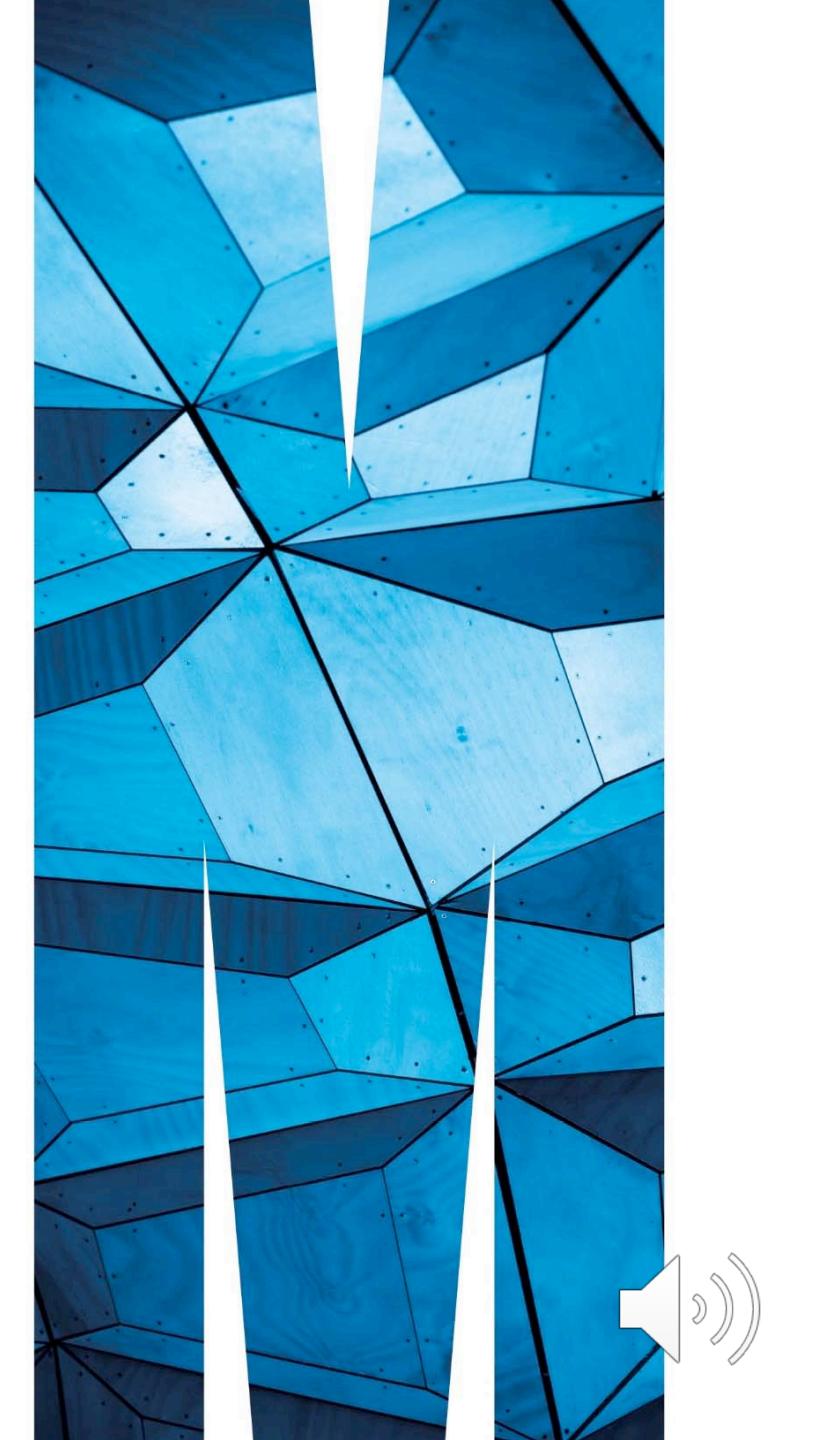


FIT1049: IT professional practice

Week 11 Wrap-up: IT security risks and crisis management

S2, 2020



IT/data security breach: A matter of ‘when’ not ‘if’

Home > Security

OPINION

Top cybersecurity facts, figures and statistics for 2018

Some hard numbers from studies and surveys give you a sense of the state of cybersecurity.



By **Josh Fruhlinger**

CSO | OCTOBER 10, 2018 09:52 AM PT

11 top cybersecurity statistics at-a-glance

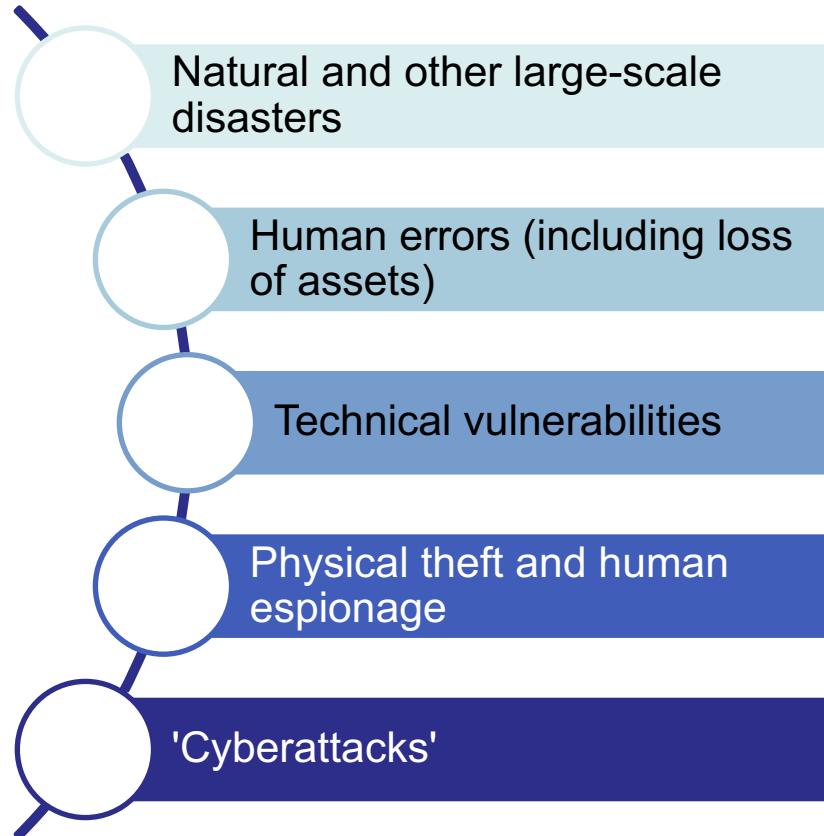
- 90% of remote code execution attacks are associated with cryptomining.
- 92% of malware is delivered by email.
- 56% of IT decision makers say targeted phishing attacks are their top security threat.
- 77% of compromised attacks in 2017 were fileless.
- The average ransomware attack costs a company \$5 million.
- It takes organizations an average of 191 days to identify data breaches.
- 69% of companies see compliance mandates driving spending.
- 88% companies spent more than \$1 million on preparing for the GDPR.
- 25% of organizations have a standalone security department.
- 54% of companies experienced an industrial control system security incident
- 61% of organizations have experienced an IoT security incident

([Fruhlinger, 2018](#))



([Sobers, 2019](#); also see the rest of the infographic too...)

Common causes of IT security (and data) breach



([OAIC, 2018](#); reported causes of data breach, based on NDBS data)

Motivations behind deliberate IT/data security breach

Personal satisfaction

Politically or ethically motivated (including whistleblowers)

Financial gains

Competitive advantage

Social engineering for political and social influences



Potential consequences and impacts

Financial loss

Destruction of/disruption to the critical infrastructure

Loss of trust, reputation and public confidence

Compromise of social orders



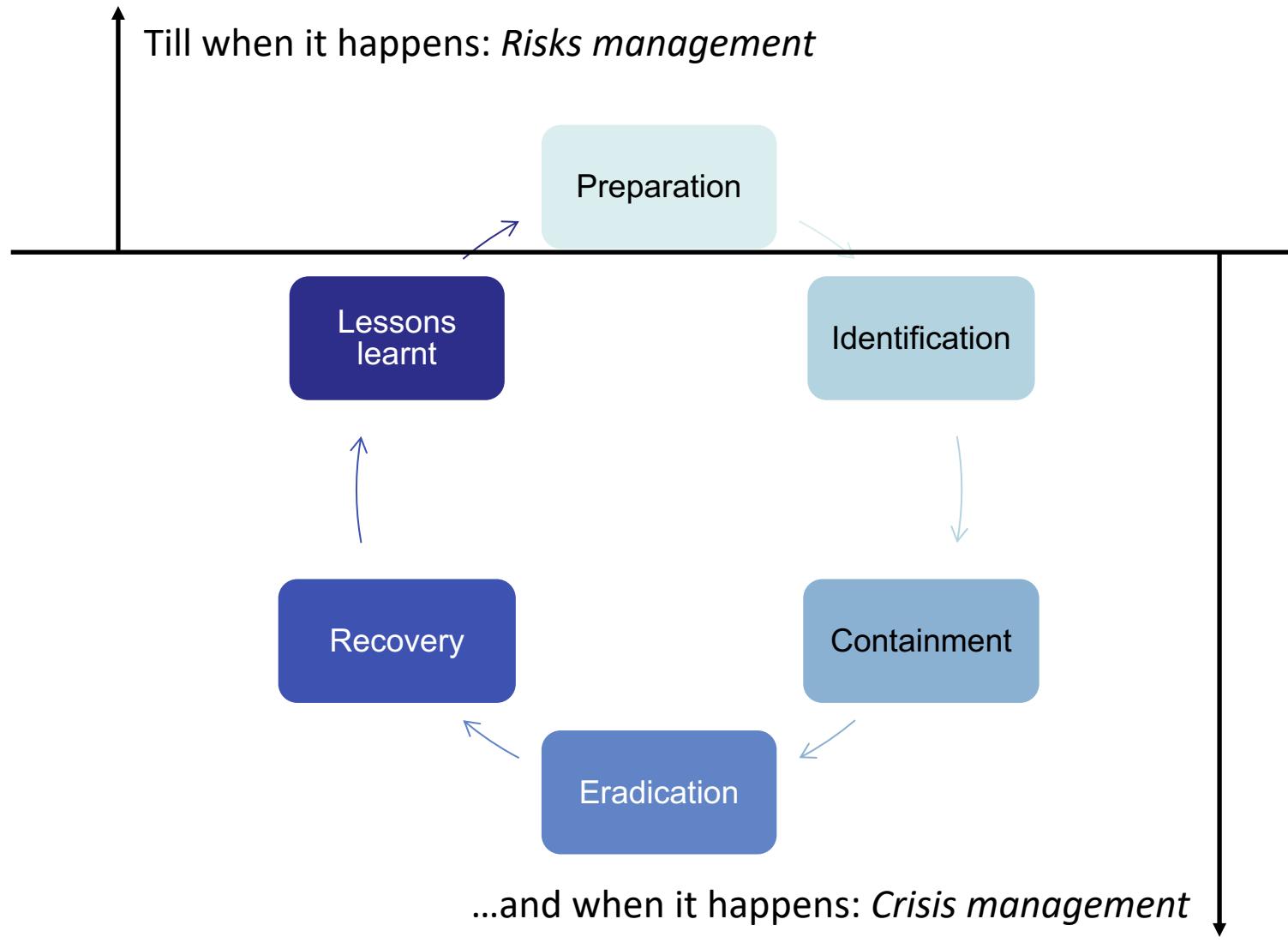
Once a piece of ransomware has got hold of your valuable information, there is very little you can do to get it back other than accede to the attacker's demands. Ransomware, a type of malware that holds a computer to ransom, has become [particularly prevalent](#) in the past few years and [virtually unbreakable encryption](#) has made it an even more powerful force.

