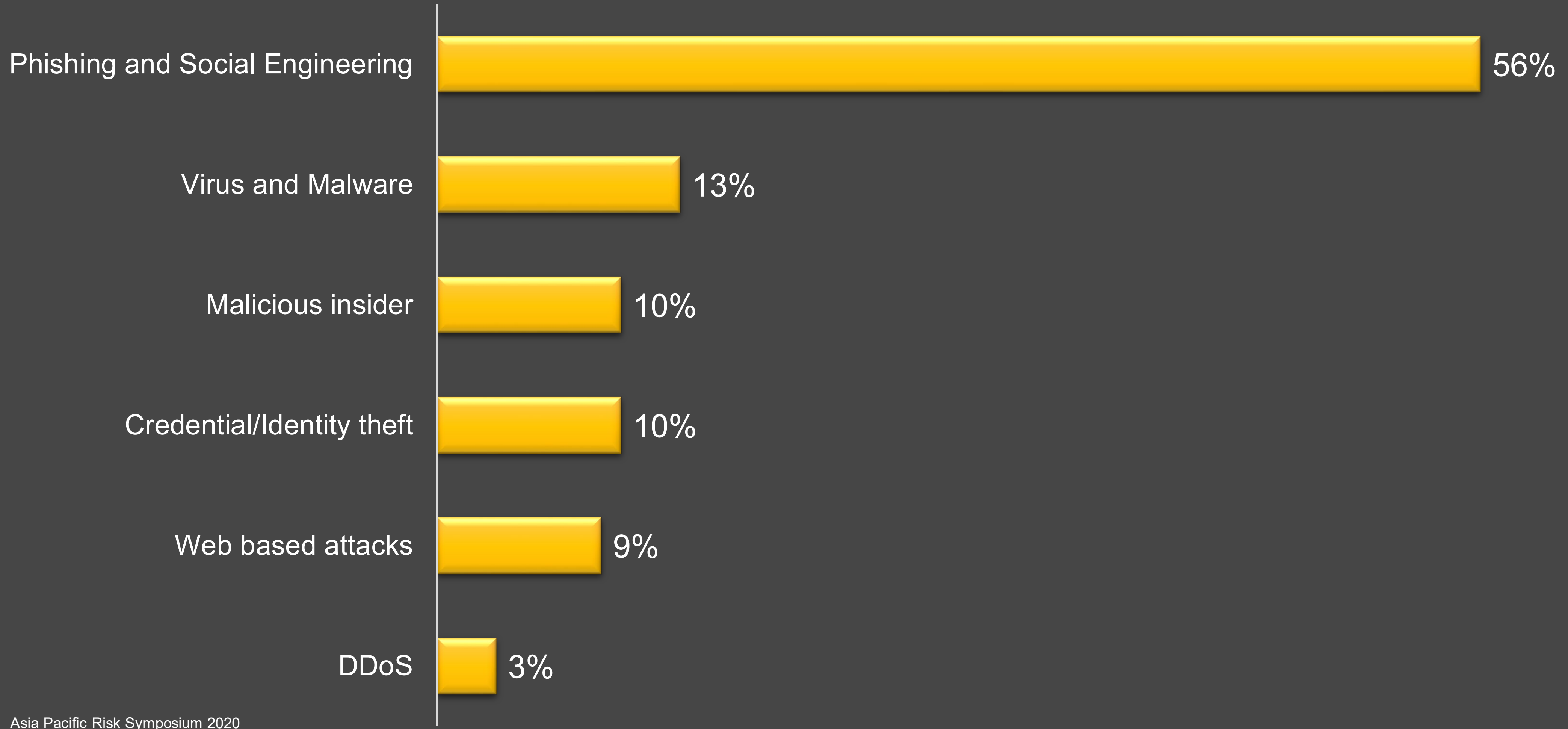
Patrick Wong
Director, Cybersecurity and Privacy
PwC Mainland China/Hong Kong

2

Cyber threats to Asia Pacific – An incident response retrospect & demo

Poll question #1

Which of the following type of cyber risks do you believe poses the most threat to your business?

