



new era.
TECHNOLOGY



Covenant
Christian School
All knowledge through Christ

Cyber Security *for School Leaders*

Presented by:
Paul Carnemolla & Solomon James

August 2024



Today's resources
and further information



Overview

- The Cyber Security Threat.
- Importance of Cyber Security in Education.
- The Covenant Story.
- Planning and Preparing for a Cyber Attack.
- Preparing a Cyber Security Incident Response Plan.
- Reporting to the Board.

The Cyber Security Threat *in educational institutions*



Cyber threats in Education

1. 29% of attacks on educational institutions originated from vulnerability exploitation and 30% from phishing campaigns on K-12 schools in 2023 ([Infosecurity Magazine](#)).
2. Ransomware attacks on K-12 and higher education globally caused over \$53 billion in downtime costs from 2018 to mid-September 2023 ([Comparitech](#)).
3. These attacks breached over 6.7 million personal records across 561 incidents ([Comparitech](#)).

Education sector graphic

From Check Point (Cyber Security Solution) research

Global Avg. Weekly Cyber Attacks per Industry
(2024 Q1 Compared to 2023 Q1)

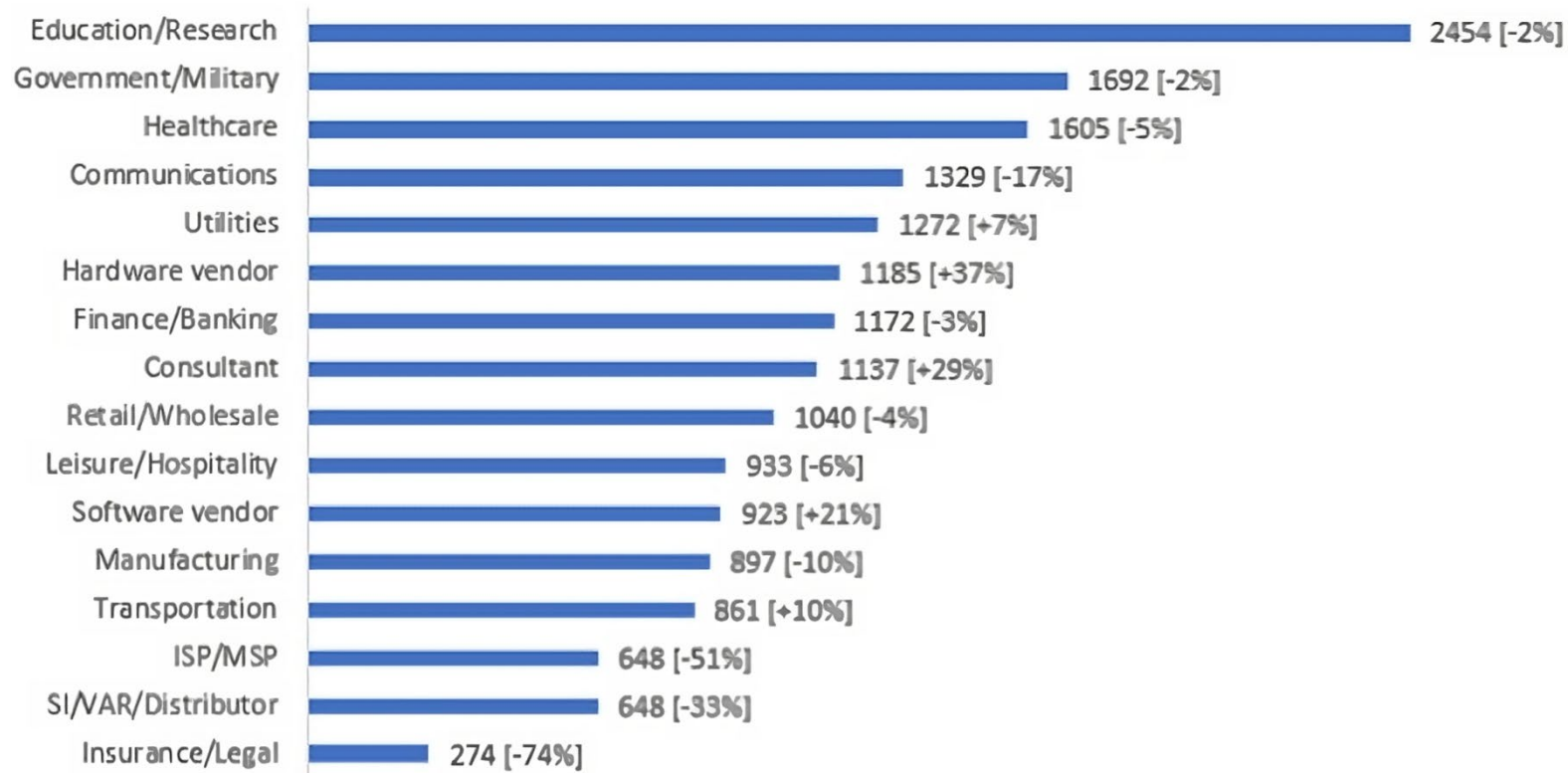


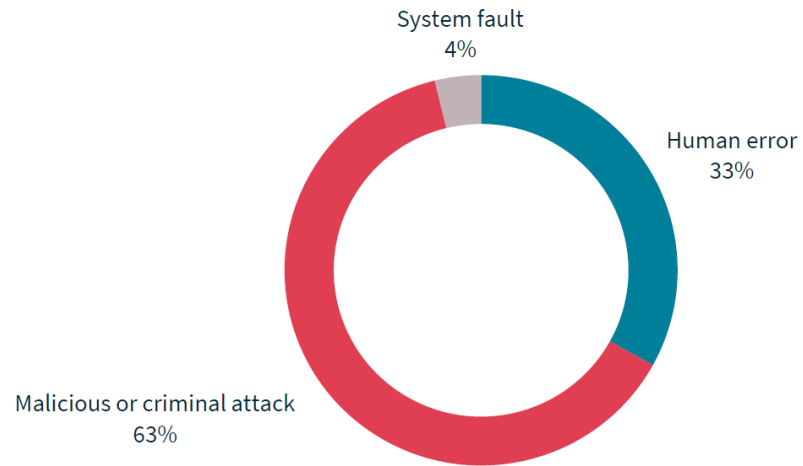
Image source: Check Point Software Technologies

Importance of Cyber Security in educational institutions

- 1 Protect Sensitive Data
- 2 Preserving Academic Integrity
- 3 Safeguarding Intellectual Property
- 4 Maintaining Operational Continuity
- 5 Protecting Financial Resources
- 6 Fostering Trust and Reputation
- 7 Promoting Digital Citizenship & Online Safety
- 8 Compliance with Regulations
- 9 Mitigating Cyber Threats and Attacks
- 10 Preparing Students for the Future

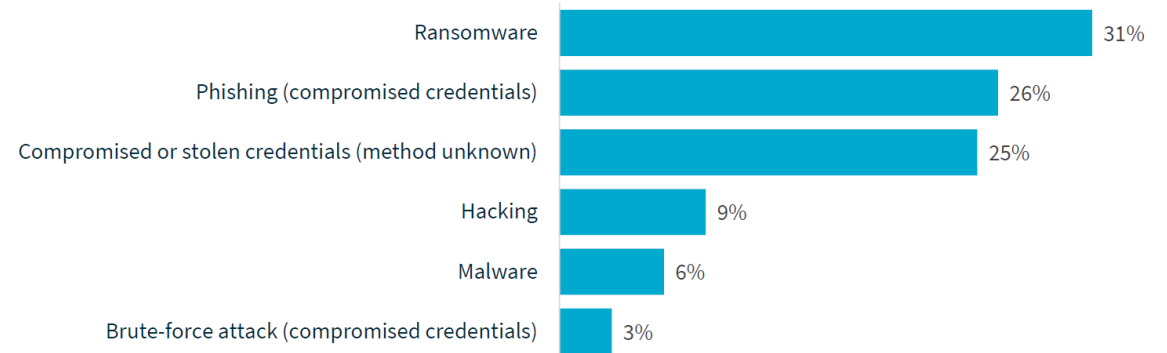
Sources of Data Breaches

Sources of data breaches



41% of all data breaches resulted from cyber security incidents
(162 notifications)

