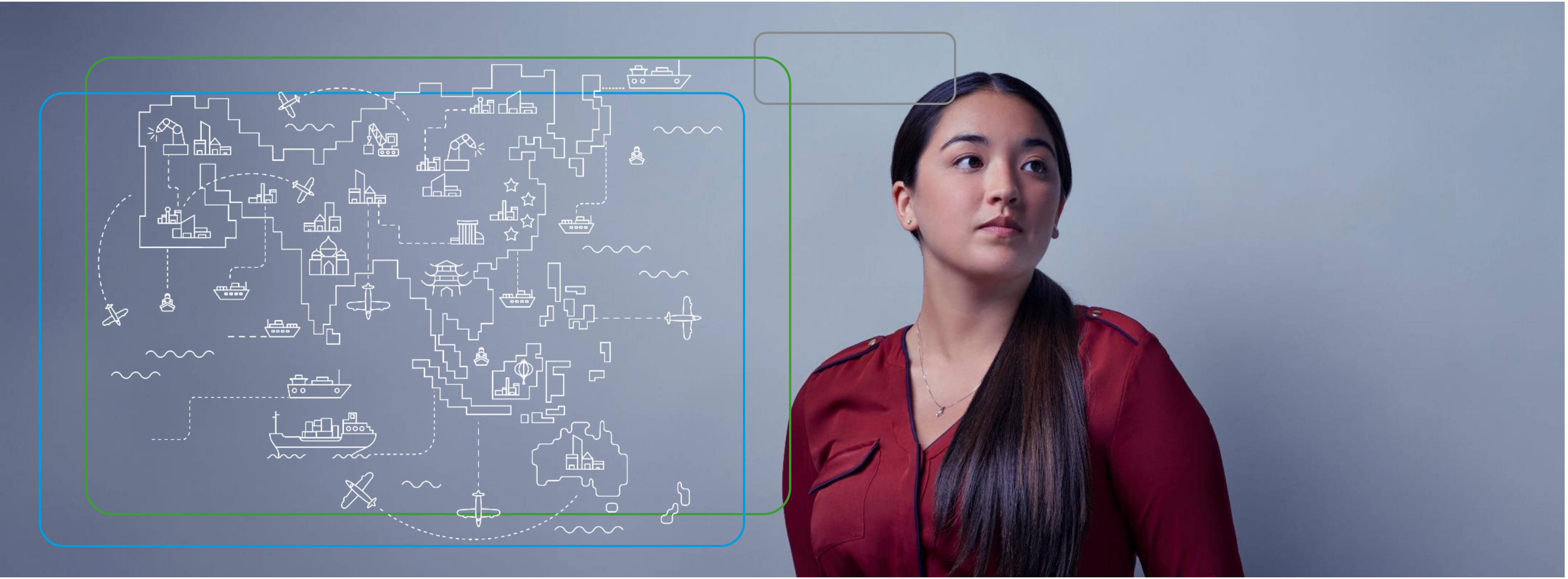


THE LATEST NEWS IN CYBER SECURITY

CREST. | PEN TEST

Now a CREST accredited company for penetration testing services in Australia, RSM provides expert services across cyber security assurance and advisory and risk consulting.

Penetration Testing, Information and Cyber Security Risk, Privacy, Digital Forensics and Incident Response, Security Transformation and Cloud Security

KEY CONTACT

Darren Booth
National Head of Security and Privacy Risk Services

T: +61 3 9286 8158
E: darren.booth@rsm.com.au
www.linkedin.com/in/darrenbooth-rsm