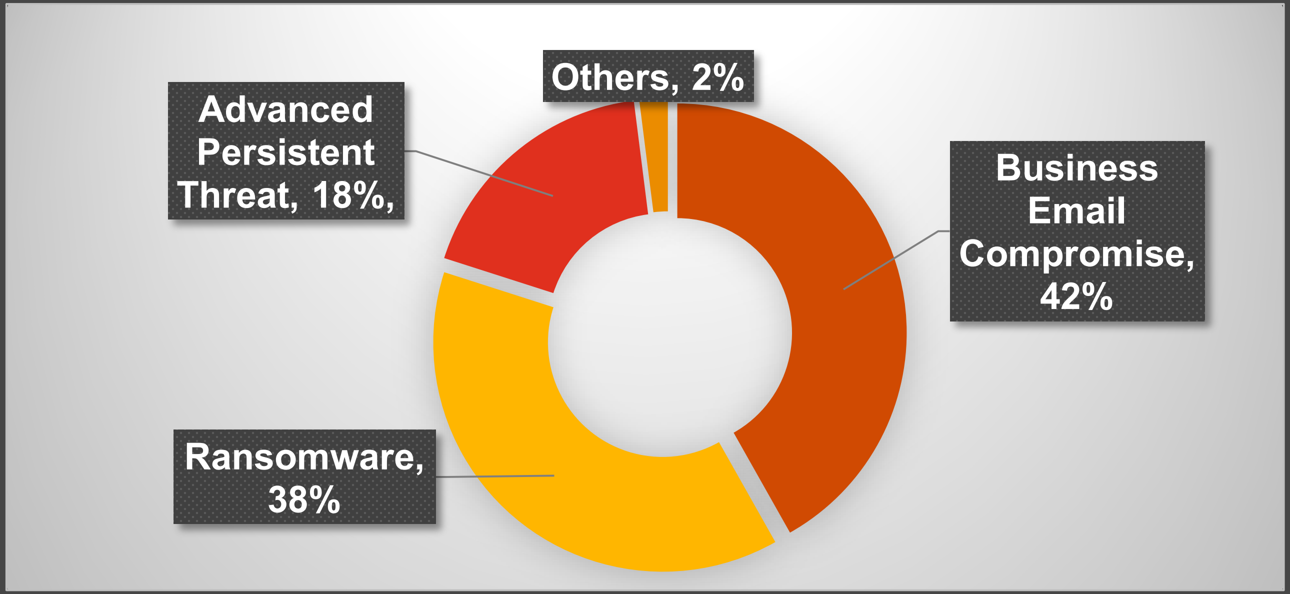


Major cyber risks in the past 2 years

Experience from PwC incident responses

Understanding the threats your organisation will likely face is key to effective cyber security. To stay ahead of the threats it is important to understand which kinds of attacks you need to look out for.

Based on the cyber security incidents PwC have responded to over the past 2 years, the top 3 cyber security incidents across Asia Pacific are as follows:



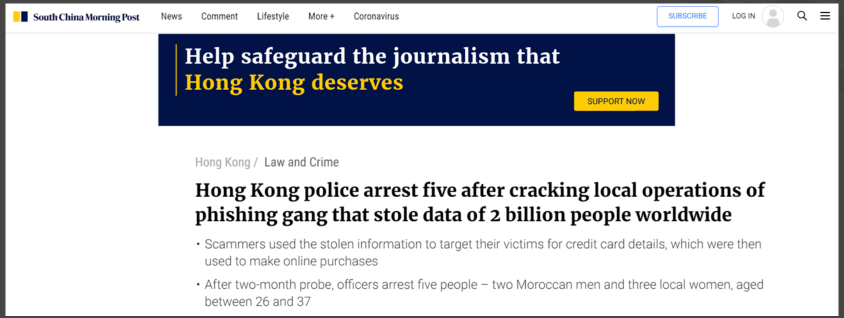
Recent major cyber risks – Hong Kong

Crackdown of Local Phishing Gang (28 July 2020)

- Hong Kong police arrest five after cracking local operations of phishing gang that stole data of 2 billion people worldwide
- Scammers used the stolen information to target their victims for credit card details, which were then used to make online purchases

Hong Kong Security Watch Report (19 May 2020)

- In the first quarter of 2020, the total number of security events raised by 45.6%, from 9,911 in 2019 Q4, to 14,433.
- The growth was mainly attributed to the increase in the number of malware hosting events, which jumped up by 3.5 times, to 5,445 in this quarter.
- The second obvious change was the rise in phishing events, up by more than 50%.
- The count of defacement and botnet events did not change much when compared with the previous quarter.



Help safeguard the journalism that Hong Kong deserves

Hong Kong / Law and Crime

Hong Kong police arrest five after cracking local operations of phishing gang that stole data of 2 billion people worldwide

- Scammers used the stolen information to target their victims for credit card details, which were then used to make online purchases
- After two-month probe, officers arrest five people – two Moroccan men and three local women, aged between 26 and 37