Ransomware is typically delivered by [powerful botnets](#) used to send out millions of malicious emails to randomly targeted victims. These aim to extort [relatively small](#) amounts of money (normally £800-£500, but more in recent times) from as many victims as possible. But according to police officers we have interviewed from UK cybercrime units, ransomware attacks are becoming increasingly targeted at high-value victims. These are usually businesses that can afford to pay very large sums of money, up to [£1,000,000](#) to get their data back.

(Connolly & Wall, 2019)



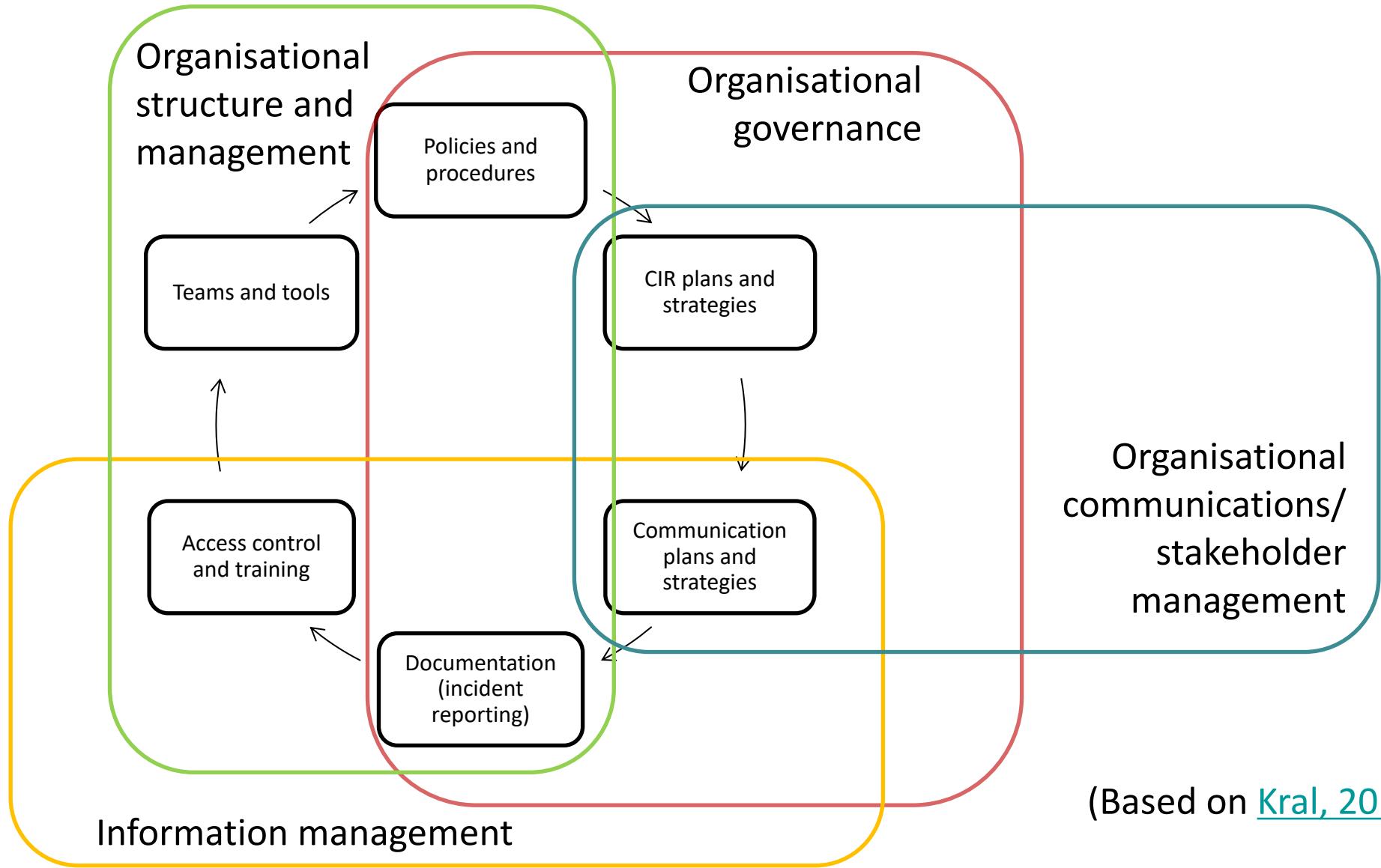
Risks and crisis management



(Based on [Kral, 201](#))

6

'Preparation' as risks management



Organisational governance and IT security

What are the risks?

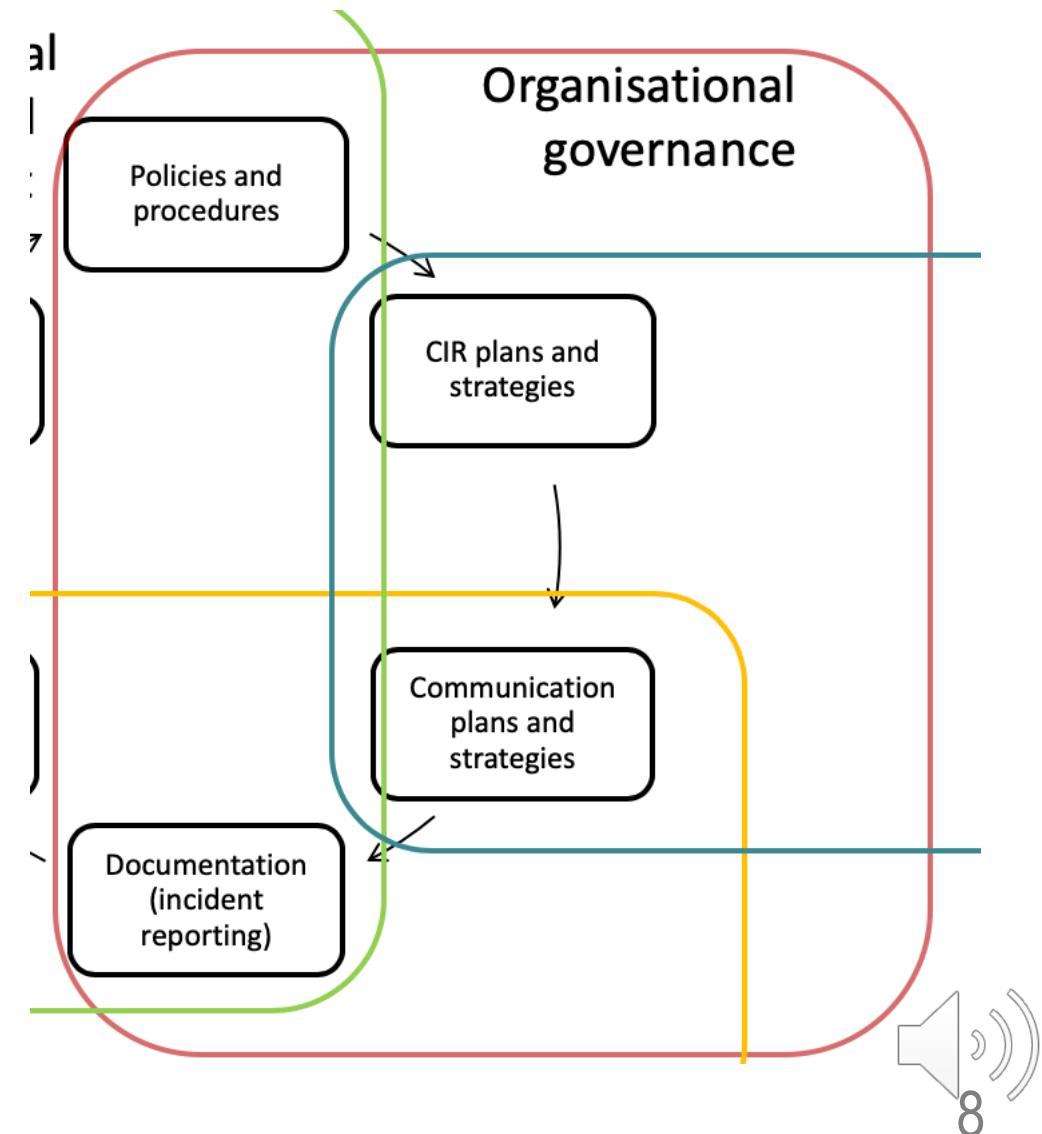
What is considered as an incident?

Who is accountable?

Who to involve?

Who to inform?

How to respond?



Guess who?

78,000+ clients

18,000+ staff

\$2.5bn+ revenue

International presence across five
countries spread over three continents

You probably heard about this
organisation...