THE POWER OF BEING UNDERSTOOD
AUDIT | TAX | CONSULTING

RSM

Agenda

current & emerging trends

digital information footprint

cyber boundary

governance & resilience

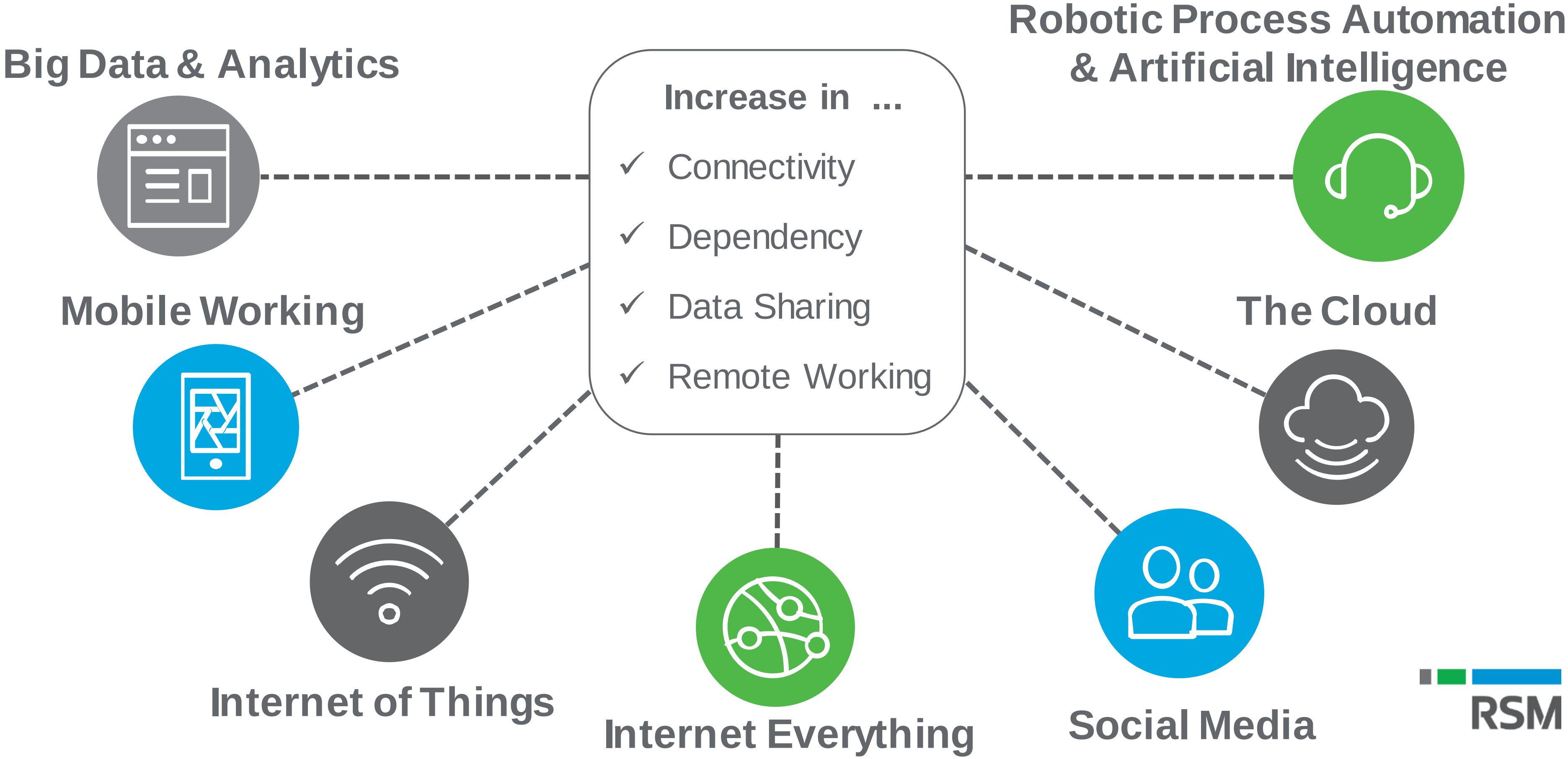
auditing approaches

audit plan

> There are only two types of companies: those that have been hacked, and those that will be.
>
> **Merging into:** those that have been hacked and will be again.

Robert Mueller (March 2012)

Current IT Trends



Increase in ...