Cyber incident breakdown



Top causes of human error breaches



Personal information emailed to the wrong recipient 38%



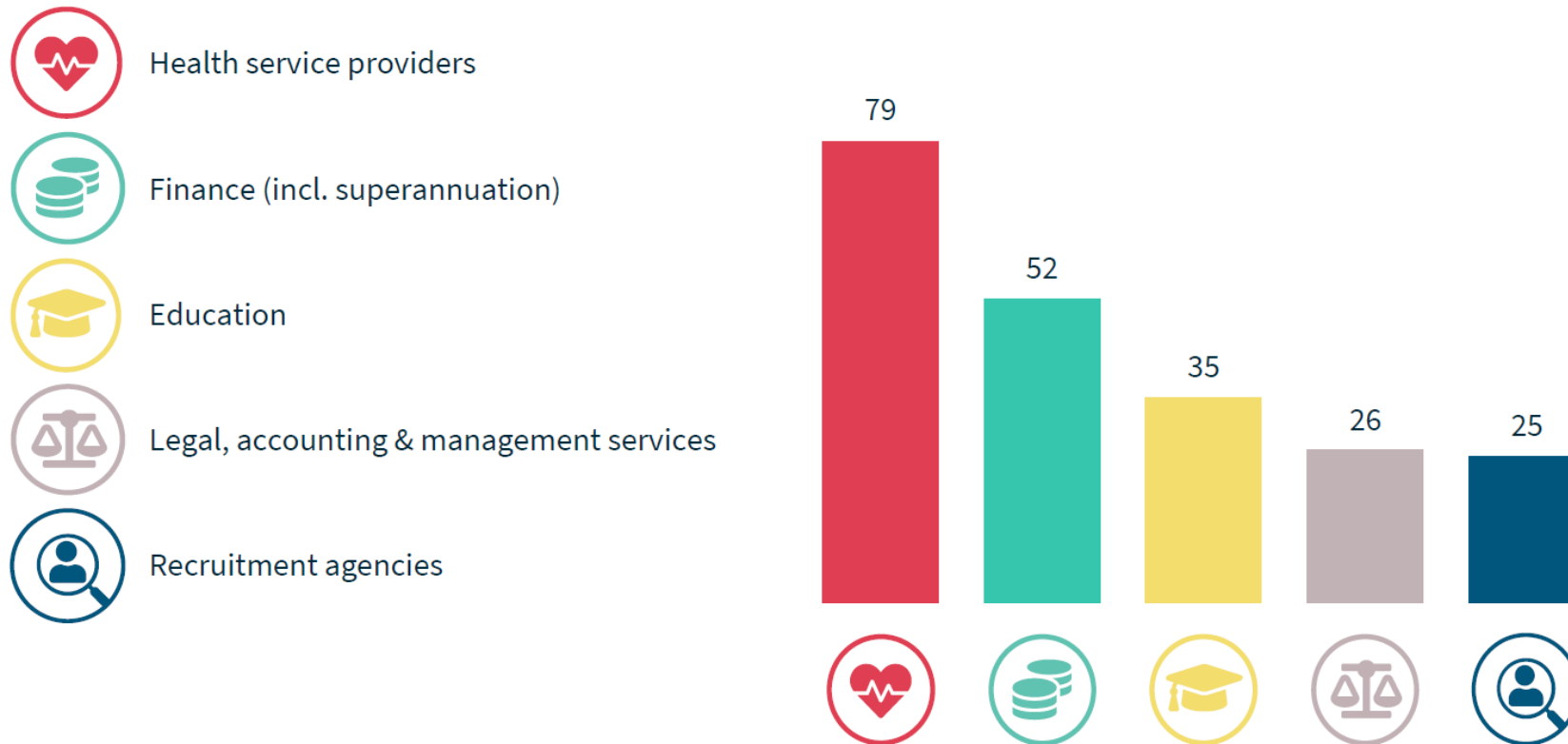
Unintended release or publication 24%



Personal information mailed to the wrong recipient 8%

Notifiable Data Breach snapshot

Top 5 sectors to notify data breaches



Cyber Security Breach
*Western Sydney
University - 2024*





Dear Solomon James,

I am writing to notify you of an incident of unauthorised access to our information technology (IT) network.

Today the University has issued a public notification about unauthorised access to the University's storage platform, known as the Isilon storage platform (Isilon). A copy of the public notification is available here: www.westernsydney.edu.au/cyberincident.

In particular, the University is drawing its public notification to the attention of our community, which includes but is not limited to, our former and current students and staff.