Hong Kong Security Watch Report

2020 Q1

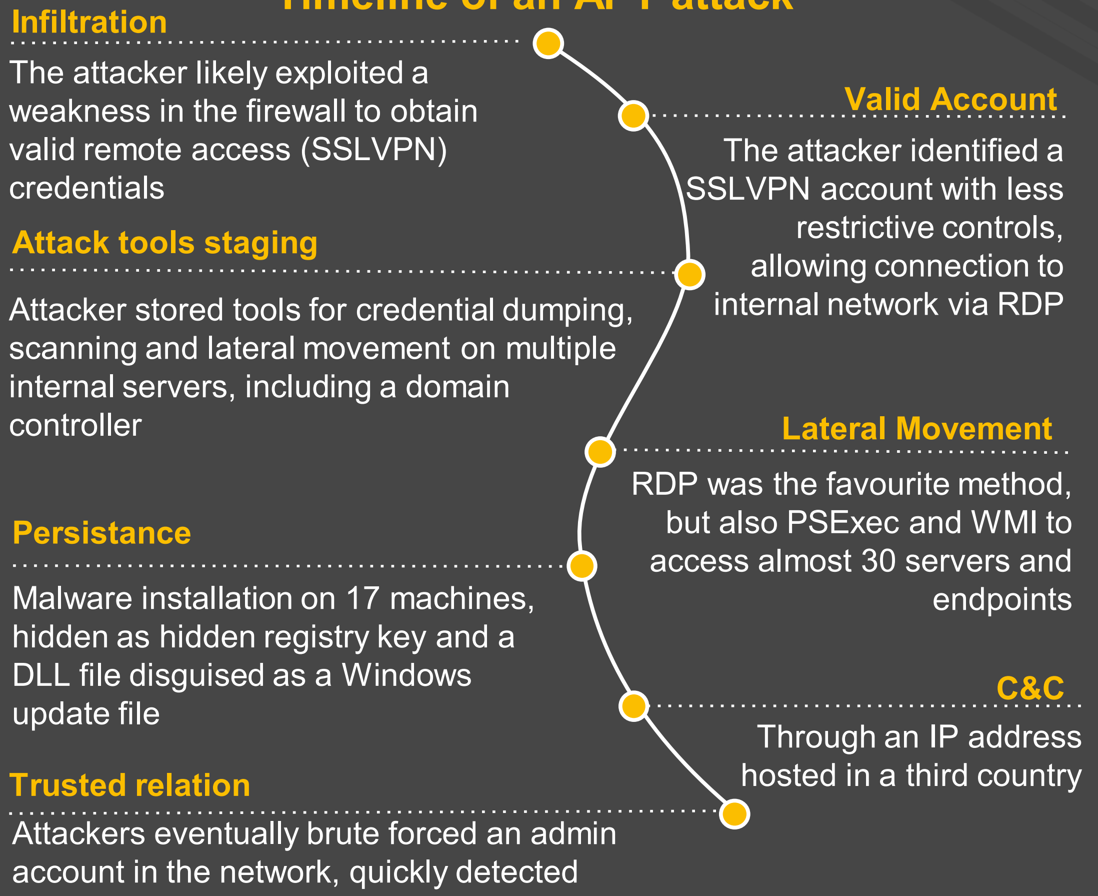
Incident response threat trends

Hong Kong perspective

2019 – APT

- One of the most sophisticated incidents that we helped our client
- Intrusion started in a subsidiary of a large organisation
- ~40 days dwell time
- Significant use of living-off-the-land techniques for lateral movement
- Criminals leveraged victims’ unpatched vulnerability in system and inadequate network segmentation

Timeline of an APT attack



Infiltration

The attacker likely exploited a weakness in the firewall to obtain valid remote access (SSLVPN) credentials

Valid Account

The attacker identified a SSLVPN account with less restrictive controls, allowing connection to internal network via RDP

Attack tools staging

Attacker stored tools for credential dumping, scanning and lateral movement on multiple internal servers, including a domain controller

Lateral Movement

RDP was the favourite method, but also PSExec and WMI to access almost 30 servers and endpoints

Persistance

Malware installation on 17 machines, hidden as hidden registry key and a DLL file disguised as a Windows update file

C&C

Through an IP address hosted in a third country

Trusted relation

Attackers eventually brute forced an admin account in the network, quickly detected

Recent major cyber risks – Singapore

Web defacement

Increased about 45% from last year, victims are mainly SMEs in education, retails, finance & manufacturing sectors. A large portion of defacement links to overseas hacktivists groups and political conflicts.

Ransomware

Cases related to Ryuk, Maze Sodinokibi regularly targets gaming, travel and tourism, manufacturing, and logistics companies.

Phishing

Threat actors impersonate trusted organisations and individuals to steal sensitive data from unsuspecting victims. Most common spoofed organisations are Apple, Paypal, Microsoft, etc.. Common government organisations are spoofed by hackers/scammers are Immigration & Checkpoint authority, Ministry of Manpower, Singapore Police force and Ministry of Health. Business e-mail compromise is another form of spear phishing which is increasing

Cloud incidents

7 of 10 Singapore organisations are victims of public cloud breaches due to a increased adoption of cloud. The awareness of security in cloud among SMEs, Fintech is still low and there is continuous struggle between moving fast/agile vs. good security governance in large organisations.