- ✓ Connectivity
- ✓ Dependency
- ✓ Data Sharing
- ✓ Remote Working

Big Data & Analytics

Mobile Working

Internet of Things

Internet Everything

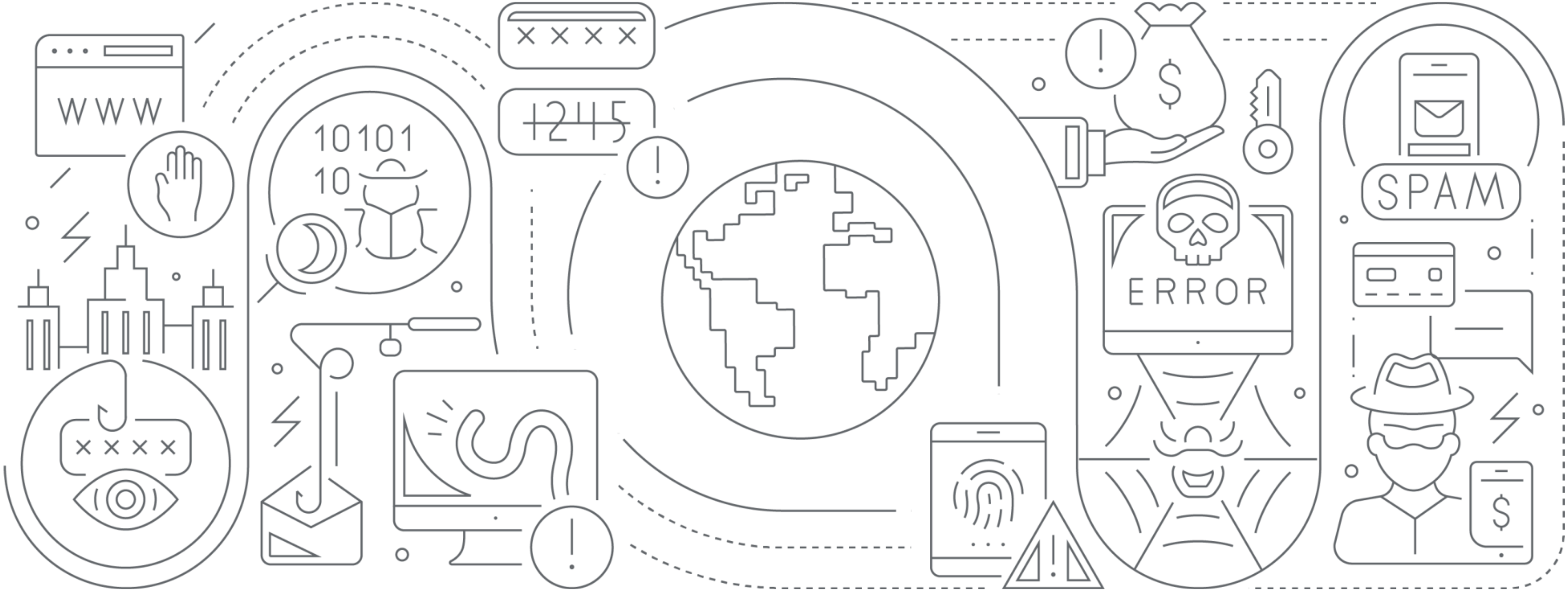
Social Media

The Cloud

Robotic Process Automation & Artificial Intelligence

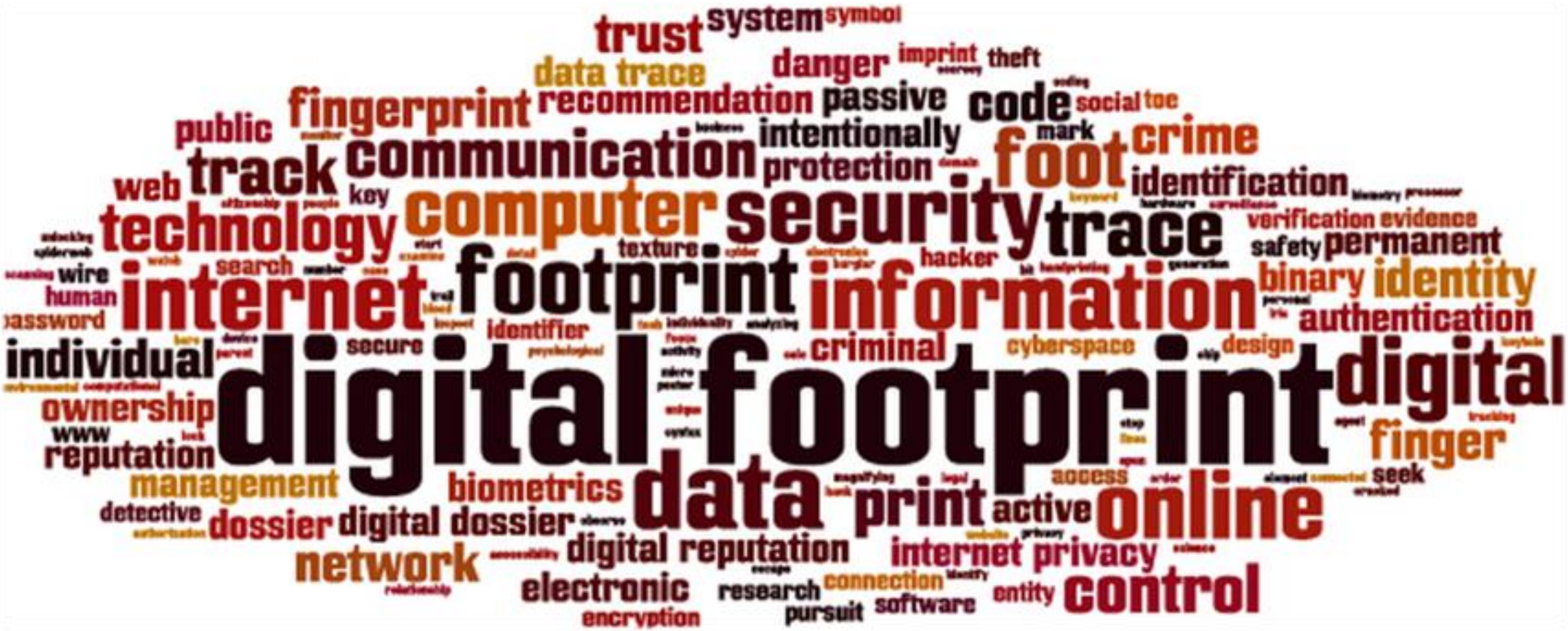
RSM

Cyber Security Risks



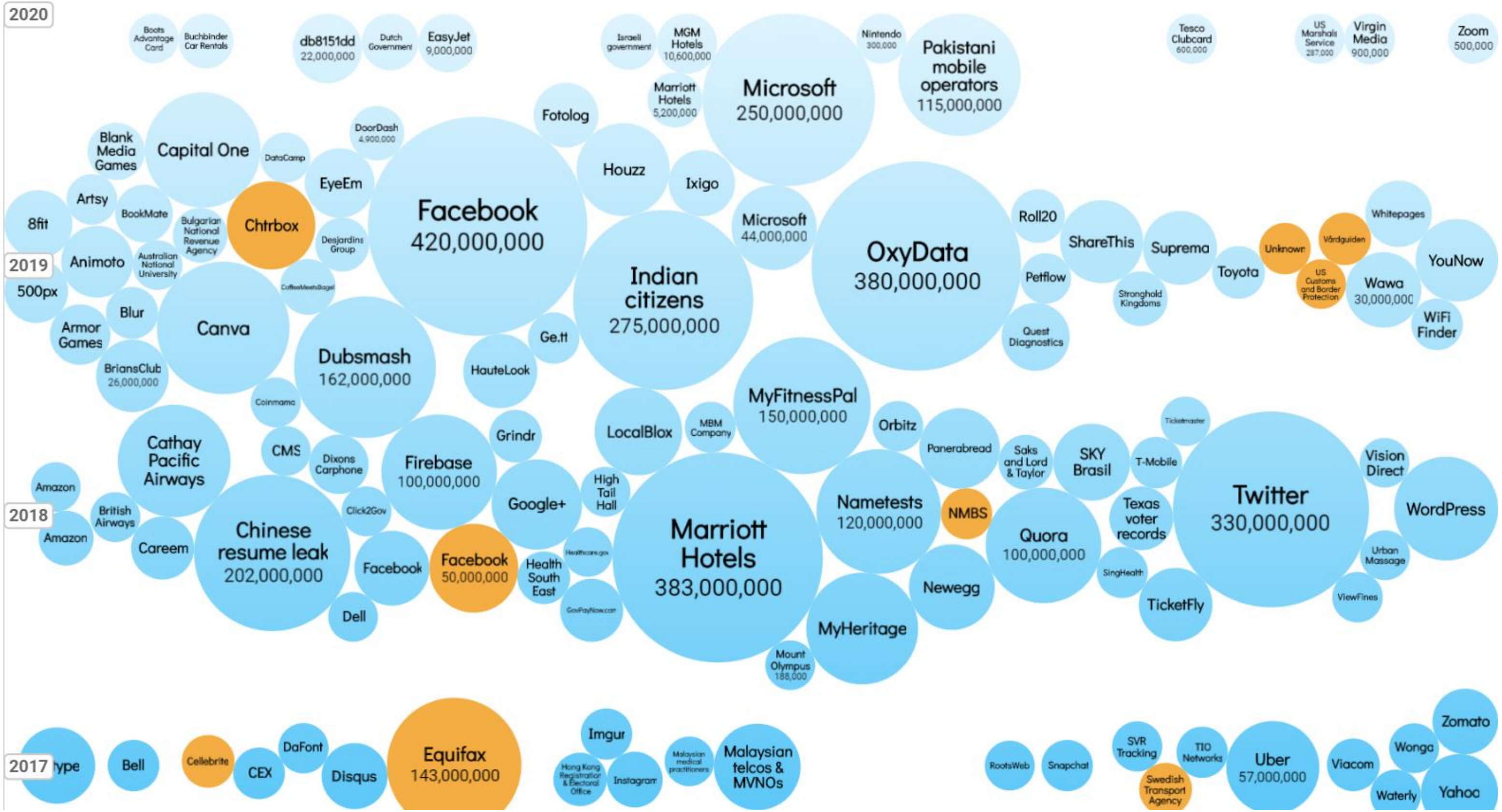
RSM

Your organisation's digital information footprint