Project Timeline

The Covenant Story



Covenant ICT Team



	Role	Org	FTE
Paul Carnemolla	Director of ICT	New Era	0.5
Solomon James	ICT Manager	New Era	0.8
Justina Lowe	ICT Support	Covenant	0.8
Leon Dhemba	ICT Support	Covenant	1
Nicholas Sargent	ICT Support	Covenant	1
Nino Galeos	Senior Engineer	New Era	0.2
Chirag Shah	Senior Engineer	New Era	0.1
Anastasia Yew	Casual ICT Support	Covenant	n/a
Annie Wye	Casual AV Support	Covenant	n/a

REMEDIATION

INCEPTION

BASELINE

2021 • Term 3

Pre-ICT Leadership - New Era

On-premise services:

- Active Directory
- Attache (Finance)
- FileShare
- WebHelpdesk
- CounselPro

Cloudwork for MFA/SSO

Microsoft 365 A5 Suite

Hybrid Exchange in Cloud and Azure

2021 • Term 4

Penetration Test

- Internal
- External
- Wi-Fi

Disaster Recovery Planning

2021-2022 School Holidays

1st Internal Pen. Remediation

2021 • Term 3

Implementation of Intune / Endpoint Manager

Upgrade Endpoint Security

2022 • Term 4

Jamf Pro Security Audit + Jamf Connect Config

Windows 11 Configuration and AutoPilot Setup

2022-2023 School Holidays

2nd Pen. Remediation

2023 • Term 1

Secure-ISS SIEM Implementation

Security Uplift Project (x2)

2023 • Term 2

Security Awareness platform – Knowbe4

Microsoft 365 Security Audit

2023 • Term 2

Microsoft 365 Security Remediation

2023 • Term 3

Incident Response Plan – Project

2023 • Term 4

Definitiv Cloud payroll solution

Cyber Security framework

Cyber Security Risk Assessment

2024 • Term 1

Secondary Laptop Program

vCISO Project

Microsoft Unified Support and On Demand Assessments

Linewize Parent Access trial

Microsoft Security Uplift

Security features and enablers within the suite of Microsoft products in use:

- Microsoft Endpoint Manager
- Microsoft Security Score
- Defender for Endpoint Plan 2 and Office 365 Plan 2
- Conditional Access
- Data Loss Prevention
- Compliance Program for Microsoft Cloud

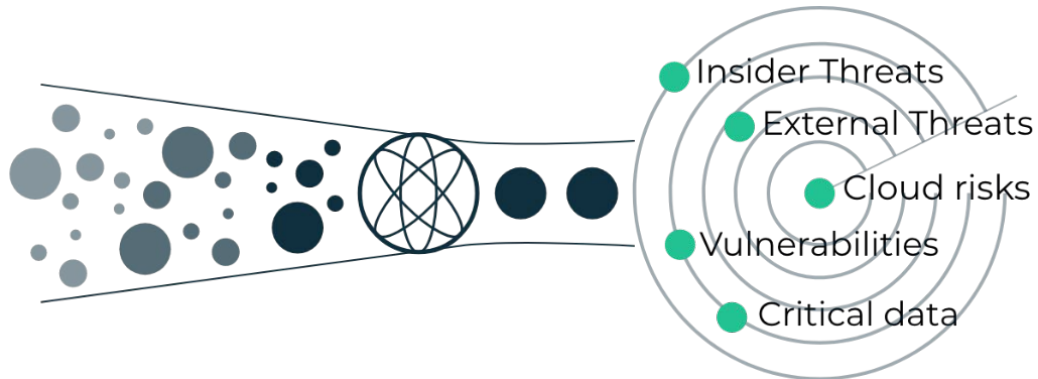
[Microsoft License Feature Comparison](#)

Security Information and Event Management

Secure-ISS - <https://secure-iss.com/>

- Correlates events from all available log sources in real-time ensure threat alerts are prioritised
- 24/7 SOC (Security Operation Centre) escalate and contain identified threats
- Minimal resources required from the IT team

ENDPOINT
NETWORK ACTIVITY
DATA ACTIVITY
USERS AND IDENTITIES
THREAT INTELLIGENCE
CONFIGURATION INFORMATION
VULNERABILITIES AND THREATS
APPLICATION ACTIVITY
CLOUD PLATFORMS