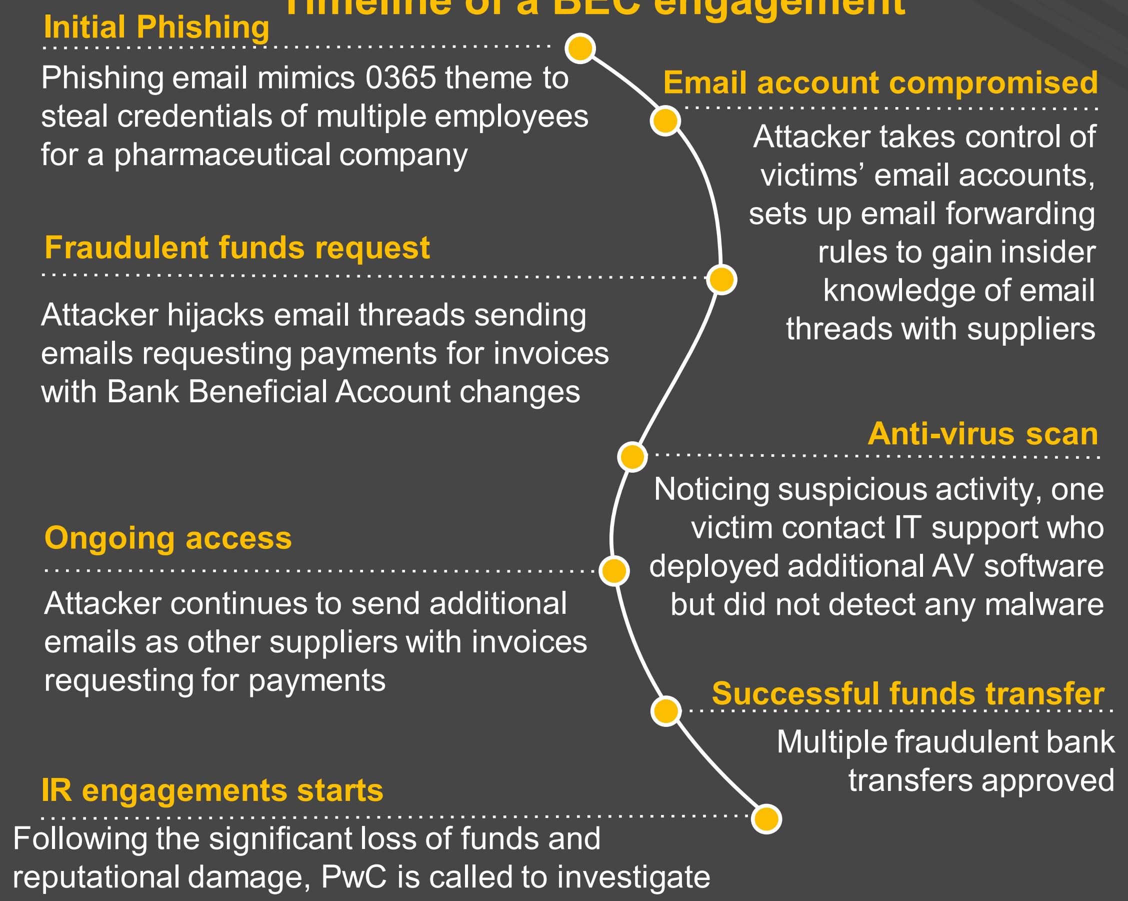
Incident response threat trends

A Singapore perspective

2019 - Business Email Compromise (BEC)

- Business Email Compromise is now the biggest cause of cybercrime financial losses totalled US$1.7B (2019 FBI Internet Crime Report)
- In 2019, almost 25% of the incidents we responded were relatively low sophistication business email compromise scams.
- Criminals targeted financial services companies because victims were likely accustomed to large transfer of sums
- Criminals leveraged victims' compromised credentials and lack of multi-factor authentication

Timeline of a BEC engagement



Initial Phishing

Phishing email mimics 0365 theme to steal credentials of multiple employees for a pharmaceutical company

Email account compromised

Attacker takes control of victims' email accounts, sets up email forwarding rules to gain insider knowledge of email threads with suppliers

Fraudulent funds request

Attacker hijacks email threads sending emails requesting payments for invoices with Bank Beneficial Account changes

Anti-virus scan

Noticing suspicious activity, one victim contact IT support who deployed additional AV software but did not detect any malware

Ongoing access

Attacker continues to send additional emails as other suppliers with invoices requesting for payments

Successful funds transfer

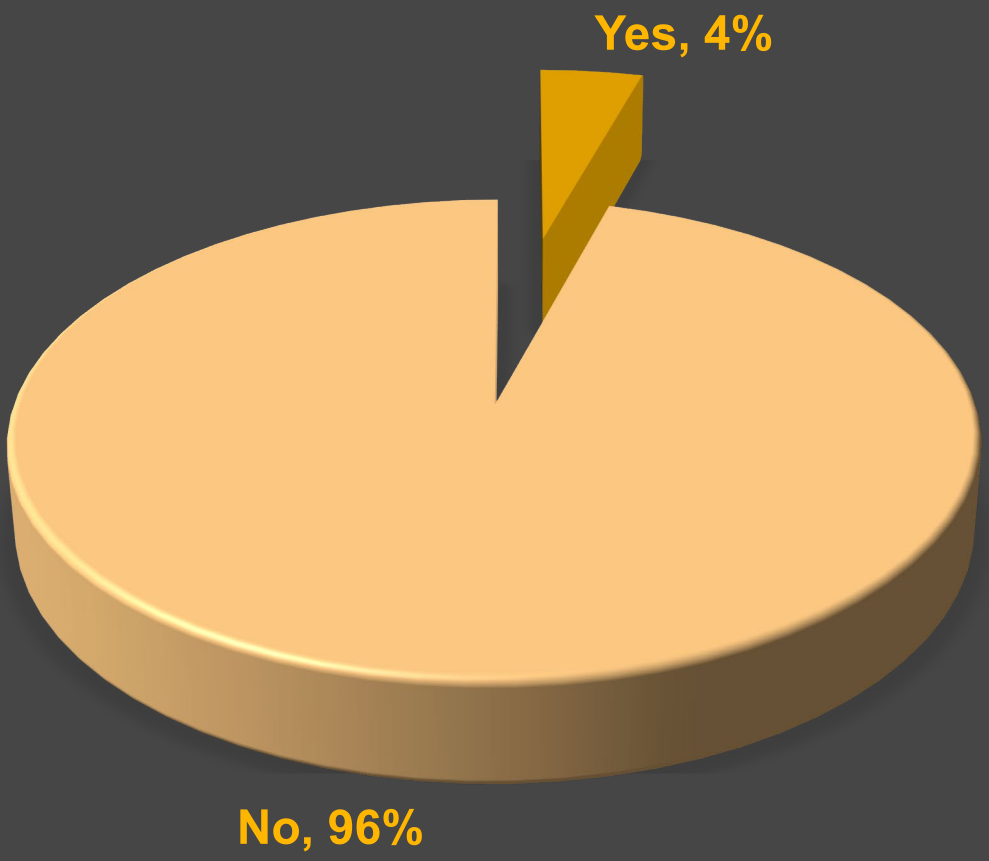
Multiple fraudulent bank transfers approved

IR engagements starts

Following the significant loss of funds and reputational damage, PwC is called to investigate

Poll question #2

If you are a victim of a ransomware attack, should you pay for ransom?