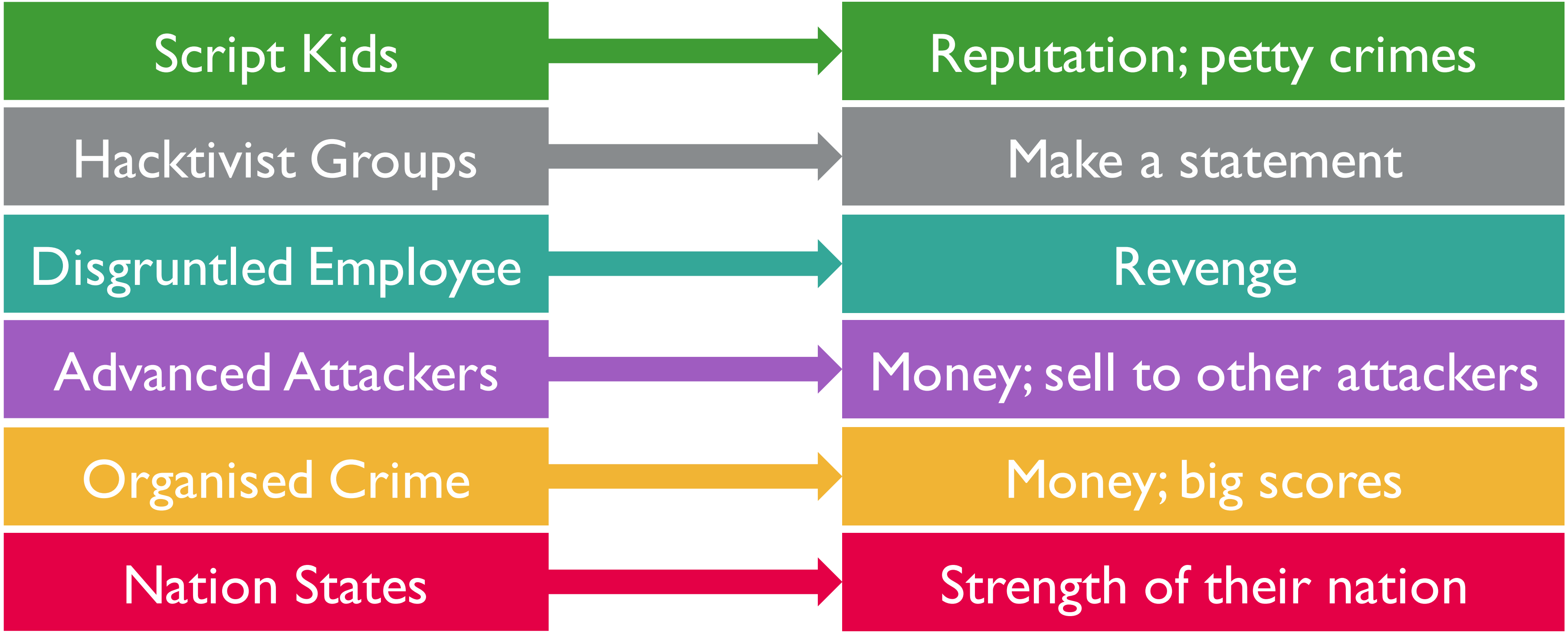
RSM

What is the scale of the issue



https://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

Threat actors



Script Kids → Reputation; petty crimes

Hacktivist Groups → Make a statement

Disgruntled Employee → Revenge

Advanced Attackers → Money; sell to other attackers

Organised Crime → Money; big scores

Nation States → Strength of their nation

RSM

What has changed?