Monash University Policy

Policy Title	ICT Security and Risk Policy
Date Effective	01-August-2014
Review Date	01-August-2017
Policy Owner	Chief Information Officer
Category	Operational
Version Number	1.1
Content Enquiries	IT Service Desk - http://monash.edu/esolutions/contact/
Scope	<ul style="list-style-type: none"> • All Australian campuses • All staff, students and other Authorised Users
Purpose	<p>To apply proportionate and effective management of ICT security risks throughout Monash University to enable the conduct of the University's business and necessary protection of the University's people, information and assets.</p> <p>To authorise the establishment of an IT Security and Risk Steering Committee and the Information Security Management System (ISMS).</p>

POLICY STATEMENT

The Chief Information Officer is authorised to develop and implement ICT Security related Procedures, and the University Information Security Management System (ISMS).

The University's Information Security Management System (ISMS) will ensure sufficient and proportionate security controls are implemented to adequately protect information assets. The ISMS is part of an overall management system, based on a business risk approach which includes organisational structure, policies, planning activities, responsibilities, practices, procedures, processes and resources.

The Chief Information Officer is responsible for assessing and monitoring the university's IT risk profile, ensuring active management of the IT risk register and related controls.

The IT Security and Risk Steering Committee will maintain oversight of the university's IT risk profile, and ICT Security related procedures and systems.

This policy applies to all Authorised Users of Monash University in their use of ICT Facilities and Services.

The University reserves the right to access, review and monitor Monash ICT Facilities and Services, and the University reserves the right to remove access or disconnect systems and services where risk is identified to the University.

Associated Framework: [ICT Security and Risk Framework](#)

Supporting Procedures	ICT Security Procedures
Responsibility for implementation	Chief Information Officer
Status	Revised

Approval Body	Name: Chief Operating Officer and Senior Vice-President (Administration) Meeting: n/a Date: 01-August-2014 Agenda item: n/a	Education Services for Overseas Students Act 2000 (Commonwealth) - specifically The National Code 2007 , Standard 3.1(d) Biological Studies (Confidentiality) Act 1981 (Commonwealth) - where relevant to a research project (needed)
Endorsement Body	Name: Chief Information Officer Meeting: n/a Date: 01-August-2014 Agenda item: n/a	Monash University (Council) Regulations Part 7 Monash University (Vice-Chancellor) Regulations Part 5 Monash University Statute
Definitions	<p>Authorised Users: All people authorised to use the ICT Facilities and Services for any purpose, including but not limited to University, members of partner organisations which Monash has an interest, honorary and alumni and users accessing via a federated arrangement.</p> <p>Authorised Staff: All people authorised by the CIO to monitor accounts, files, stored data and network data, and to disconnect IT equipment in the event of an IT security breach. Normally eSolutions Division staff.</p> <p>CIO: Chief Information Officer</p> <p>ICT: Information and Communications Technology</p> <p>ICT Facilities and Services: Shall include but not be limited to owned computers and associated ICT networks, internet access, email, hardware, data storage, computer accounts, software (both proprietary and those developed by the University) and telephony services; any computer or device owned or operated by someone other than the University when connecting to the University information network or being used for University Business; any computer account, software or information provided or created for University Business; all physical spaces using ICT and designated for teaching, study, research and administration across the University; ICT services provided by third parties that have been engaged by the University, including any hosted or similar service through which University information is stored or services are provided to enable Users to undertake University Business; and ICT services made accessible to Monash users through federated access arrangements.</p> <p>ISMS: Information Security Management System – set of standards-based documents that govern operation of the key information security management process. ISMS is that part of the overall management system, based on a risk approach, to establish, implement, operate, monitor, review, and improve information security.</p>	ICT Security and Risk Framework Electronic Information Security Policy Social Media Policy Acceptable Use of Information Technology Facilities by Students Policy Information Technology Use Policy - Staff & Other Authorised Users
Legislation Mandating Compliance	<p>Monitoring: To Monitor: Tasks (including testing and scanning) undertaken by Authorised Staff to ensure maintenance of security of ICT services and systems</p> <p>University: Monash University</p> <p>University Business: Any activity conducted either in the course of employment or as part of or related to a University course or other University activity that is not purely personal.</p>	Privacy Act 2009 (Victoria) - note Information Privacy Principles within the Act (Section 14 and Schedule 1) Privacy Act 1988 (Commonwealth) Privacy Amendment (Enhancing Privacy Protection) Act 2012 (Commonwealth) Health Records Act 2001 (Vic) - note Health Privacy Principles within Act (Section 19 and Schedule 1) Higher Education Support Act 2003 (Commonwealth) - note Part 5-4 Management of Information, and specifically section 179-10 Use of Personal Information

(Monash University, 2017a)

ICT Security and Risk Framework

Parent Policy
ICT Security and Risk Policy

Definitions

Scope

All Australian campuses

Version Number

1.0

Effective Date

10/08/2015

Table of Contents

[1 Organisation of ICT Security and Risk Management](#)

[1.1 Internal Organisation](#)

[2 Human Resource Security](#)

[2.1 Prior to People Accessing the University's Electronic Information](#)

[2.2 People's Information Security Responsibilities](#)

[2.3 Termination or Change of People's Responsibilities](#)

[3 Asset Management](#)

[3.1 Responsibility for The University's Electronic Information, Information Systems, Information Services, and Information System Facilities](#)

[3.2 Information Classification, Management and Handling](#)

[4 Access Control](#)

[4.1 Access control requirements and management](#)

[4.2 People's responsibilities](#)

[4.3 Information System and Information Service Access Control](#)

[5 Physical and Environmental Security](#)

[5.1 Secure Areas](#)

[5.2 Information Systems](#)

[6 Operations Security](#)

[6.1 Operational Procedures and Responsibilities](#)

[6.2 Key Management](#)

[6.3 Logging and Monitoring](#)

[6.4 Control of Operational Software](#)

[6.5 Technical Vulnerability Management](#)

[6.6 Mobile Devices and Remote Working](#)

[7 Communications Security](#)

[7.1 Network and Communications Management](#)

[8 Security in Development and Implementation](#)

[8.1 Defined Requirements](#)

[8.2 Security in the Development and Implementation Lifecycle](#)

[9 External Party Relationship Management](#)

[9.1 Relationships with External Parties](#)

[9.2 External Service Provider Delivery Management](#)

[9.3 Information Services Provided to External Parties](#)

[9.4 External Information Services Security Management](#)

[10 Information Security Incident Management](#)

[10.1 Information Security Incident Management](#)

[11 Disaster Recovery and Business Continuity Management](#)

[11.1 Information Security Continuity](#)

[11.2 Disaster Recovery](#)

[12 Compliance](#)

[12.1 Compliance with External and Contractual Requirements](#)

[12.2 Information Systems Audit Considerations](#)

[12.3 Compliance with Information Security Policy and Procedures](#)

10. Information Security Incident Management

Operational Responsibilities:

Responsibility	Scope
IT Security and Risk Manager	Security related aspects of incident management
Service Management Office Manager	IT incident management

Objective: To ensure a consistent and effective approach to the management of information security incidents, including communication on security events, threats and vulnerabilities, as part of an overall incident management process. #ISO27002.2013:16.1

10.1 Information Security Incident Management

10.1.1 Responsibilities and Procedures

C110 Incident management responsibilities and procedures shall be developed, maintained and implemented, and include effective, risk-based response to information security incidents, in consideration of the University's electronic information security classification. #ISO27002.2013:16.1.1, #LSA:14.6

10.1.2 Reporting Events and Weaknesses

C111 Any suspected or actual information security event, weakness, and technology risk related event shall be reported through approved procedures as quickly as possible. #ISO27002.2013:16.1.2, #ISO27002.2013:16.1.3, #LSA:3.7, #LSA:14.6

10.1.3 Assessment and Response

C112 Information security events, weaknesses, and ICT risk related events shall be risk assessed. Information security incidents shall be classified based on approved, risk-based criteria and the incident management priority matrix. #ISO27002.2013:16.1.4, #LSA:14.6

C133 Information security incidents shall be responded to in accordance with the approved incident response procedures. #ISO27002.2013:16.1.5, #LSA:14.6

10.1.4 Learning From Incidents

C114 Incident management procedures shall include the use of a post-incident review process, and the knowledge gained from analysing and resolving information security incidents shall be used to reduce the likelihood or impact of future incidents. #ISO27002.2013:16.1.6

10.1.5 Collection of Evidence

C115 Evidence shall be identified, collected, acquired, and preserved according to established, documented, and maintained procedures, in consideration of The University's electronic information security classification. #ISO27002.2013:16.1.7



Federal Agency Incident Categories

Category	Name	Description	Reporting Timeframe
CAT 0	Exercise/Network Defense Testing	This category is used during state, federal, national, international exercises and approved activity testing of internal/external network defenses or responses.	Not Applicable; this category is for each agency's internal use during exercises.
CAT 1	*Unauthorized Access	In this category an individual gains logical or physical access without permission to a federal agency network, system, application, data, or other resource	Within one (1) hour of discovery/detection.
CAT 2	*Denial of Service (DoS)	An attack that <i>successfully prevents or impairs</i> the normal authorized functionality of networks, systems or applications by exhausting resources. This activity <i>includes</i> being the victim or participating in the DoS.	Within two (2) hours of discovery/detection if the successful attack is still ongoing and the agency is unable to successfully mitigate activity.
CAT 3	*Malicious Code	<i>Successful</i> installation of malicious software (e.g., virus, worm, Trojan horse, or other code-based malicious entity) that infects an operating system or application. Agencies are NOT required to report malicious logic that has been <i>successfully quarantined</i> by antivirus (AV) software.	Daily
CAT 4	*Improper Usage	A person violates acceptable computing use policies.	
CAT 5	Scans/Probes /Attempted Access	This category includes any activity that seeks to access or identify a federal agency computer, open ports, protocols, service, or any combination for later exploit. This activity does not directly result in a compromise or denial of service.	
CAT 6	Investigation	<i>Unconfirmed</i> incidents that are potentially malicious or anomalous activity deemed by the reporting entity to warrant further review.	