Security Event Monitoring	Secure ISS	School Resource
Deployment of virtual appliance(s) to collect and store security logs	✓	
Integration into IBM QRadar Management Console (SIEM)	✓	
Tuning	✓	✓
Monitoring & Detection (24x7)	✓	
Security Analyst - Reporting and Notification Period (8x5)	✓	
Threat Intelligence (IBM X-Force + collection/sharing of school threats)	✓	
Cloud Security Monitoring	✓	
Incident Management (Triage, Investigate, Analyse)	✓	
Security Operations Centre Touchpoints:	✓	
Live Updates of Security Incidents	✓	
Monthly Security Operation & Governance Reporting	✓	
Incident Response (Disrupt & Contain)	✓	✓
Incident Remediation	✓	✓

Security Event Monitoring is priced at **\$1 per month, per enrolled student** (based on the above scope of work / service)

Secondary Laptop Program

- Board endorsed decision to move to school managed Windows devices for secondary students
- Web filtering and content control
- Enhanced security controls
- Centralised monitoring and management
- Data protection and controlled software deployment
- Swift remediation of any vulnerability or software threats
- Conditional Access management

	4-year rollout					
	7	8	9	10	11	12
2024	x		x			
2025	x	x	x	x		
2026	x	x	x	x	x	
2027	x	x	x	x	x	x
2028	x	x	x	x	x	x
2029	x	x	x	x	x	x



Linewize

Notable Advantages

- School configured filtering rules are applied regardless of network connection (school Wi-Fi, hot-spotting or home Wi-Fi).
- Client can be installed securely and remotely and cannot be removed by students.
- Parent Integration: 24/7 network filtering, with parents able to add additional time/category-based restrictions outside of school hours via Qustodio.

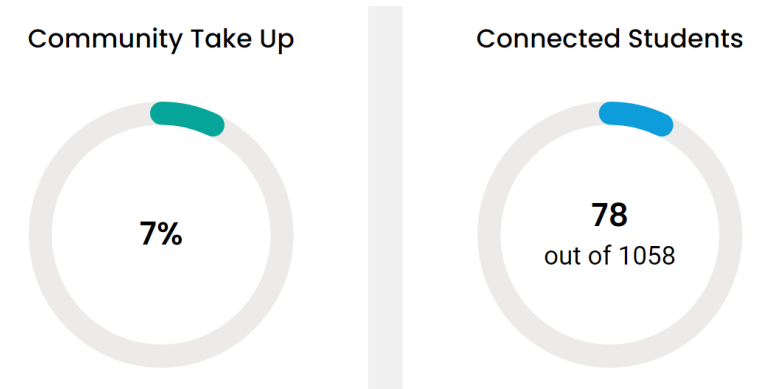


Diagram of active parent integrations

Linewize

Example of Daily Use

- **Issue:** Student Wellbeing received their usual weekly report. They requested clarification regarding a student's flagged traffic.
- **Solution:** A more detailed report on Linewize School Manager was provided, with all network activity from the student around the time of the flagged traffic.
- **Resolution:** With this context it was confirmed that the student had been using their device inappropriately. This clarified the situation for Student Wellbeing and enabled them to act on it.

Other Key Projects

- KnowBe4 Security Awareness Training and regular Phishing campaigns
- Data Classification
- Security Improvements:
 - Enhanced network segregation
 - 802.1x network authentication for wired network
- Security Questionnaire for Third-Party Vendors
- Cyber Security Incidence Response Plan
- Microsoft Unified Support including on demand assessments
- vCISO (Virtual Chief Information Security Officer) audit and cyber security framework based reporting