Ransomware is the new payload of choice

Ransomware: 3.8m attacks in 2015 rose to 205m in 2018

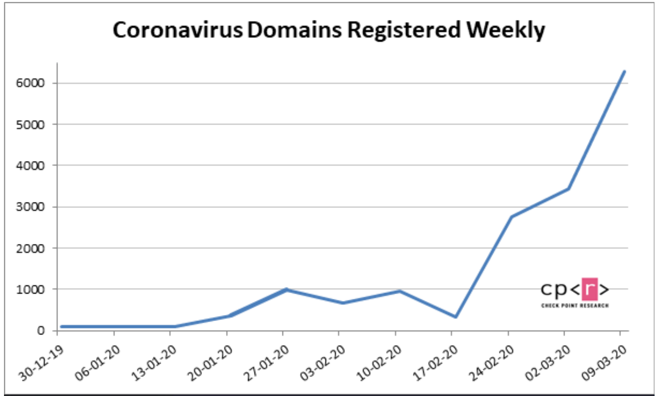
Social (people) attacks used in 51% of ransomware cases in 2018

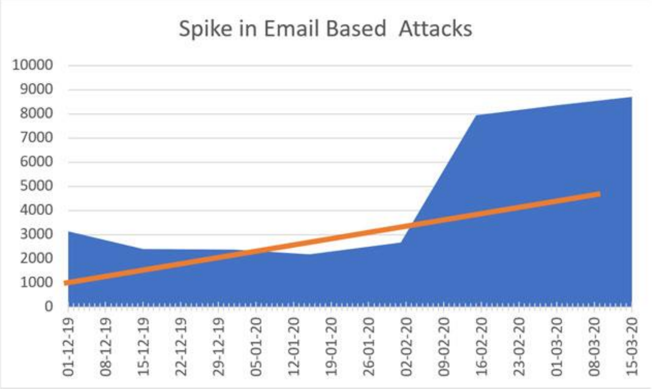
Australia is ranked fifth in the number of exposed records by country.

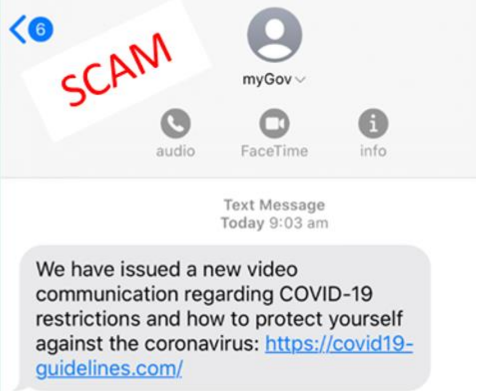
Source: Malwarefox Ransomware Report 2019
https://www.malwarefox.com/ransomware-statistics-infographic/

RSM

What has changed with COVID-19

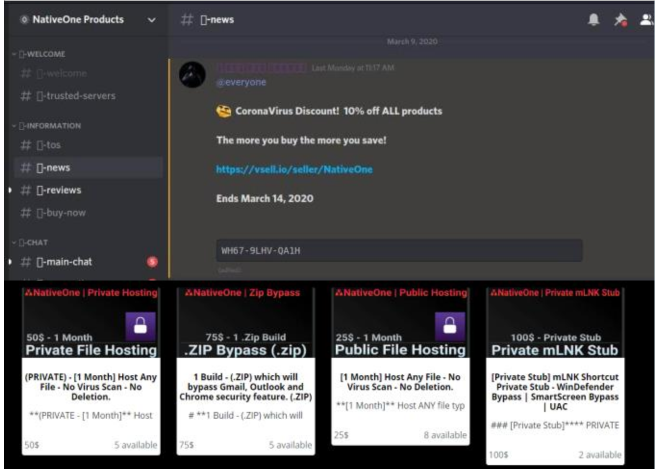






Text Message
Today 9:03 am

We have issued a new video communication regarding COVID-19 restrictions and how to protect yourself against the coronavirus: https://covid19-guidelines.com/



March 9, 2020

[redacted] Last Monday at 11:17 AM

@everyone

CoronaVirus Discount! 10% off ALL products

The more you buy the more you save!

https://vsell.io/seller/NativeOne

Ends March 14, 2020

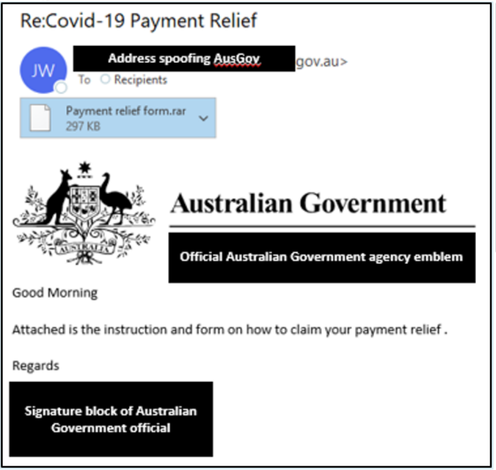
```
WH67-9LHV-QA1H
```

NativeOne | Private Hosting
50$ - 1 Month
Private File Hosting
(PRIVATE) - [1 Month] Host Any File - No Virus Scan - No Deletion.
(PRIVATE - [1 Month] Host
50$ 5 available

NativeOne | Zip Bypass
75$ - 1 .Zip Build
.ZIP Bypass (.zip)
1 Build - (.ZIP) which will bypass Gmail, Outlook and Chrome security feature. (.ZIP)
**1 Build - (.ZIP) which will
75$ 5 available

NativeOne | Public Hosting
25$ - 1 Month
Public File Hosting
[1 Month] Host Any File - No Virus Scan - No Deletion.
[1 Month] Host ANY file typ
25$ 8 available

NativeOne | Private mLNK Stub
100$ - Private Stub
Private mLNK Stub
[Private Stub] mLNK Shortcut Private Stub - WinDefender Bypass | SmartScreen Bypass | UAC
[Private Stub]**** PRIVATE
100$ 2 available


Re:Covid-19 Payment Relief

JW Address spoofing AusGov gov.au>

To ○ Recipients

Payment relief form.rar
297 KB

Australian Government

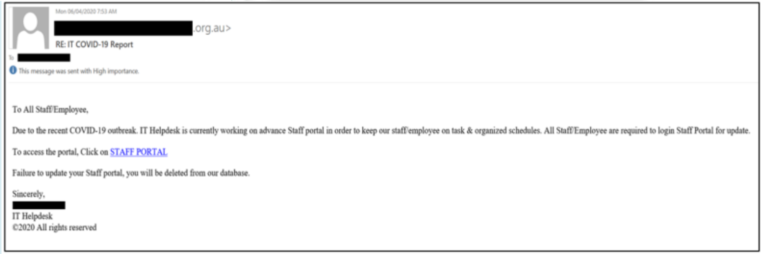
Official Australian Government agency emblem

Good Morning

Attached is the instruction and form on how to claim your payment relief .