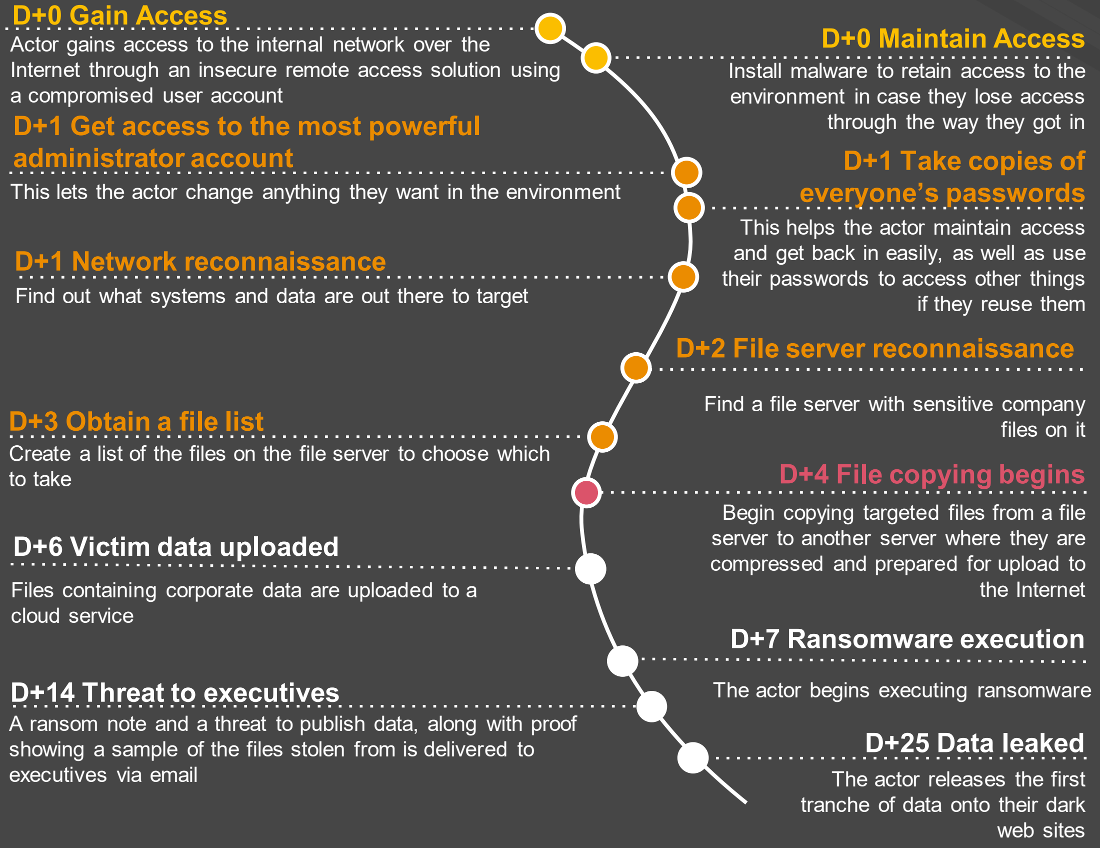
Incident response threat trends

Australia perspective

2019 - Ransomware

- In 2019, almost 70% of the incidents we responded to were either cryptomining or ransomware
- While phishing is still the most common infection vector accounting for >90%, this is not the case in all of our incidents
- Web application is one of the most vulnerable target in financial services
- Criminals uses “Living-off-the-land” to avoid antivirus detection
- Criminals leveraged victims’ unpatched and vulnerable systems and applications

Timeline of a Ransomware attack



D+0 Gain Access
Actor gains access to the internal network over the Internet through an insecure remote access solution using a compromised user account

D+0 Maintain Access
Install malware to retain access to the environment in case they lose access through the way they got in

D+1 Get access to the most powerful administrator account
This lets the actor change anything they want in the environment

D+1 Take copies of everyone’s passwords
This helps the actor maintain access and get back in easily, as well as use their passwords to access other things if they reuse them

D+1 Network reconnaissance
Find out what systems and data are out there to target

D+2 File server reconnaissance
Find a file server with sensitive company files on it

D+3 Obtain a file list
Create a list of the files on the file server to choose which to take

D+4 File copying begins
Begin copying targeted files from a file server to another server where they are compressed and prepared for upload to the Internet

D+6 Victim data uploaded
Files containing corporate data are uploaded to a cloud service

D+7 Ransomware execution
The actor begins executing ransomware

D+14 Threat to executives
A ransom note and a threat to publish data, along with proof showing a sample of the files stolen from is delivered to executives via email

D+25 Data leaked
The actor releases the first tranche of data onto their dark web sites

Recent major cyber risks – Australia

Prime Minister’s Announcement (30 June 2020)

- Malicious cyber activity against Australian networks
- $1.35 billion over the next decade to enhance the cyber security capabilities
- Over $31 million to enhance the ability of ASD to disrupt cybercrime offshore
- $35 million to deliver a new cyber threat-sharing platform on malicious cyber activity
- $12 million towards strategic mitigations and active disruption options
- Over $118 million for ASD to expand its data science and intelligence capabilities
- $470 million investment to expand the cyber security workforce