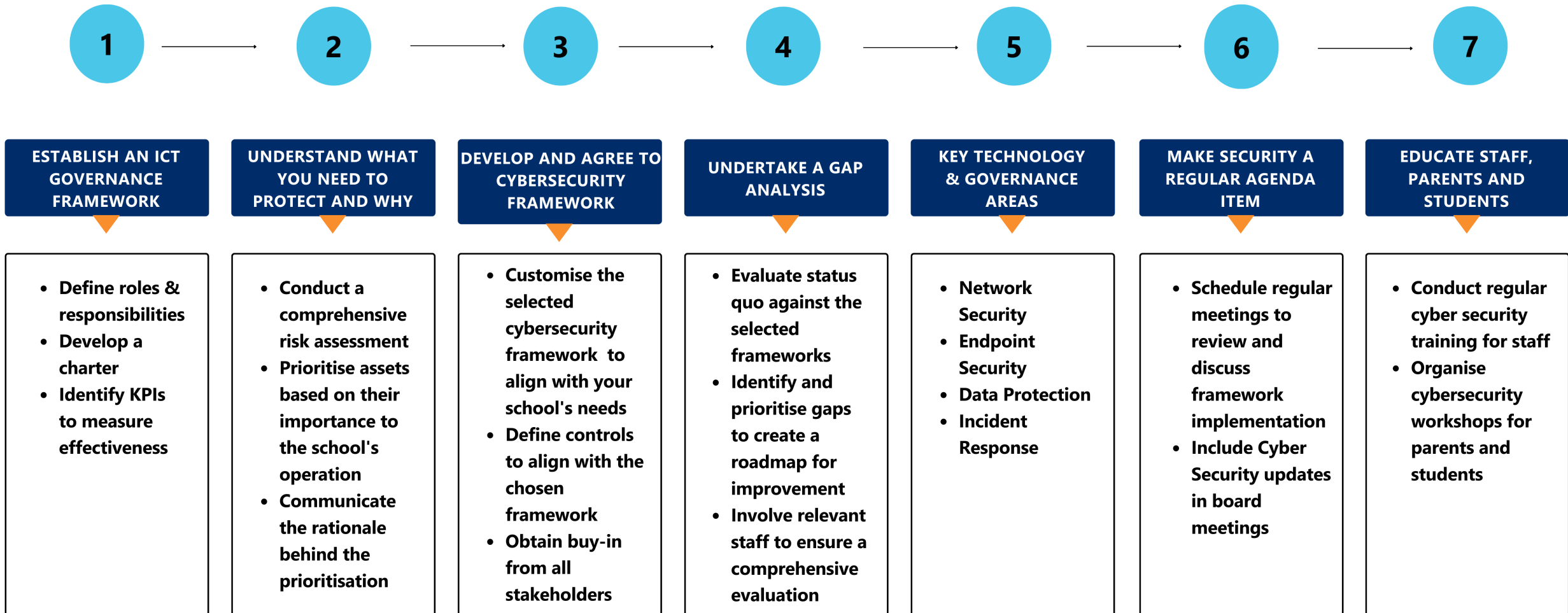
Planning and preparing *for a cyber-attack*

Minimising:

- Risk
- impact



Planning and preparing for a Cyber-Attack



1 – Establish an ICT Governance Framework

- 1 GOVERNANCE
- 2 PROTECT
- 3 FRAMEWORK
- 4 GAP ANALYSIS
- 5 KEY TECH
- 6 AGENDA ITEM
- 7 EDUCATE

The key tasks to establishing an ICT Governance Framework with an IT Steering Committee include:



2 – What to Protect and Why?

- 1 GOVERNANCE
- 2 PROTECT
- 3 FRAMEWORK
- 4 GAP ANALYSIS
- 5 KEY TECH
- 6 AGENDA ITEM
- 7 EDUCATE

To effectively protect your school's assets, it is crucial to understand what needs to be protected and why.



What is Data and Application Mapping?

- Identify data-app relationships
- Understand data flow, access, manipulation
- School gains insights into:
 - IT data flow
 - App interaction
 - Data protection
 - Ingress/egress points to network
 - Security weaknesses

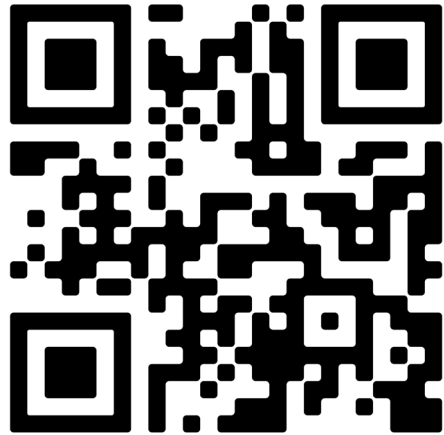
Cyber Risk Assessment

Data Map and Sensitivity Rating

- Data Sensitivity
 - Public
 - Personal
 - Sensitive
- Visual representation of risk in each system.
- Can be reviewed internally or by software provider
- Data classification categories:
 - Student and Parent Data
 - Staff Data
 - Finance
 - HR and Payroll
 - Marketing
 - Governance, Risk and Compliance
 - IT Data