*Defined by NIST Special Publication 800-6

[\(InfoSecNirvana, 2015\)](#)

[\(InfoSecNirvana, 2015\)](#)

Incident Category	Description
Denial of service	DOS or DDOS attack.
Forensics	Any forensic work to be done by CSIRT
Compromised Information	Attempted or successful destruction, corruption, or disclosure of sensitive corporate information or Intellectual Property.
Compromised Asset	Compromised host (root account, Trojan, rootkit), network device, application, user account. This includes malware-infected hosts where an attacker is actively controlling the host.
Unlawful activity	Theft / Fraud / Human Safety / Child Porn. Computer-related incidents of a criminal nature, likely involving law enforcement, Global Investigations, or Loss Prevention.
Internal Hacking	Reconnaissance or Suspicious activity originating from inside the Company corporate network, excluding malware.
External Hacking	Reconnaissance or Suspicious Activity originating from outside the Company corporate network (partner network, Internet), excluding malware.
Malware	A virus or worm typically affecting multiple corporate devices. This does not include compromised hosts that are being actively controlled by an attacker via a backdoor or Trojan. (See Compromised Asset)
Email	Spoofed email, SPAM, and other email security-related events.
Consulting	Security consulting unrelated to any confirmed incident.
Policy Violations	Sharing offensive material, sharing/possession of copyright material. Deliberate violation of InfoSec policy. Inappropriate use of corporate asset such as computer, network, or application. Unauthorized escalation of privileges or deliberate attempt to subvert access controls



Information security guidelines

- Application Security Guideline
- Change Management Guideline
- Cryptography Guideline
- Digital Backup Guideline
- Information Handling Guideline
- IT Disaster Recovery Guideline
- IT Third-Party Management Guideline
- Minimum Security Standards
- Platform Security Guideline
- Security Incident Management Guideline
- User Access Control Guideline
- Vulnerability Management Guideline



(Monash University, 2019b)

Monash University Standard

Standard Title	Information Handling Standard
Parent Procedure	Electronic Information Security Minimum Security Controls Procedure
Date Effective	01 Sep 2017
Review Date	01 Mar 2022
Version Number	1.0
Purpose	The purpose of this standard is to provide the minimum guidelines for the labeling, handling, retention and destruction of Monash University owned or managed information.
STANDARD STATEMENT	

1. General Requirements

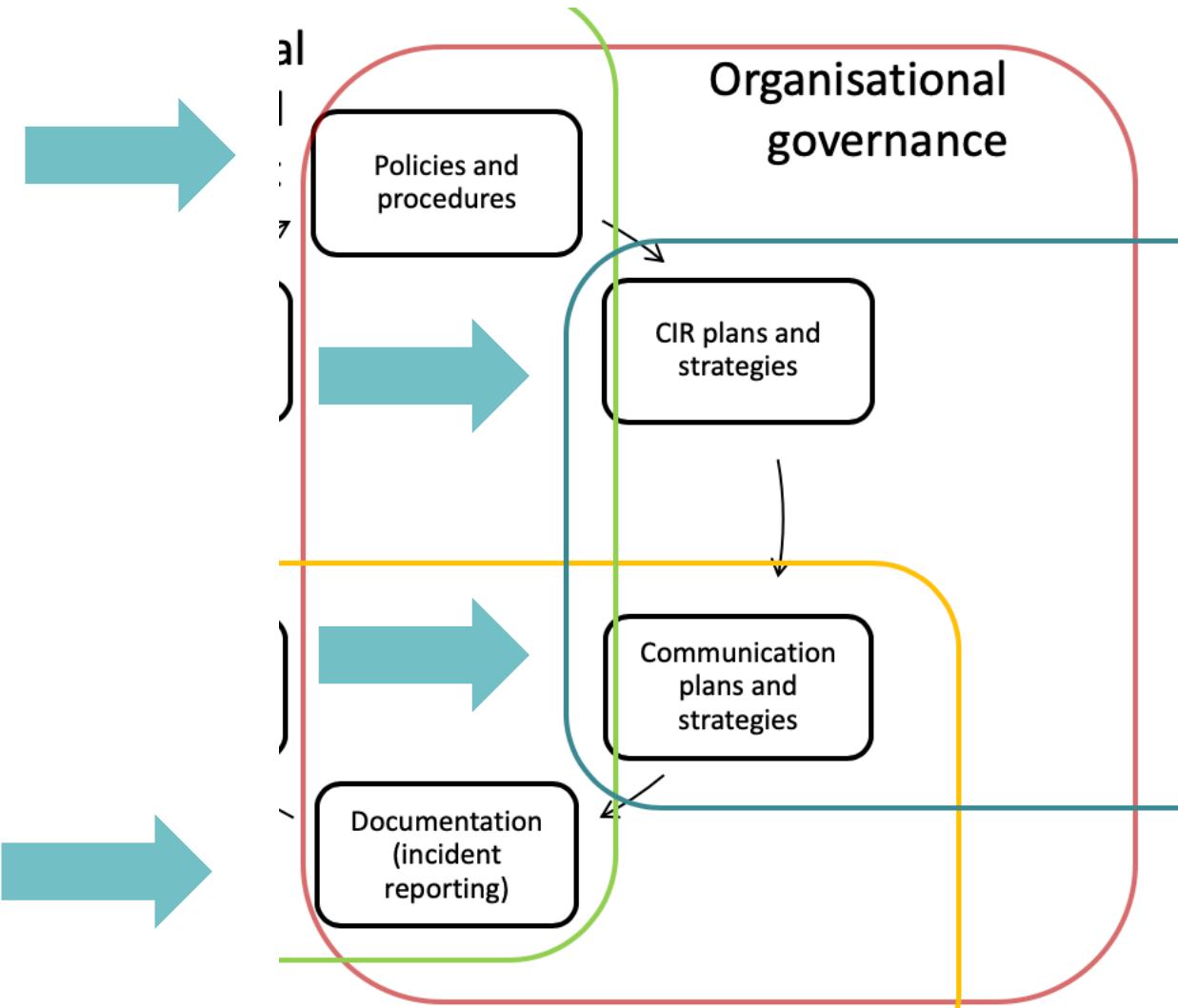
All Staff:

- 1.1. Must access, use, store and disseminate information based on its classification (See Monash Electronic Information Security- Minimum Security Controls Procedure)
- 1.2. Must lock all devices when not in use.
- 1.3. Must remain at the printer while Critical or Protected documents are printed.
- 1.4. Must not email Critical, Protected or Restricted information to personal email addresses.
- 1.5. Must only use authorized file sharing services (Google Drive, CloudStor).
- 1.6. Must prevent unauthorised access to Critical and Protected information when stored outside of Monash University's networks or systems.
- 1.7. Must use an approved encryption method when protecting all information.
- 1.8. Must securely destroy information when it is no longer required for organizational, legal or regulatory use.
- 1.9. Must use acceptable information destruction methods (incinerating, shredding, physical destruction, disk wipes etc...)
- 1.10. Must ensure contracts are in place prior to providing Critical, Protected or Restricted information to any third parties.

(Monash University, 2017b)

(Monash University, 2019c)

Organisational governance and IT security



10. Information Security Incident Management

Operational Responsibilities:

Responsibility	Scope
IT Security and Risk Manager	Security related aspects of incident management
Service Management Office Manager	IT incident management

Objective: To ensure a consistent and effective approach to the management of information security incidents, including communication on security events, threats and vulnerabilities, as part of an overall incident management process. #ISO27002.2013:16.1

10.1 Information Security Incident Management

10.1.1 Responsibilities and Procedures

C110 Incident management responsibilities and procedures shall be developed, maintained and implemented, and include effective, risk-based response to information security incidents, in consideration of the University's electronic information security classification. #ISO27002.2013:16.1.1, #LSA:14.6

10.1.2 Reporting Events and Weaknesses

C111 Any suspected or actual information security event, weakness, and technology risk related event shall be reported through approved procedures as quickly as possible. #ISO27002.2013:16.1.2, #ISO27002.2013:16.1.3, #LSA:3.7, #LSA:14.6

10.1.3 Assessment and Response

C112 Information security events, weaknesses, and ICT risk related events shall be risk assessed. Information security incidents shall be classified based on approved, risk-based criteria and the incident management priority matrix. #ISO27002.2013:16.1.4, #LSA:14.6

C133 Information security incidents shall be responded to in accordance with the approved incident response procedures. #ISO27002.2013:16.1.5, #LSA:14.6

10.1.4 Learning From Incidents

C114 Incident management procedures shall include the use of a post-incident review process, and the knowledge gained from analysing and resolving information security incidents shall be used to reduce the likelihood or impact of future incidents. #ISO27002.2013:16.16

10.1.5 Collection of Evidence

C115 Evidence shall be identified, collected, acquired, and preserved according to established, documented, and maintained procedures, in consideration of The University's electronic information security classification. #ISO27002.2013:16.17



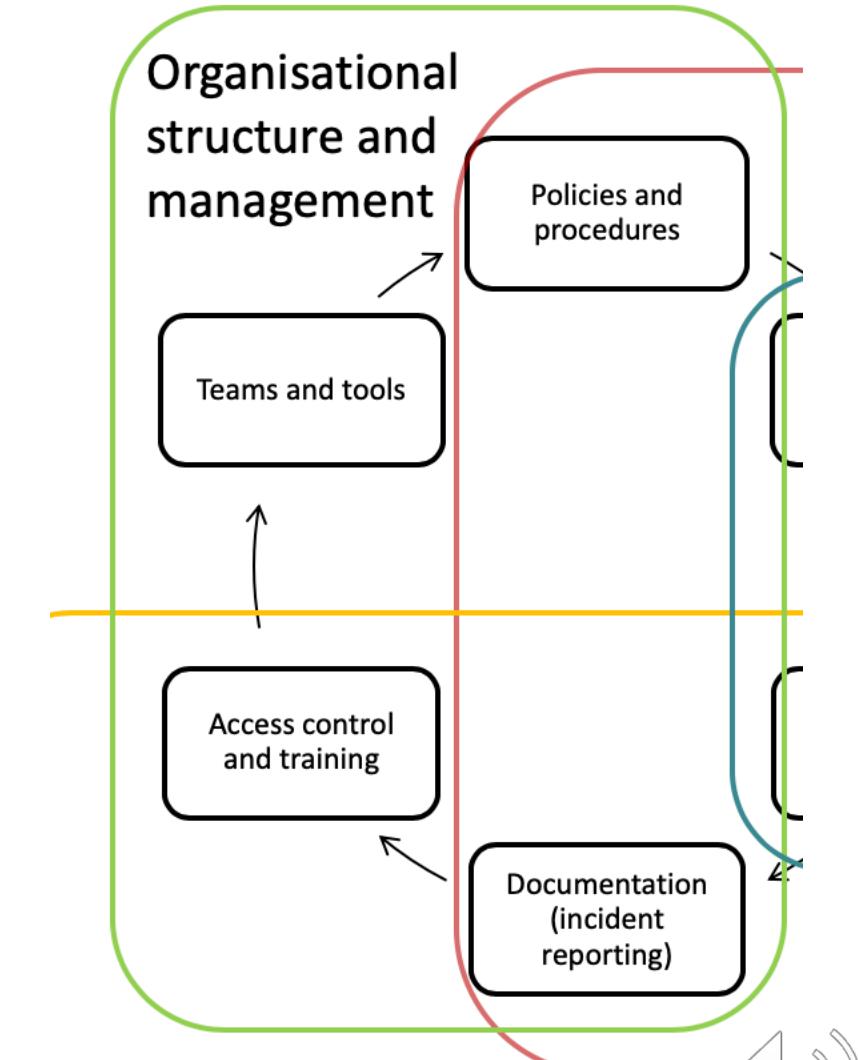
Management structure and IT security

How is IT security positioned in the organisation?