Australian Cyber Strategy 2020 was unveiled on 06/08/20

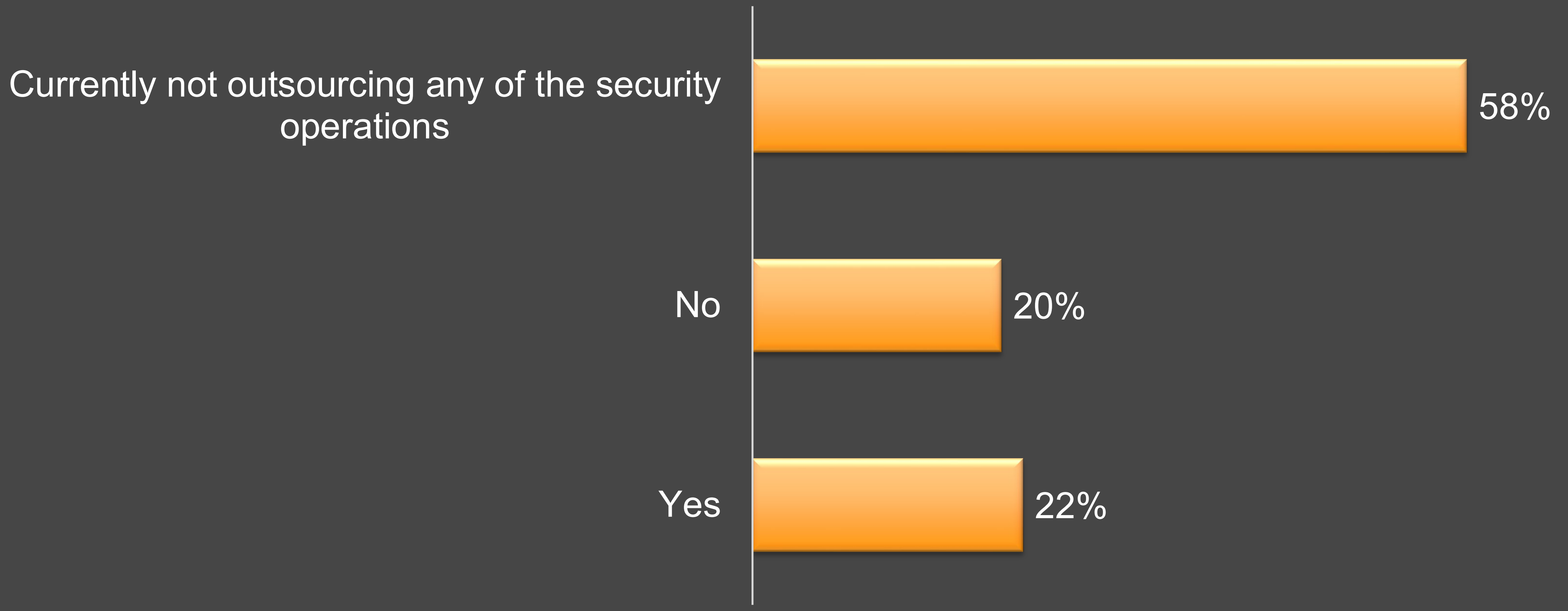
- Commitment to Protecting Critical Infrastructure and Systems of National Significance
- Law enforcement agencies given greater ability to protect Australians online
- Australian Government to build trust online by supporting businesses’ cyber resilience, sharing threat information and setting clear expectations of roles.
- voluntary Code of Practice will set out the Australian Government’s security expectations for the internet-connected consumer devices Australians use every day

Australian Government

AUSTRALIA’S CYBER SECURITY STRATEGY 2020

Poll question #3

If you are currently outsourcing some or part of your security operations, do you feel you are getting the most value out of your MSSP?



Incident response threat trends

Summary of common and recurring issues

1

Unpatched vulnerabilities in systems and applications

2

Weak and compromised credentials

3

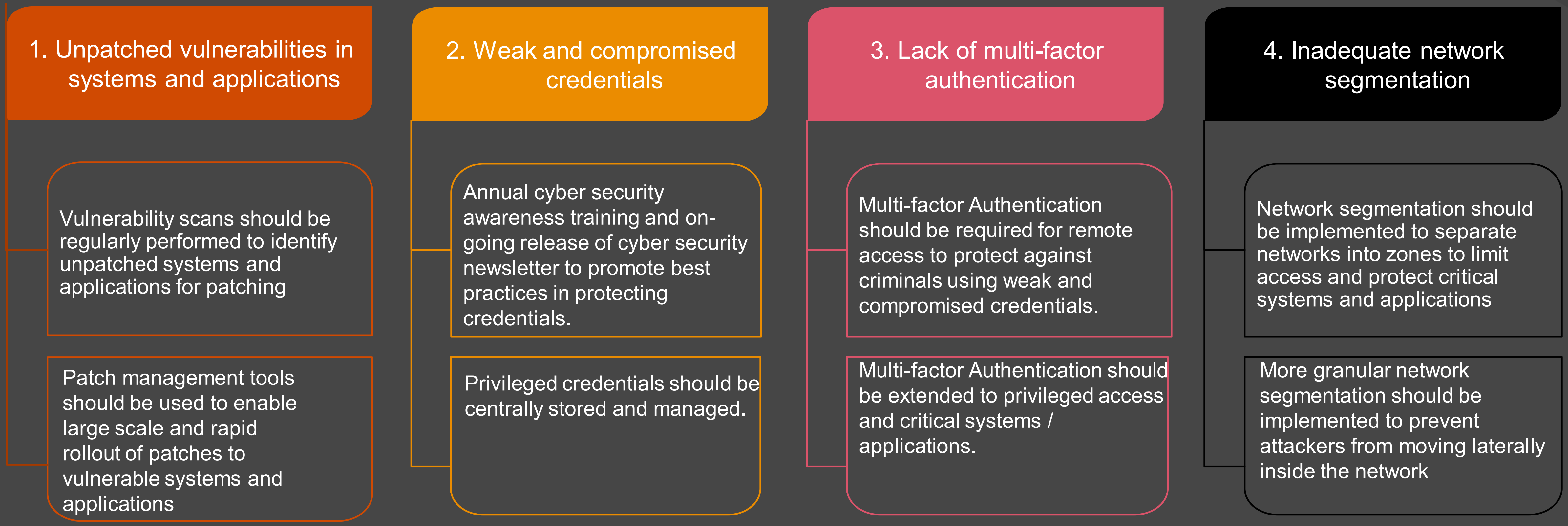
Lack of multi-factor authentication

4

Inadequate network segmentation

Best practices to address common causes of cyber security incidents

Based on the recent cyber security incident responses performed by PwC, the following best practices will help address many common and recurring issues leading to cyber security incidents.