Data Categories	Data Items	Sensitivity Label Impact to school if information is included in a data breach High = 5, Low = 1
Cloud or On Premise		
MFA Enabled		
Student and Parent Data	Student - Name	3
	Student - Address	4
	Student - Photos	4
	Student - DOB	4
	Student - Medical records	5
	Student - Academic Records	4
	Student - School email address	3
	Student - Mobile phone number	3
	Student - Counselling notes	5
	Student - discipline notes	5
	Student - welfare notes	5
	Parent - Name	3
	Parent - Address	4
	Parent - Phone number	3
	Parent - email address	3
	Parent - Bank account details	5
	Parent - Credit card details	5
Staff data	Staff - Name	3
	Staff - Address	4
	Staff - DOB	4
	Staff - Personal phone numbers	4
	Staff - Photos	4
	Staff - Personal email address	4
	Staff - License or other	5

Data Classification Activity



Or go to this link and click

"View Data Classification Exercise":

<https://www.neweratech.com/au/covenant-principals-conference-cybersecurity-in-schools/>

- 1 GOVERNANCE
- 2 PROTECT
- 3 FRAMEWORK
- 4 GAP ANALYSIS
- 5 KEY TECH
- 6 AGENDA ITEM
- 7 EDUCATE



Risk Rating Worksheet					
Data Categories	Data Items	Sensitivity Label* High = 5, Low = 1	Student Information System	HR System	Payroll System
Student and Parent Data	Student - Name	3			
	Student - Address	4			
	Student - Photos	4			
	Student - DOB	4			
	Student - Medical records	5			
	Student - Academic Records	4			
	Parent - Name	3			
	Parent - Address	4			
	Parent - Phone number	3			
	Parent - email address	3			
Staff data	Parent - Bank account details	5			
	Parent - Credit card details	5			
	Staff - Name	3			
	Staff - Address	4			
	Staff - DOB	4			
	Staff - Personal phone numbers	4			
	Staff - Photos	4			
	Staff - Personal email address	4			
	Staff - License or other identity documents	5			
	Staff - Tax File Numbers	5			
Finance	Invoicing Ledger Data	4			
	Historic Invoicing Data	4			
	Bank Details	5			
	Tax Return Data	5			
	Vendor/Supplier/Contractor Contact and Bank Details for payment	3			
HR and Payroll	Staff ID (DCL), Addresses, Copies of Identity Documents	5			
	Salary & Payroll Data	5			
	Staff Tax File Numbers	5			
	Employee Contracts	4			
Marketing	Police Checks	5			
	Website Data	2			
Governance, Risk and Compliance	Marketing Campaign Data	2			
	Board Papers & Minutes	3			
	Breach Reports	5			
	Regulatory Reports	3			
IT Data	Risk Register Data	2			
	Incident Register Data	4			
	Infrastructure map	5			
	IT passwords	5			
	Asset Lists	5			
	Data Maps	5			

* Sensitivity Label: Impact to school if information is included in a data breach



Cyber Risk Assessment

Cyber Security Questionnaire for Vendors

Gauge how the vendors treat your data and what security practises they employ:

- Data protection
- Security and integrity
- Backups and recovery
- Compliance and certifications
- Risk management

Easy to access online questionnaire using Microsoft Forms



Or go to this link and click
"Questions to ask Third-Party Vendors":

General Security

4. What security measures do you have in place to protect against common threats like malware, DDoS attacks, and data breaches?

Enter your answer

5. Do you conduct regular security audits or penetration tests to identify vulnerabilities?

Enter your answer

6. Are your systems and applications regularly patched and updated to address known security vulnerabilities?

Enter your answer

3 – Develop and Agree to a Cyber Security Framework

Cyber Security Frameworks

- 1 GOVERNANCE
- 2 PROTECT
- 3 FRAMEWORK
- 4 GAP ANALYSIS
- 5 KEY TECH
- 6 AGENDA ITEM
- 7 EDUCATE

**Essential 8
Maturity Model
Australian Cyber Security
Centre (ACSC)**

**National Institute of
Standards and Technology
(NIST) Cyber Security
Framework**

Essential 8 (Maturity Model)

Strategies

- 1 GOVERNANCE
- 2 PROTECT
- 3 **FRAMEWORK**
- 4 GAP ANALYSIS
- 5 KEY TECH
- 6 AGENDA ITEM
- 7 EDUCATE



Application control

To control the execution of unauthorised applications / software



Patching applications

To remediate known security vulnerabilities



Configure Microsoft Macro Settings

To block untrusted macros and only allow checked macros from trusted locations



User application hardening

Configure web browsers to block and disable potential malware



Restrict Admin privileges

To limit powerful access to important business information and systems



Patch Operating Systems

To remediate known security vulnerabilities



Multi-Factor Authentication

To protect against unauthorised access



Daily Backups

To maintain the availability of critical business data

Essential 8 (Maturity Model)