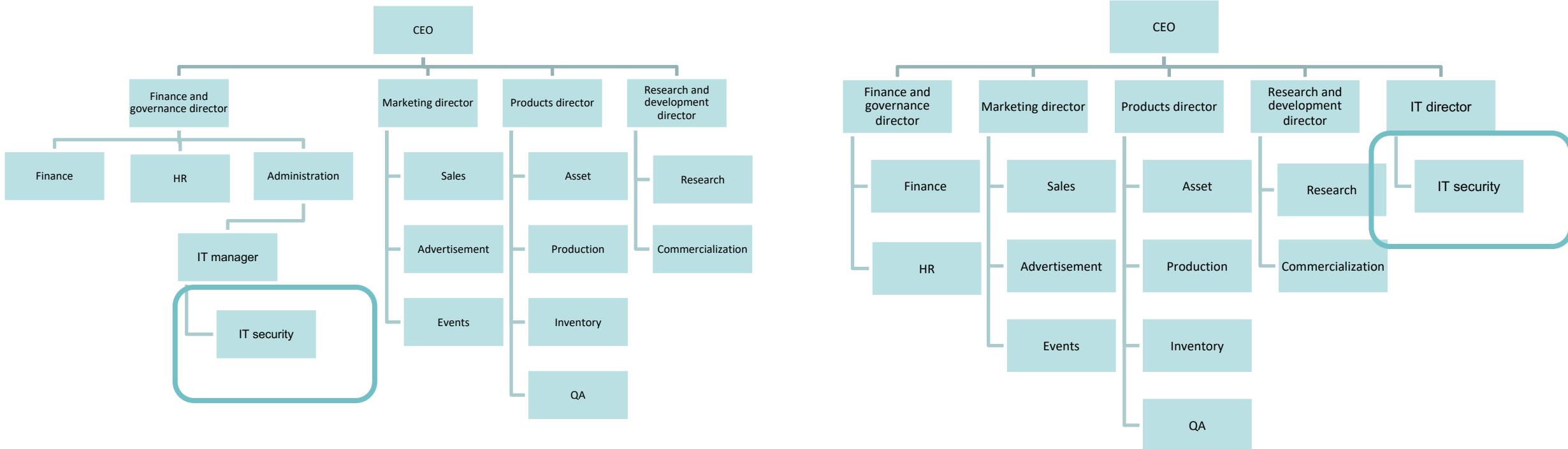
Do they have sufficient authority?

Is IT (security) resourced adequately?

Is the governance functioning?



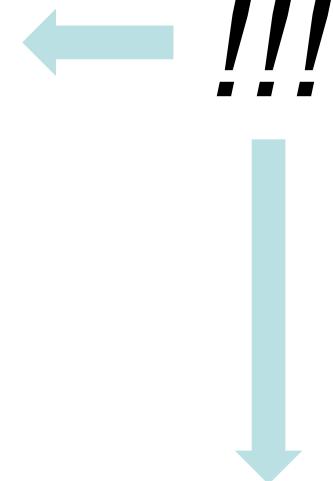
Spot the difference?



Jump Bag Recommendations:

- Incident Handlers Journal to be used for documenting the who, what, where, why, and how during an incident.
- Contact list of all CIRT members.
- USB Drives.
- A bootable USB drive or Live CD with up-to-date anti-malware and other software tools that can read and/or write to file systems of the computing environment that the incident response is to be performed in. One example is that of the Bart's PE disk for Windows XP (or later) environments.
- A laptop with forensic software (e.g. FTK or EnCase), anti-malware utilities, and internet access (if necessary for researching solutions or downloading tools).
- Computer and network tool kits to add/remove components, wire network cables, etc.
- Hard duplicators with write-block capabilities to create forensically sound copies of hard drive images.
- A bag that properly store all of the aforementioned tools in an organized and protective fashion.

[\(Kral, 2012\)](#)

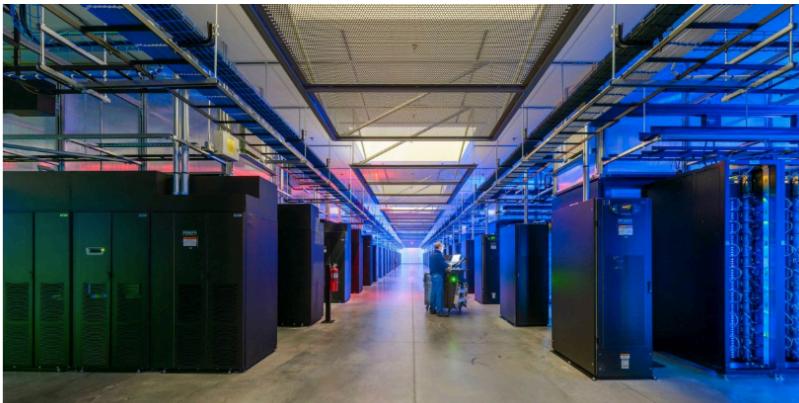


Peek inside Facebook's massive data centres that store all your photos, 'likes,' and chats

JILLIAN D'ONFRO

SEP 19, 2015, 6:45 AM

[FACEBOOK](#) [TWITTER](#) [REDDIT](#) [LINKEDIN](#) [EMAIL](#)



Alan Brandt

If you open Facebook on your phone for 30 seconds, you're activity likely touches over 1,000 servers.

Much of that "magic" happens in the social network's own massive data centres.

Since 2011, Facebook has built four centres in Oregon, Iowa, North Carolina, and Sweden with innovative, environmentally-conscious designs [that it has made available to the public through its Open Compute Project](#).

(D'onfro, 2015)

How Microsoft's secret-level DC bolsters open source

Microsoft Azure's new Canberra region is about much more than public sector workloads with secret-level protection: it also adds strength to Australia's open source hosting capability.

[Red Hat and Microsoft](#)

21 September, 2018 09:00

[FACEBOOK](#) [LINKEDIN](#) [TWITTER](#) [EMAIL](#)

Microsoft recently cut the ribbon on its two new Azure data centres in the Canberra suburbs of Fyshwick and Hume, bringing its global region count to 54.

The operation, opened in April, has the strongest physical security anywhere in Australia – so hardened, in fact, that it can house government 'secret' level information within the walls.

That is the physical walls and biometrics side of it; on the services side, the Australian Signals Directorate put Microsoft through the wringer and assessed 35 Azure services across the Australian region as fit to be qualified to meet the coveted "PROTECTED" classification.

Extreme resilience, even within Australia

Microsoft and Red Hat are proud of the two Canberra data centres' extreme resilience characteristic. They are designed to meet the Australian Government's needs and work alongside the Sydney and Melbourne data centres.

"However, what's really unique about Azure, which our competitors can't match," Carter says, "is that we're not dependent on Sydney."

"For customers that have extraordinarily sensitive workloads that they want to move to the cloud and have the ability to deploy it in a high availability, disaster tolerant way, they can deploy it into Canberra DC1 and 2 (Australia Central Region 1 and 2) and then replicate it to Sydney and Melbourne. They then have four geographically dispersed regions that their application can be run from. There are 35 Azure services they can consume within the overall Australian region which are certified for Protected Status."

"With our competitors, if you had a natural or man-made disaster in Sydney, it would be difficult for them to replicate their clients' data out. With the ability to serve customers from geographically dispersed regions within the same country."

(ComputerWorld, 2018)