1. Unpatched vulnerabilities in systems and applications

- Vulnerability scans should be regularly performed to identify unpatched systems and applications for patching
- Patch management tools should be used to enable large scale and rapid rollout of patches to vulnerable systems and applications

2. Weak and compromised credentials

- Annual cyber security awareness training and on-going release of cyber security newsletter to promote best practices in protecting credentials.
- Privileged credentials should be centrally stored and managed.

3. Lack of multi-factor authentication

- Multi-factor Authentication should be required for remote access to protect against criminals using weak and compromised credentials.
- Multi-factor Authentication should be extended to privileged access and critical systems / applications.

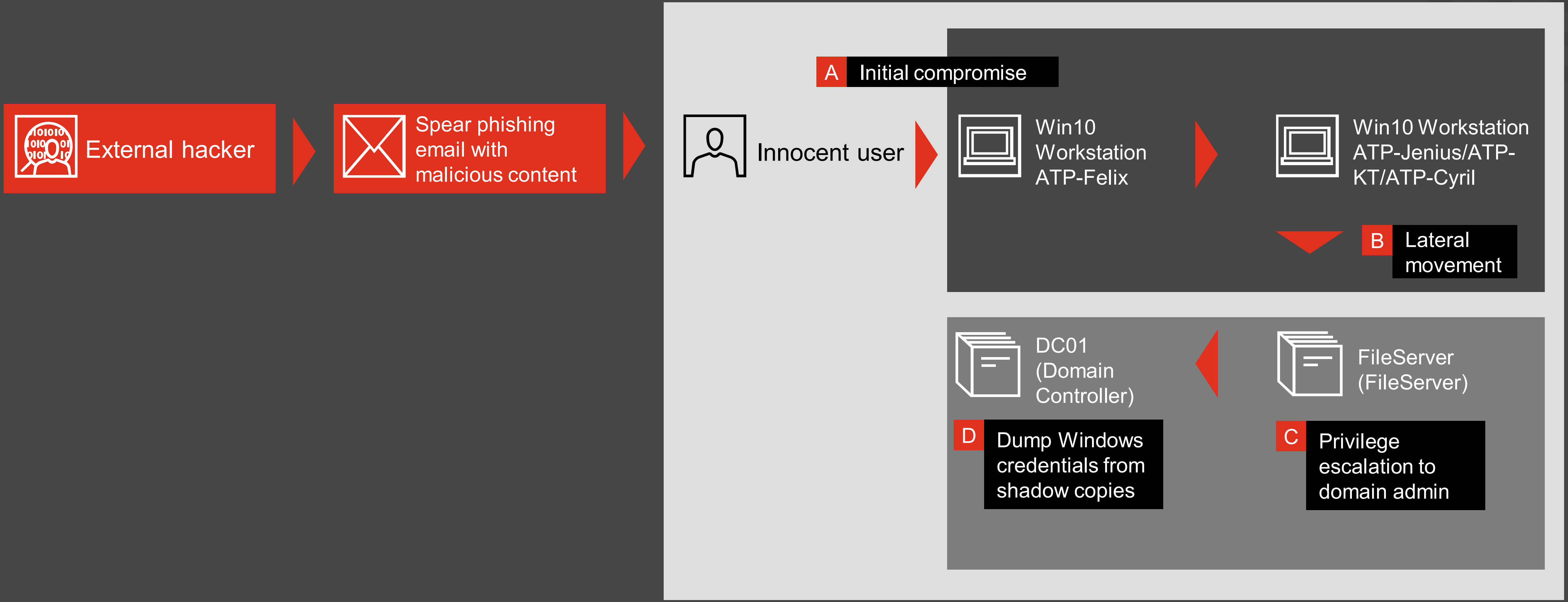
4. Inadequate network segmentation

- Network segmentation should be implemented to separate networks into zones to limit access and protect critical systems and applications
- More granular network segmentation should be implemented to prevent attackers from moving laterally inside the network

3

Demo

Live demo


External hacker
Spear phishing email with malicious content
A Initial compromise
Innocent user
Win10 Workstation ATP-Felix
Win10 Workstation ATP-Jenius/ATP-KT/ATP-Cyril
B Lateral movement
FileServer (FileServer)
C Privilege escalation to domain admin
DC01 (Domain Controller)
D Dump Windows credentials from shadow copies

Don’t forget physical security

Physical security is every bit as important as cyber security. According to the 2020 Verizon’s Data Breach Investigations Report, physical actions still accounts for 4% of the data breaches in 2019.

It is important to make sure that an organisation's physical security weaknesses will not undermine the cyber security controls. Here are some common vulnerabilities we find in our physical penetration testing exercises:

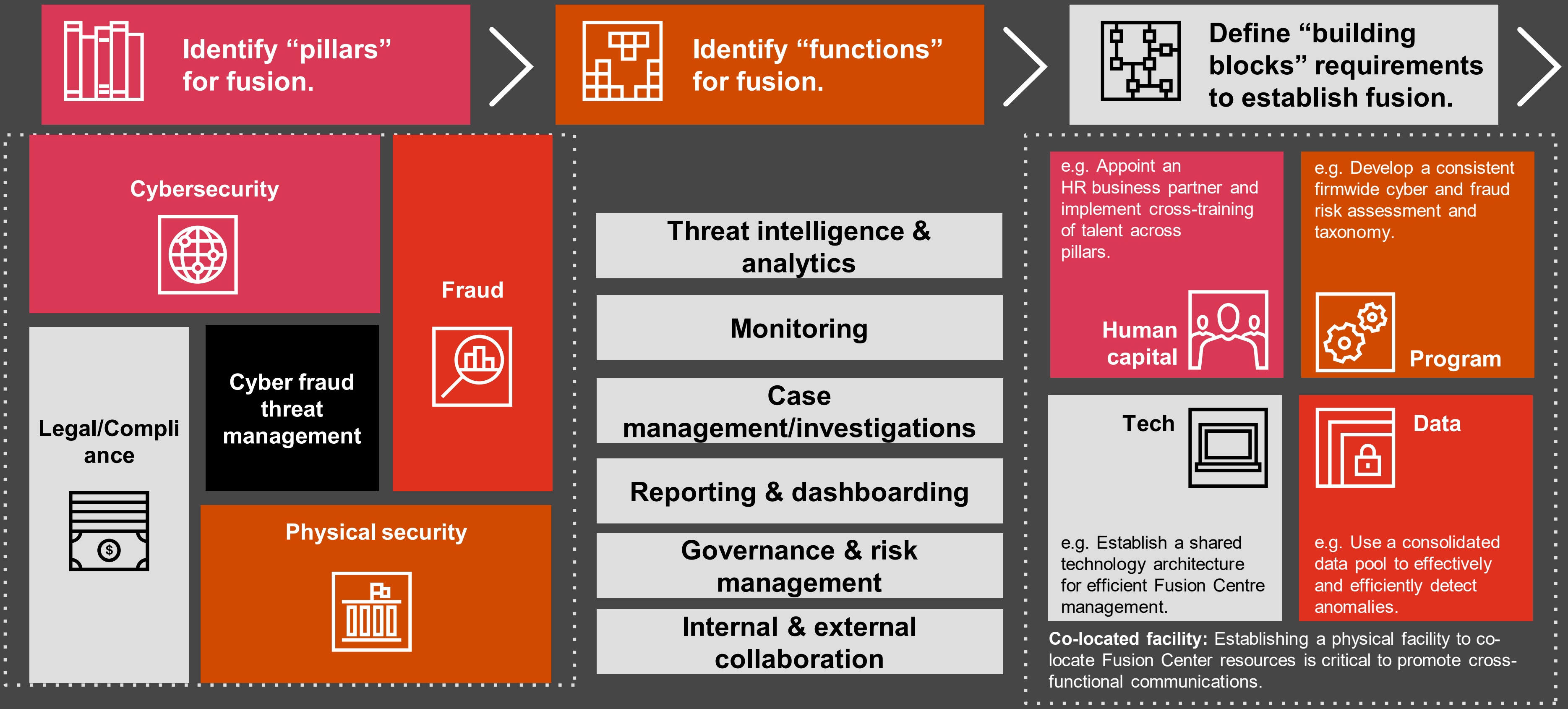
Threat 1: Tailgating	Threat 2: Leakage of sensitive documents and notes	Threat 3: Theft of laptop and portable devices with sensitive data	Threat 4: Stolen Identification	Threat 5: Rouge USB drives
Examples:				
A criminal relies on human trust to gain access to a secure building or area	Sensitive documents and notes fallen into the wrong hands	Theft of unattended laptop and portable devices in office, cars, airports, hotels and restaurants	Cloning of access card	Employee found a rogue USB drive and inserted it into their computer
Safeguards:				
Discourage tailgating with awareness training and encourage reporting of suspicious activities	Do not write passwords and leave sensitive documents on desk	Never leave laptop or portable devices unsecured, even for "just a minute".	No sharing or lending of cards. Multi-factor authentication for highly sensitive area	Awareness Training

4

Panel discussion – The challenges ahead

Fusion Centre

An optimal Fusion Centre strategy and operating model is achieved by identifying, streamlining and integrating the right capabilities across core organisational pillars to increase risk reduction and improve efficiencies.



Identify “pillars” for fusion.

Identify “functions” for fusion.

Define “building blocks” requirements to establish fusion.

Cybersecurity

Fraud

Legal/Compliance

Cyber fraud threat management

Physical security

Threat intelligence & analytics

Monitoring

Case management/investigations

Reporting & dashboarding

Governance & risk management

Internal & external collaboration

Human capital

e.g. Appoint an HR business partner and implement cross-training of talent across pillars.

Program

e.g. Develop a consistent firmwide cyber and fraud risk assessment and taxonomy.

Tech

e.g. Establish a shared technology architecture for efficient Fusion Centre management.

Data

e.g. Use a consolidated data pool to effectively and efficiently detect anomalies.

Co-located facility: Establishing a physical facility to co-locate Fusion Center resources is critical to promote cross-functional communications.

Future directions in companies post COVID….

Expansion of Ecosystem Business Models

Ecosystem business models that encompass a network of third parties are able to adapt and change to rapidly evolving risks more effectively than traditional supplier-customer models.

Accelerated Adoption of Cloud

Whilst most organisations have adopted Cloud for a variety functions, there is likely going to be a broader reassessment of how Cloud can help to alleviate some of the recent challenges.

Redefined Meaning of a Resilient Business

Revisit disaster recovery and business continuity plans, apply lessons learnt and consider what makes a business resilient.

Augmented Reality/Virtual Operations Functions

The use of new technology could change the way businesses and users interact with each other by extending location agnostic services and capabilities and by maximising virtual experiences.

Cross Business Industry Resilience

Assessing how businesses work together during these periods could influence the way in which cross business and industry resilience is addressed in the future.

5

Q&A and wrap up

Thank you

pwc.com

This content is for general information purposes only, and should not be used as a substitute for consultation with professional advisors.