Regards

Signature block of Australian Government official


Mon 06/04/2020 7:53 AM

[redacted].org.au>

RE: IT COVID-19 Report

To [redacted]

This message was sent with High importance.

To All Staff/Employee,

Due to the recent COVID-19 outbreak. IT Helpdesk is currently working on advance Staff portal in order to keep our staff/employee on task & organized schedules. All Staff/Employee are required to login Staff Portal for update.

To access the portal, Click on STAFF PORTAL

Failure to update your Staff portal, you will be deleted from our database.

Sincerely,
[redacted]
IT Helpdesk
©2020 All rights reserved

RSM

Remote working environment changes

Desktops and BYOD

- No longer behind the corporate firewall and protection, reliant on home security.

Rushed Virtual Private Network (VPN) & Firewall changes

- Capacity to support the workforce
- Legacy systems | • Change management

Data loss prevention

- People at home act different to in the office
- Increased use of cloud storage / sharing

‘Noise’ in monitoring tools

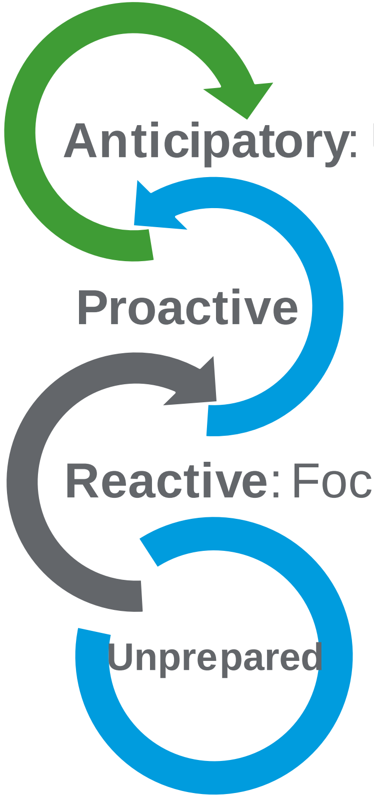
- Phishing attacks
- More remote access

Third party resources

- Rushed roll-out by vendors
- Use of new tools without usual training

> Cyber resilience refers to an organisation’s ability to continuously deliver the intended outcome despite adverse cyber events.