Data centre power use greater than Woolworths, Coles combined

By Cole Latimer

23 September 2018 – 4:07pm

f t e A A A

21 View all comments

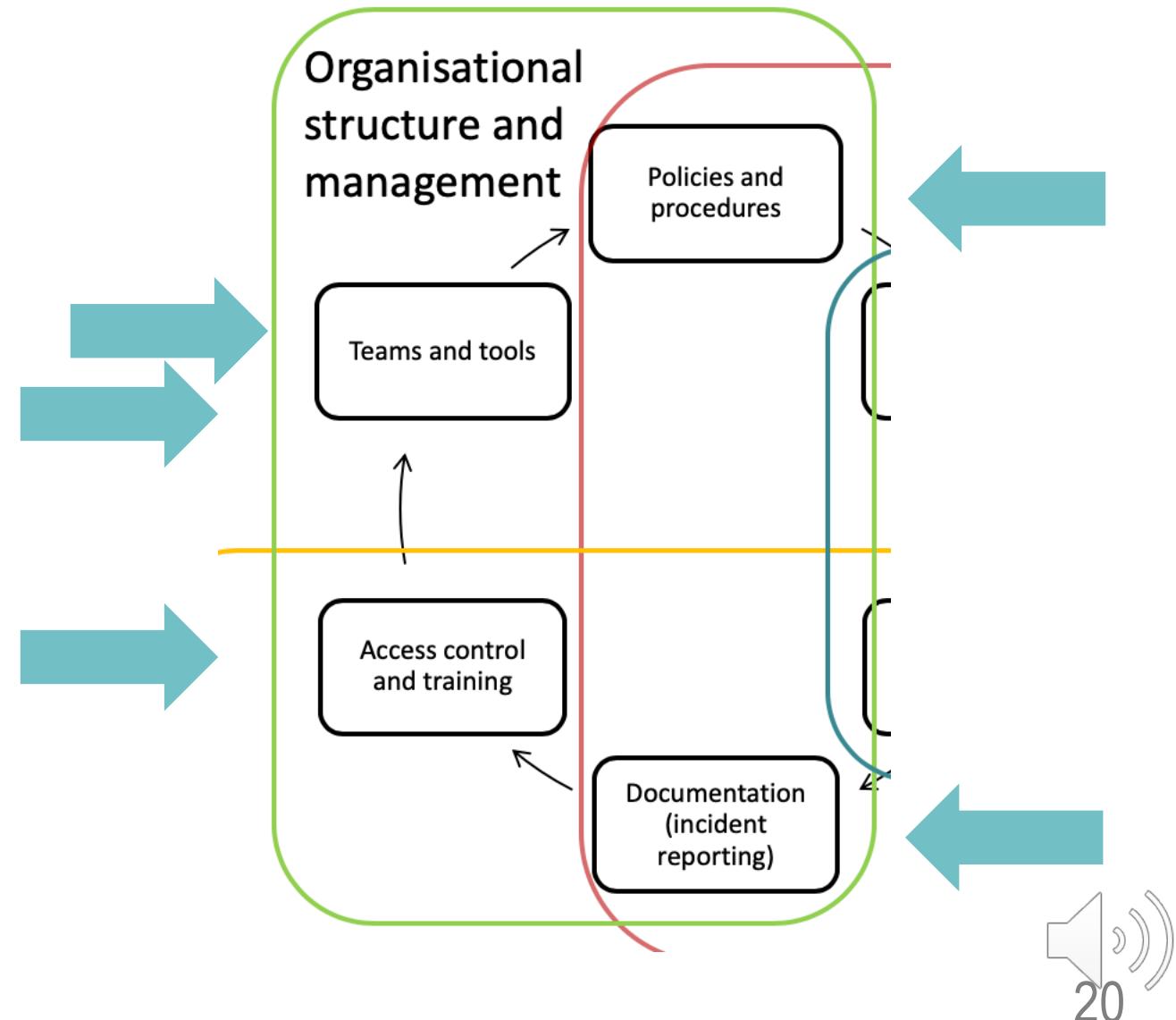
Australia's obsessions with social media and search engines, alongside a cloud computing drive from corporations, is powering the growth in energy intensive data centres, which now use as much energy as regional cities.

Deon Newman, vice-president of strategy for IBM Asia Pacific, explained that the world is creating more information every day than humanity did over the course of a century.



(Latimer, 2018)

Management structure and IT security



Information management and IT security

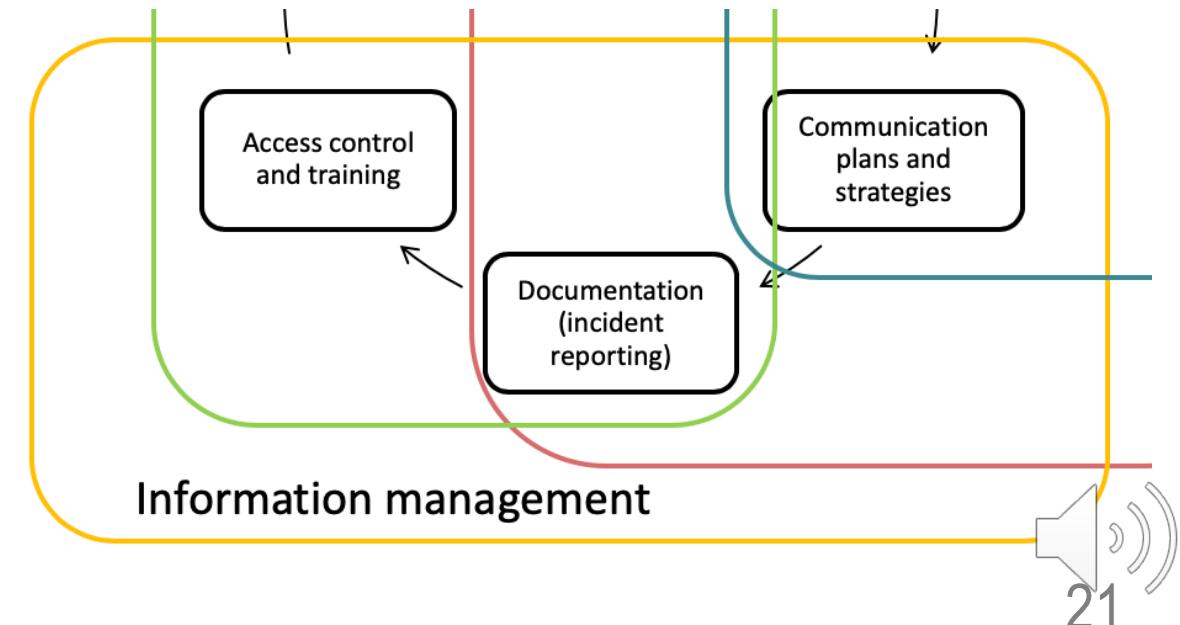
Are staff aware of IT security risks and threats?

Do they report the incidents?

Do they know what to do when they noticed any threats?

Do they know only what they should know?

Can they keep secrets?



Recognising the risks 1

You are engaged as a programmer in a project that is highly confidential within your organisation. Which one of the following is NOT an effective strategy to maintain the secrecy of this project?

1. Implement a set of strict protocols that define who could access which information.
2. Have the anti-eavesdropping physical facilities specifically for the project in a secret location.
3. Give a codename for the project so that others won't know what you are talking about.

Users Really Do Plug in USB Drives They Find

Matthew Tischer[†] Zakir Durumeric^{††} Sam Foster[†] Sunny Duan[†]
Alec Mori[†] Elie Burszttein[○] Michael Bailey[†]

[†] University of Illinois, Urbana-Champaign [○] University of Michigan [○] Google, Inc.
(tischer1, sfoster3, syduan2, ajmori2, mdbailey)@illinois.edu
zakir@umich.edu elieb@google.com



eSolutions

Type your search term



Home > Accounts and passwords

Multi-factor authentication (MFA)

Multi-factor authentication (MFA) provides you with increased protection, keeping your personal information private and secure. It requires using another factor to verify your identity, as well as your password, when logging in.



Why is MFA important

MFA makes it difficult for an attacker who has your password from being able to access your account or breach University systems. Even if you don't think you have sensitive information in your account, some University systems maintain information about you that may include:

- address and contact details
- banking details
- medical information
- emergency contact information
- academic results.

(Monash University, 2019d)

Abstract— We investigate the anecdotal belief that end users will pick up and plug in USB flash drives they find by completing a controlled experiment in which we drop 297 flash drives on a large university campus. We find that the attack is effective with an estimated success rate of 45–98% and expeditious with the first drive connected in less than six minutes. We analyze the types of drives users connected and survey those users to understand their motivation and security profile. We find that a drive's appearance does not increase attack success. Instead, users connect the drive with the altruistic intention of finding the owner. These individuals are not technically incompetent, but are rather typical community members who appear to take more recreational risks than their peers. We conclude with lessons learned and discussion on how social engineering attacks—while less technical—continue to be an effective attack vector that our community has yet to successfully address.

I. INTRODUCTION

The security community has long held the belief that users can be socially engineered into picking up and plugging in seemingly lost USB flash drives they find. Unfortunately, whether driven by altruistic motives or human curiosity, the user unknowingly opens their organization to an internal attack when they connect the drive—a physical Trojan horse. Our community is filled with anecdotes of these attacks and pentesters have even boasted that they can *hack humans* by crafting labels that will pique an individual's curiosity [1]: “While in the bathroom, I place an envelope in one stall. On the cover of the envelope I put a sticker that says PRIVATE. Inside the ‘private’ envelope is a USB key with a malicious payload on it. I do this in one stall and also in the hallway by a break room to increase my chances and hope that the person that finds one of them is curious enough to insert it into their computer. Sure enough, this method seems to always work.”

However, despite numerous anecdotes of malicious peripheral efficacy, there has been little research on whether this attack is effective nor work, we investigate the effectiveness of this attack in a controlled experiment in which we drop 297 flash drives on a large university campus. We measure the efficacy of this attack by measuring the success rate of the attack, the time taken for the first drive to be connected, and the types of drives that are connected.

Abstract:

We investigate the anecdotal belief that end users will pick up and plug in USB flash drives they find by completing a controlled experiment in which we drop 297 flash drives on a large university campus. We find that the attack is effective with an estimated success rate of 45–98% and expeditious with the first drive connected in less than six minutes. We analyze the types of drives users connected and survey those users to understand their motivation and security profile. We find that a drive's appearance does not increase attack success. Instead, users connect the drive with the altruistic intention of finding the owner. These individuals are not technically incompetent, but are rather typical community members who appear to take more recreational risks than their peers. We conclude with lessons learned and discussion on how social engineering attacks—while less technical—continue to be an effective attack vector that our community has yet to successfully address.

(Tischer et al., 2016)



Recognising the risks 1

You are engaged as a programmer in a project that is highly confidential within your organisation. Which one of the following is NOT an effective strategy to maintain the secrecy of this project?

1. Implement a set of strict protocols that define who could access which information.
2. Have the anti-eavesdropping physical facilities specifically for the project in a secret location.
3. Give a codename for the project so that others won't know what you are talking about.

Recognising the risks 1

You are engaged as a programmer in a project that is highly confidential within your organisation. Which one of the following is NOT an effective strategy to maintain the secrecy of this project?

1. Implement a set of strict protocols that define who could access which information.
2. Have the anti-eavesdropping physical facilities specifically for the project in a secret location.
3. **Give a codename for the project so that others won't know what you are talking about.**

Recognising the risks 2

Bianca is a security analyst in an IT consulting firm, and over last two weeks she went through hundreds of emails employees of the client's company sent using the company's email system. This work was conducted in order to identify inappropriate use of the company's emails, and she naturally had to read some emails that included the employees' personal information and/or some personal photos of the employees, some of which were rather compromising for these individual employees. Bianca found some of the things people write in their emails rather funny, and posted on her personal blog called 'The secret life of an IT security analyst' an article about these 'embarrassing' emails however de-identified. What kind of risks can you see?

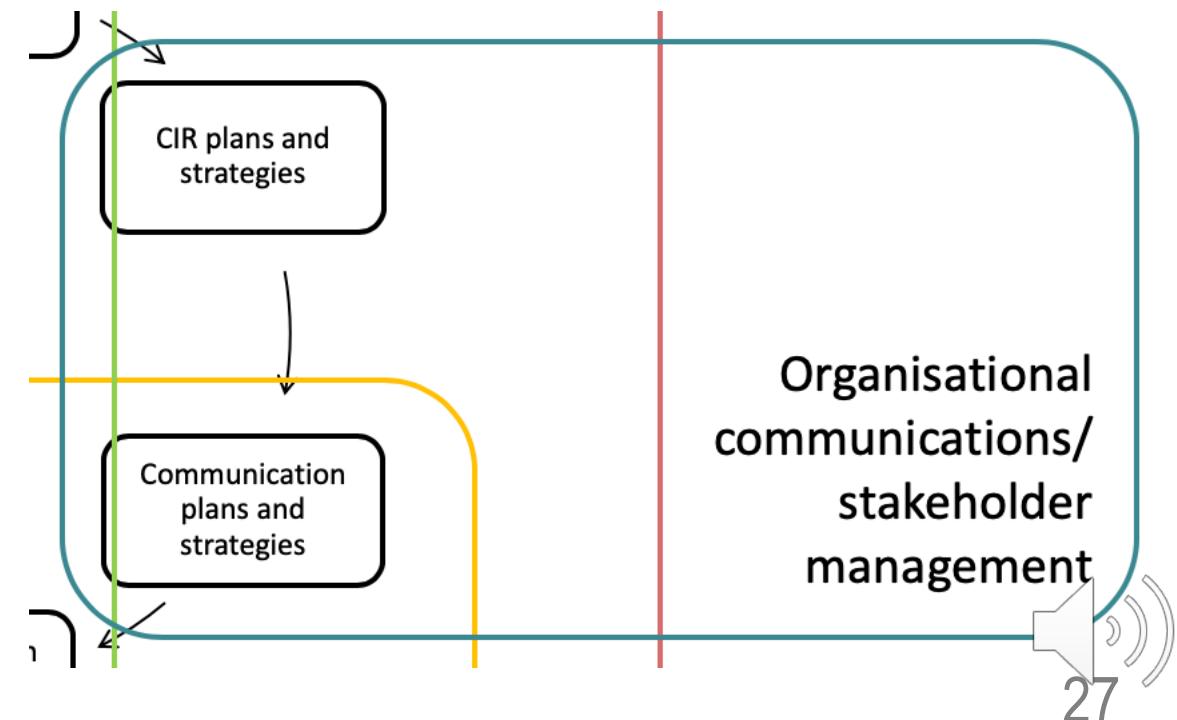
Organisational communications and IT security

What do we tell?

How and when do we tell?

How do we know that they heard?

How do we know that they actioned?





We protect you online with industry-leading security.

Everything that we make is protected with powerful built-in security technologies that help detect and block threats such as spam, malware and viruses from ever reaching you. And we share these security technologies with partners and competitors alike, raising industry standards that help keep everyone safer online.



BUILT-IN PROTECTION

Building protection into everything that we make

Google services are continuously protected by one of the world's most advanced security infrastructures. This built-in security detects and prevents online threats, so you can be confident that your personal information is secure.

[Learn more](#)

SECURITY LEADERSHIP

Collaborating to strengthen security across the Internet

Google has a long history of openly sharing our security learning, experiences and technologies with partners, competitors and organisations around the world. And as security threats evolve, this continuous industry-wide collaboration is critical to protecting users and helping to create a more secure Internet together.

[Learn more](#)

SECURITY TIPS

Tips to help you stay more secure online

We've put together some quick tips and best practices for you to create stronger passwords, protect your devices, avoid phishing attempts and browse the Internet securely.

[Learn more](#)

(Google, 2019a)

The screenshot shows a section of the Google Help Center titled 'Suspicious sign in prevented' email. It explains that receiving such an email means Google has blocked an attempt to access the user's account from a different location or device. It provides instructions for checking account activity and changing the password if needed. Below this, there's a 'Report a suspicious message' section and a 'Related Articles' section with links to 'unusual sign-ins' and 'Recent Activity reports'. At the bottom, there's a poll asking if the article was helpful, with 'Yes' and 'No' buttons.

(Google, 2019b)



Making it easy to understand what data we collect and why

When you use Google services, you trust us with your data. It's our responsibility to be transparent about the data that we collect and how we use it in making our services work better for you.

Being transparent about the data that we use

Information that we collect as you use our services

When you use our services – for example, do a search on Google, get directions on Maps or watch a video on YouTube – we collect data to make these services work better for you. This can include:

- Things that you search for
- Videos that you watch
- Ads that you view or click
- Your location
- Websites that you visit
- Apps, browsers and devices that you use to access Google services

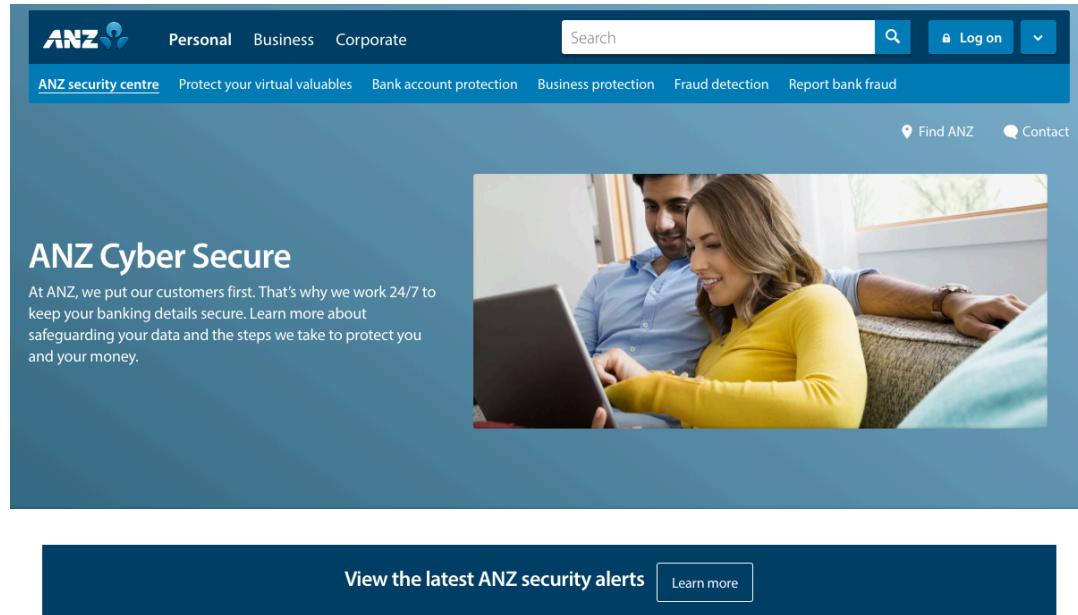
Information that you create or provide to us

When you sign up for a Google account, you provide us with personal information. If you are signed in, we collect and protect information that you create when using our services. This can include:

- Your name, birthday and gender
- Your password and phone number
- Emails that you write and receive on Gmail
- Photos and videos that you save
- Docs, Sheets and Slides that you create on Drive
- Comments that you make on YouTube
- Contacts that you add
- Calendar events

(Google, 2019c)





The screenshot shows the ANZ Cyber Secure homepage. At the top, there's a navigation bar with the ANZ logo, Personal, Business, Corporate, a search bar, Log on, and a dropdown menu. Below the navigation is a secondary header with links for ANZ security centre, Protect your virtual valuables, Bank account protection, Business protection, Fraud detection, and Report bank fraud. A 'Find ANZ' button and a 'Contact' link are also present. The main content area features a large blue banner with the heading 'ANZ Cyber Secure'. Below the banner, a text block says: 'At ANZ, we put our customers first. That's why we work 24/7 to keep your banking details secure. Learn more about safeguarding your data and the steps we take to protect you and your money.' To the right of the text is a photo of a man and a woman looking at a laptop together. At the bottom of the page is a dark blue footer bar with the text 'View the latest ANZ security alerts' and a 'Learn more' button.

Four steps to protect your virtual valuables



Pause before sharing your personal information

Ask yourself, do I really need to give my information to this site or this person?



Activate two layers of security

Use two-factor authentication for an extra layer of security to keep your personal information safe.



Call out suspicious messages

Be aware of current scams. If an email, call or SMS seems unusual, check it through official contact points or report it.