Approach aligned to maturity



Anticipatory: Understand, prevent, detect and contain emerging threats

Proactive

Reactive: Focused on current protection

Unprepared

Control types

PREVENTIVE

- Reduce the likelihood of a successful attack
- Minimise impact

DETECTIVE

- Detect attacks
- Alert the organisation to the situation

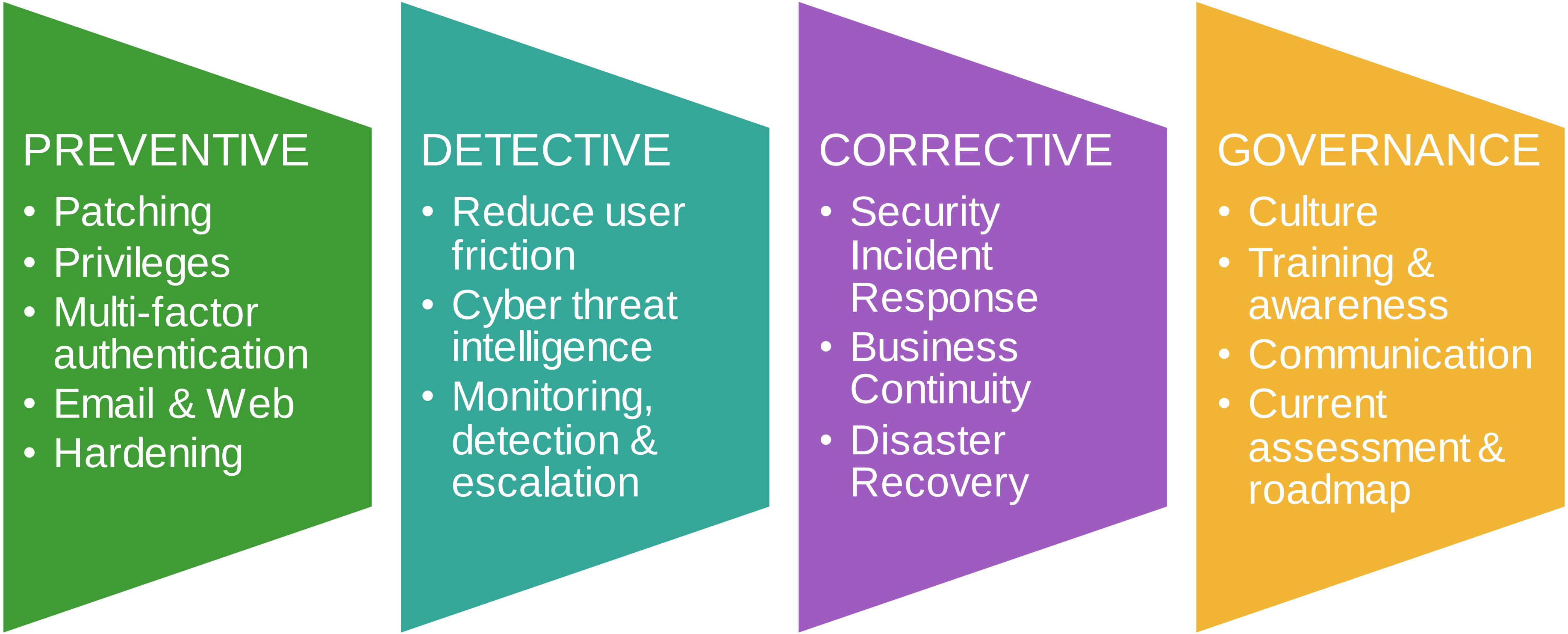
CORRECTIVE

- Respond to an incident
- Recover the organisation

GOVERNANCE

- Manage cyber security
- Monitor improvements and success

Cyber Resilience Activities



PREVENTIVE

- Patching
- Privileges
- Multi-factor authentication
- Email & Web
- Hardening

DETECTIVE

- Reduce user friction
- Cyber threat intelligence
- Monitoring, detection & escalation

CORRECTIVE

- Security Incident Response
- Business Continuity
- Disaster Recovery

GOVERNANCE

- Culture
- Training & awareness
- Communication
- Current assessment & roadmap

Standards and Guidelines

NIST
CYBERSECURITY FRAMEWORK

International Organization for Standardization
ISO
27001

CSA cloud security alliance®
CCMv3.0.1™

Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

CIS. Center for Internet Security®
CIS Controls™

Australian Government Information Security Manual

Strategies to Mitigate Cyber Security Incidents

Essential Eight Explained

NIST
NIST Special Publication 800-53

Cyber security audit plans

Cyber Security Maturity Assessment

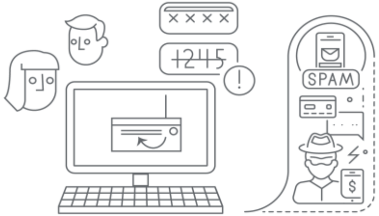
Cyber Threat Risk Assessment & Cyber Security Control Framework

Email and website filtering & threat prevention

Security Awareness & Social Engineering Tests – Phishing, vishing, physical

Third Party / Vendor Security Risk Management

Board Cyber Security Reporting



Penetration Testing – External, Internal, Wireless, Web Application, APIs

Privileged Access Management – Using tools like ADRecon

Firewall Configurations – Using tools like Nipper

Configuration Hardening – Source Code, CIS Benchmark, Office365, unsupported servers

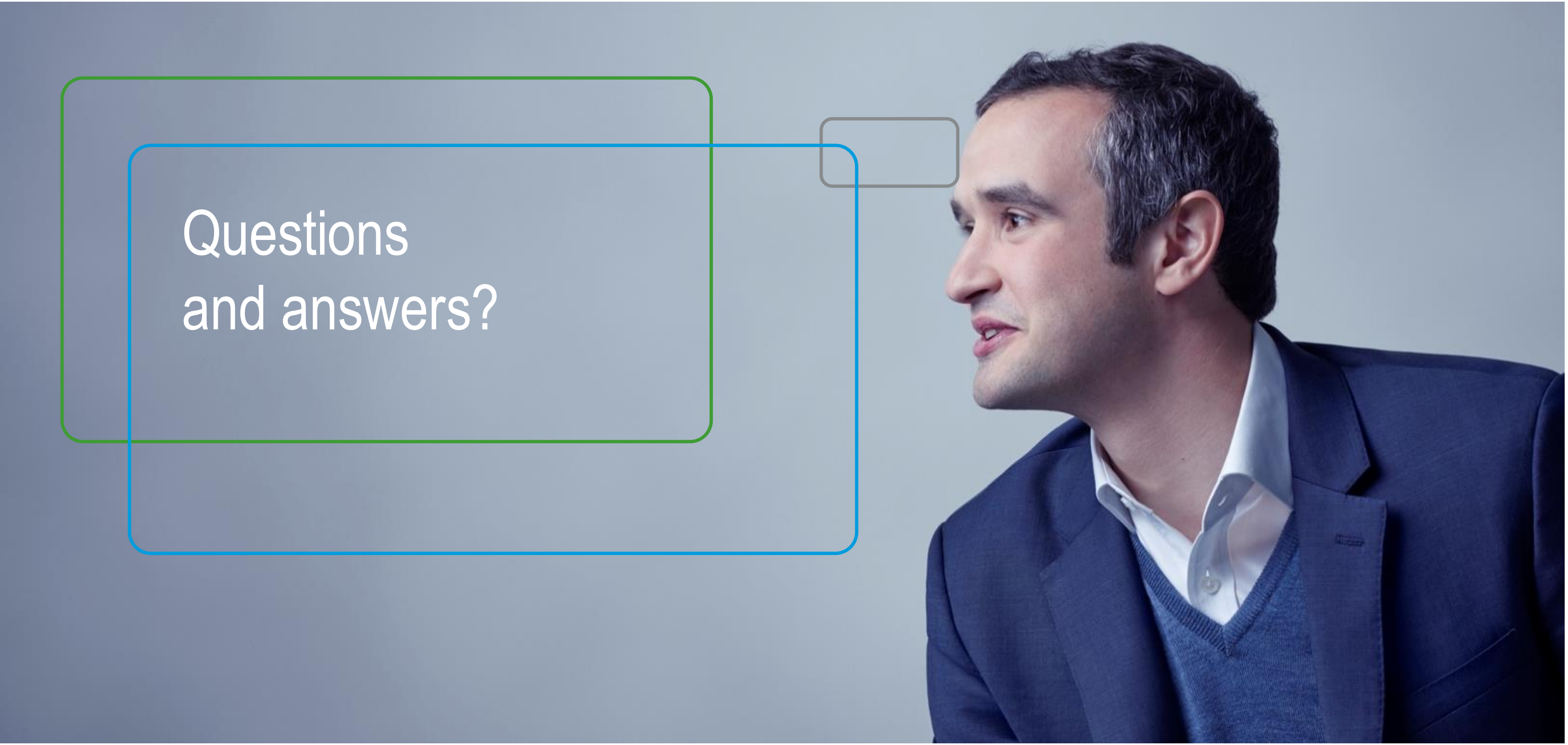
Cyber Threat Intelligence – due diligence of exposed data in deep and dark web

Vulnerability Management – Using scanning tools like Tenable Nessus

Data Loss Detection and Data Discovery (email, cloud, system leakage)

Security Event Monitoring – Audit, Log, Monitor, Review (Mitre Att&ck)

Information Asset Classification (& Segmentation)



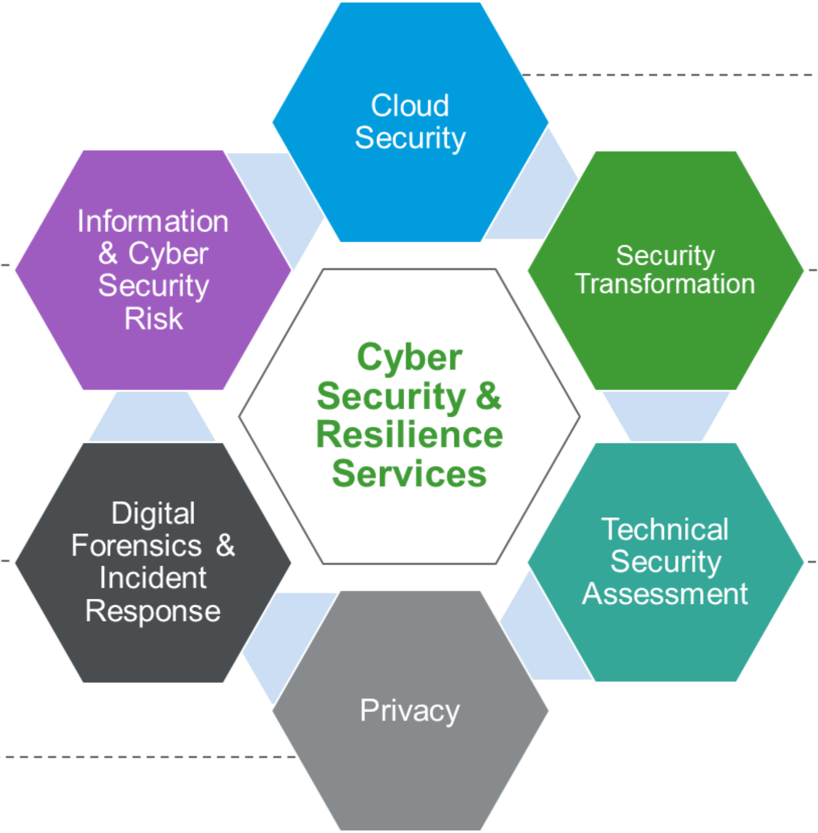
Questions and answers?

Cyber Security Services

- Cyber security maturity
- Security governance
- Information security management framework
- Cyber / Threat risk assessment
- IT audit & assurance
- Awareness & training
- Data mapping
- Vendor / Third-party risk assessment
- Due diligence
- Industry specific standards
- PCI DSS readiness
- PCI DSS facilitated self-assessment
- DevSecOps
- Virtual Chief Information Security Officer (vCISO)

- Data preservation & analysis
- Information security incidents
- Data breach
- E-discovery services
- Malware analysis
- Email compromise
- Data recovery
- Cyber tabletop exercises

- Data governance
- Data privacy program
- Data discovery & classification
- Privacy impact assessment
- Vendor / Third-party data transfer
- State & Federal regulations
- International regulations: GDPR



Cyber Security & Resilience Services

Cloud Security

Security Transformation

Technical Security Assessment

Privacy

Digital Forensics & Incident Response

Information & Cyber Security Risk

- Cloud governance & risk management
- AWS, Microsoft Azure, Google Cloud Platform assurance
- Microsoft 365 & Office 365 configurations
- SaaS assurance
- Vendor management

- Security strategy
- Security design & implementation
- Security architecture
- Project management & assurance
- Vendor selection
- Identity & access management
- Privileged access
- Security incident & event management (SIEM)
- Data loss prevention (DLP)
- Firewall assessment

- Ethical hacking
- Vulnerability assessments
- Penetration testing
- Red team
- Breach & attack simulation
- Cyber threat intelligence
- Mobile, APIs & web applications
- Applications & databases
- Cloud services
- Wireless testing
- Social engineering: phishing, telephone, physical
- Configuration hardening

CREST. PEN TEST

This presentation is intended as general information only and should not be considered as advice on any matter and should not be relied upon as such. The information in this presentation has been prepared without taking into account any individual objectives, financial situation or needs. No member of RSM Australia, no any of their employees or directors gives any warranty of accuracy or reliability nor accepts any liability in any other way including by reason of negligence for any errors or omissions contained in the presentation, to the extent permitted by law.

Liability limited by a scheme approved under Professional Standards legislation.

RSM