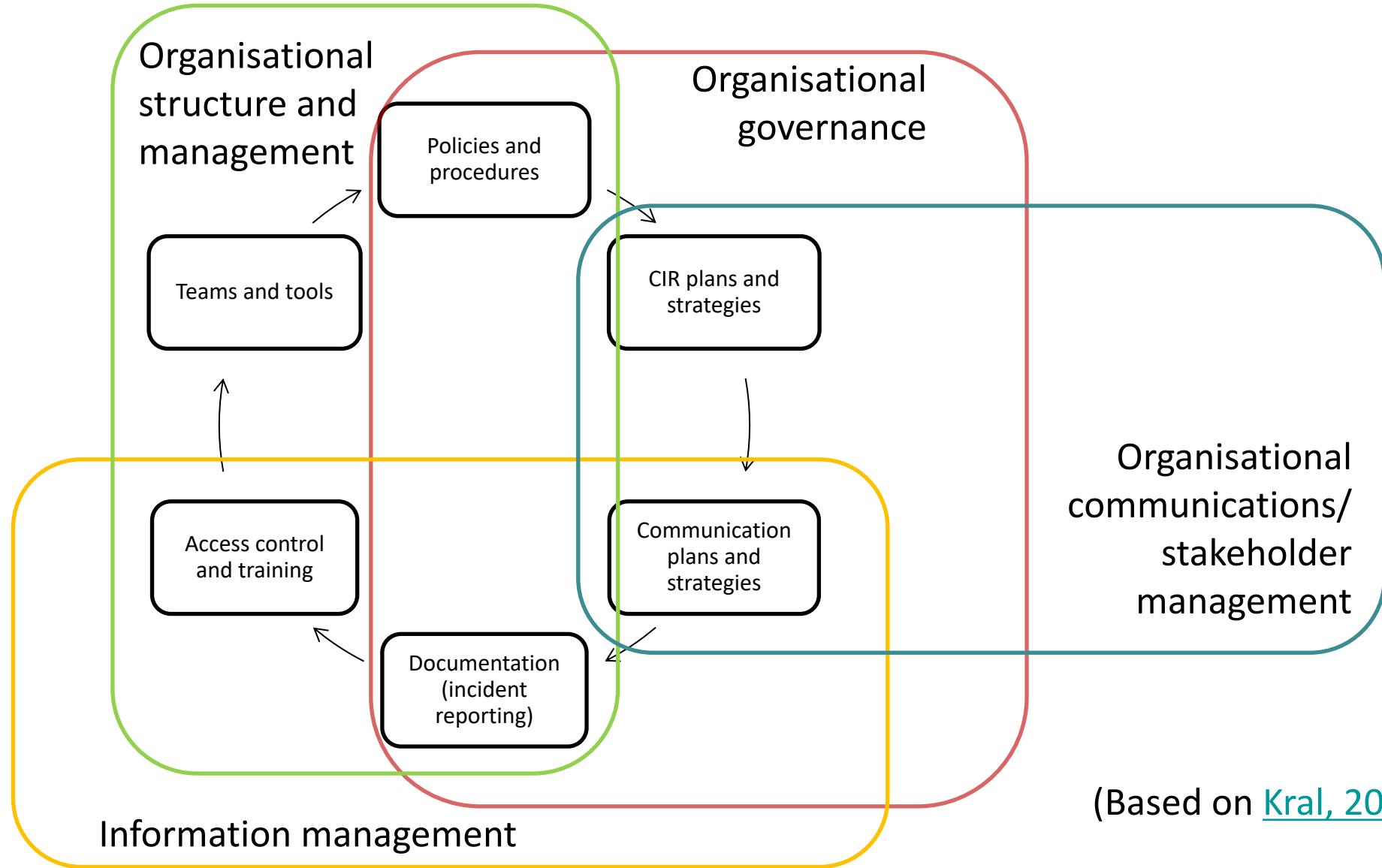
Turn on automatic software updates

Set your software, operating system and apps to auto update to make sure you get the latest security features.

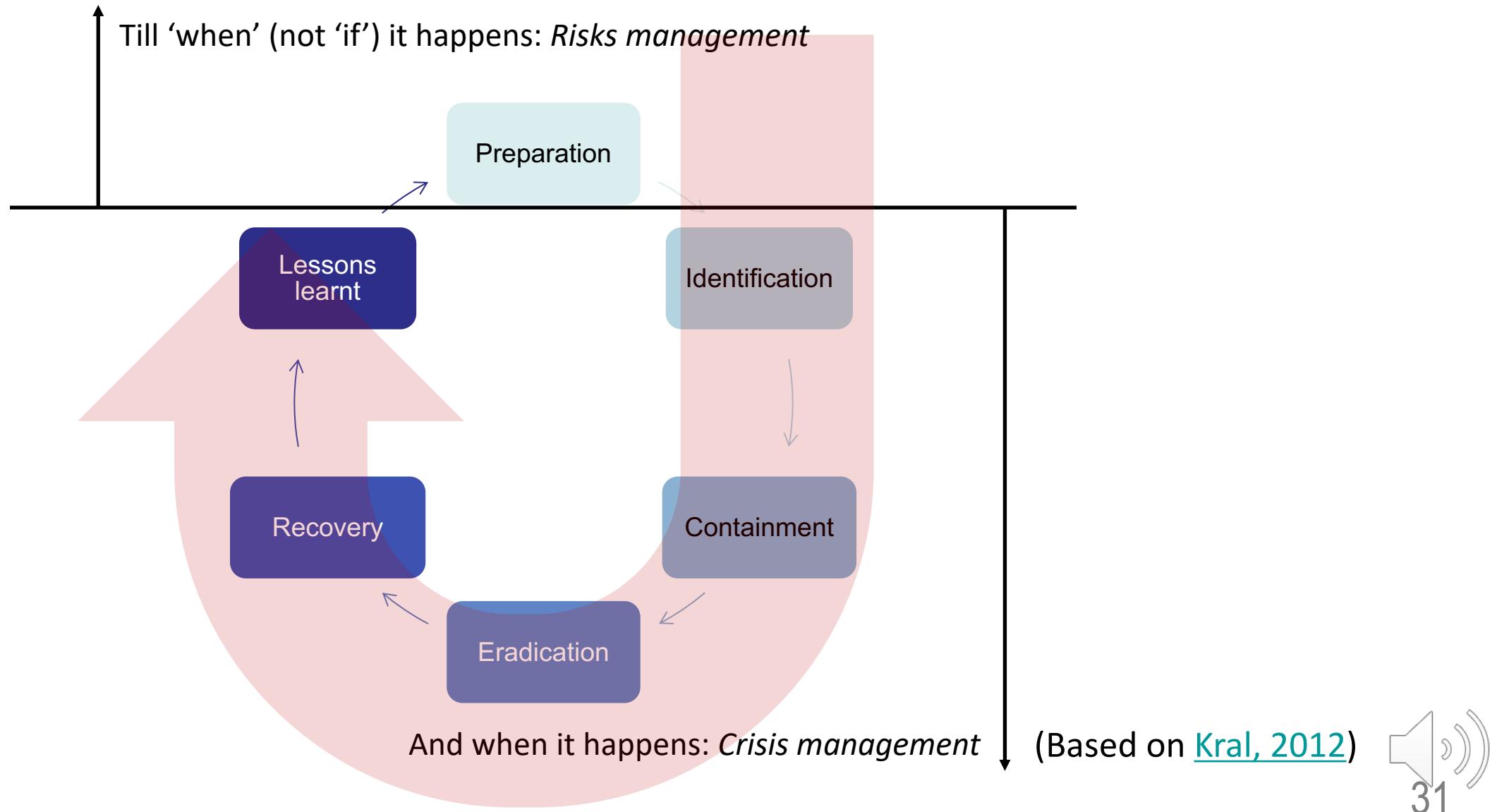
(ANZ, 2019)



(ANZ, 2015; on YouTube)



Crisis management: An organisational view



Identification

So, let's say that you are working as a security analyst for a private company that conducts a range of confidential and sensitive research projects outsourced by high-profile clients, such as government agencies and political parties. Your company is indeed reputed for the integrity that is well trusted by those high-profile clientele, and quite naturally your company stores a large amount of sensitive data as well as confidential clients information.

It's Monday in the morning, and as you arrive in your office, you noticed an unusual number of emails from the company's staff outside IT, reporting strange behaviors of the company's client management system. You and another colleague of yours in the IT security quickly check the system log, and you found a sign of suspicious traffic from unspecified hosts. You and your colleague then decided, as per the company's CIR plan, that you will coordinate communications and liaison, while your colleague will pursue more technical solution to the issue. What's your next step?

Containment 1

Back in the IT security team, your manager has now declared that this is a critical incident, and set up a ‘war room’ to control the CIR operations. Your team gradually gathered further intelligence from other sources, and based on all the evidence, it is becoming clear that there is an unknown extent of data breach where some part of the confidential client information stored in the company’s server has been compromised.

Your manager instructs the team to further contain the situation, while she asked you to keep acting as a liaison between the IT security team and the rest of the organisation. Meanwhile the IT security team’s role account has been flooded by emails from the company’s staff reporting all sorts of strange system behaviors... So what’s your next step?

Major Incident

Dear Colleagues,

Update: Email is in a degraded state.

Incident: [REDACTED]

Start: [REDACTED]

ETA: TBC

We are currently experiencing a Major Incident with the [REDACTED] mail service and large server file attachments.

A manual work around is in place for [REDACTED] reports that have not been received. [REDACTED] have been communicated with the work around. There have only been 5 reports reported as failed.

Large email printer scans will be affected.

Gmail web users are unaffected.

Representatives from eSolutions and Vendor Google are trying to identify what has gone wrong.

Representatives from [REDACTED] have been engaged.

Next update due: 17:00

For further information please contact the Service Desk on ext:51777

Kind Regards,

Service Desk

This email and any files attached to it are confidential and intended solely for the use of the individual or entity to whom they are addressed. Please do not distribute this communication outside of Monash University.



MONASH University





Notifiable Data Breaches scheme

Overview

The NDB scheme applies from 22 February 2018 to all agencies and organisations with existing personal information security obligations under the Privacy Act. It was established by the passage of the *Privacy Amendment (Notifiable Data Breaches) Act 2017*.

The scheme includes an obligation to notify individuals whose personal information is involved in a data breach that is likely to result in serious harm. The notification must include recommendations about the steps individuals should take in response to the breach. The Australian Information Commissioner (Commissioner) must also be notified of eligible data breaches.

Agencies and organisations must be prepared to conduct a quick assessment of a suspected data breach to determine whether it is likely to result in serious harm, and as a result require notification.

Notifications to the Commissioner should be lodged through the [Notifiable Data Breach form](#).

([OAIC, 2019d](#))

Containment 2

So you now sent out an internal communique to inform the company's staff of the situation, and you have also made sure that the company has engaged with the relevant authorities. You then noticed that your phone started to ring. Apparently some of the company's staff posted something about the incident without knowing its seriousness, and the local media had picked it up as a potential story. It is a well-known fact that your company has an impressive list of powerful clients, so you can see why they'd be interested.

And of course, your company's clients now started contact your company using a range of channels to clarify what's going on. Now what would you do?

Eradication

It's Day 2, and just when all the communications have gone out to stakeholders, you got your team's latest update that they have now identified and isolated the affected part of the system. They are not yet sure how long it would take to actually restore the system fully, but they seem to be optimistic, while also making the unaffected part of the system available so that the company can still operate however in a limited capacity. *Oh, by the way, they also told you that the data has been compromised at least for last two years, the extent of which is rather hard to know...*

How much of all this information can you share with your stakeholders?

Recovery

The team has now set up a timeframe for recovery, and they are now confident that the system would be restored in the next four days or so, unless they find any other vulnerabilities in the process of recovery. The system is still not operating in its full capacity, but the company's operations seem to be coping 'okay'.

Meanwhile there are still lots of social media posts, emails and phone calls coming in to your company. You were also told by some sources that some powerful clients are demanding detailed public explanations on how the company is responding to the issue, while others are making speculative comments on the incident, fueling the anxiety of others. What's your next step?

Lessons learnt...

So four days past, the chaos of dealing with all sorts of stakeholder engagement finally started to settle. The management, the CIR team as well as a third-party security consultant all agreed that the system could be restored however with a period of strict monitoring. The ‘war room’ has been dissolved, and things are starting to return to normal.

So what else do you have to do now?

Crisis management: An organisational view