Maturity Levels

- 1 GOVERNANCE
- 2 PROTECT
- 3 FRAMEWORK
- 4 GAP ANALYSIS
- 5 KEY TECH
- 6 AGENDA ITEM
- 7 EDUCATE

Level 0



There are weaknesses in an organisation's overall cybersecurity posture

Level 1



The organisation can likely hold its own against a noncommittal attack using basic tradecraft and tools

Level 2



The organisation is ready to handle attacks from a more committed attack

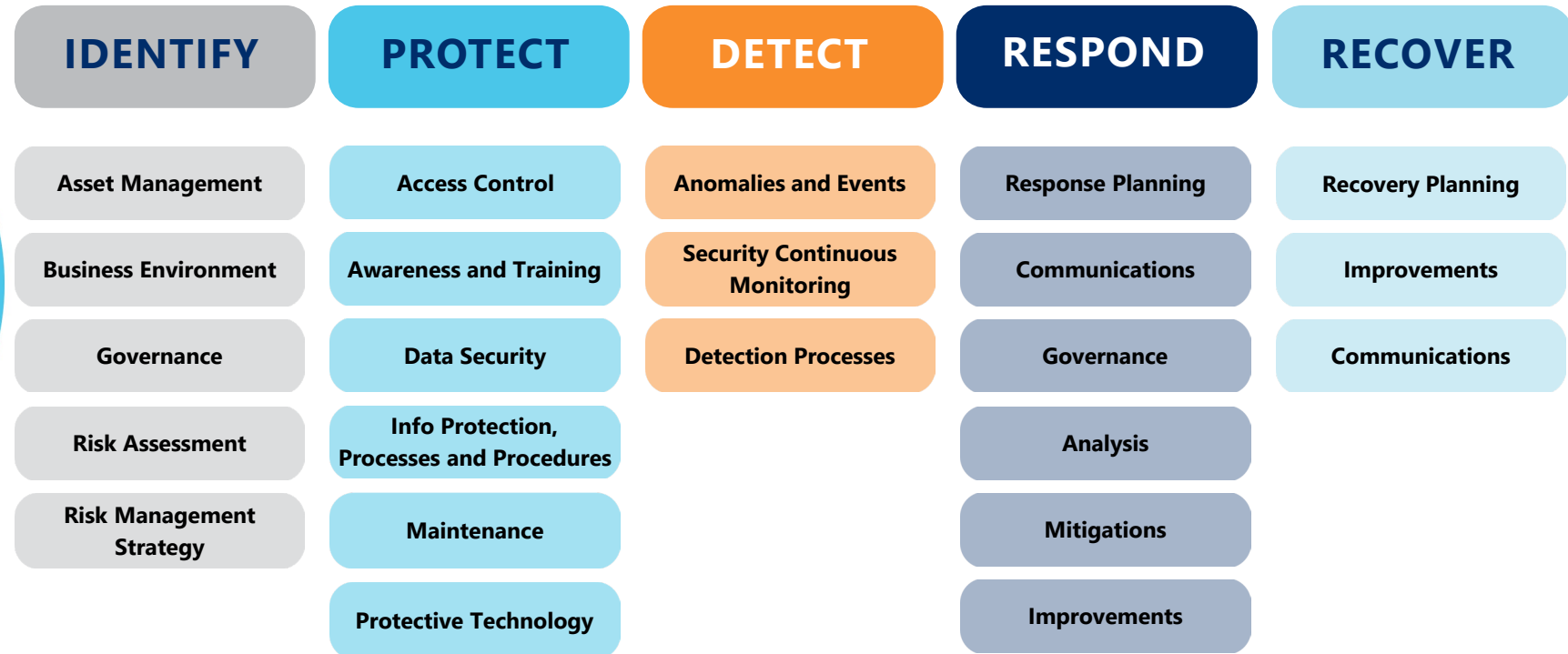
Level 3



The organisation can mitigate attacks from a dedicated threat actor using advanced tradecraft and techniques

NIST Cybersecurity Framework

- 1 GOVERNANCE
- 2 PROTECT
- 3 FRAMEWORK
- 4 GAP ANALYSIS
- 5 KEY TECH
- 6 AGENDA ITEM
- 7 EDUCATE



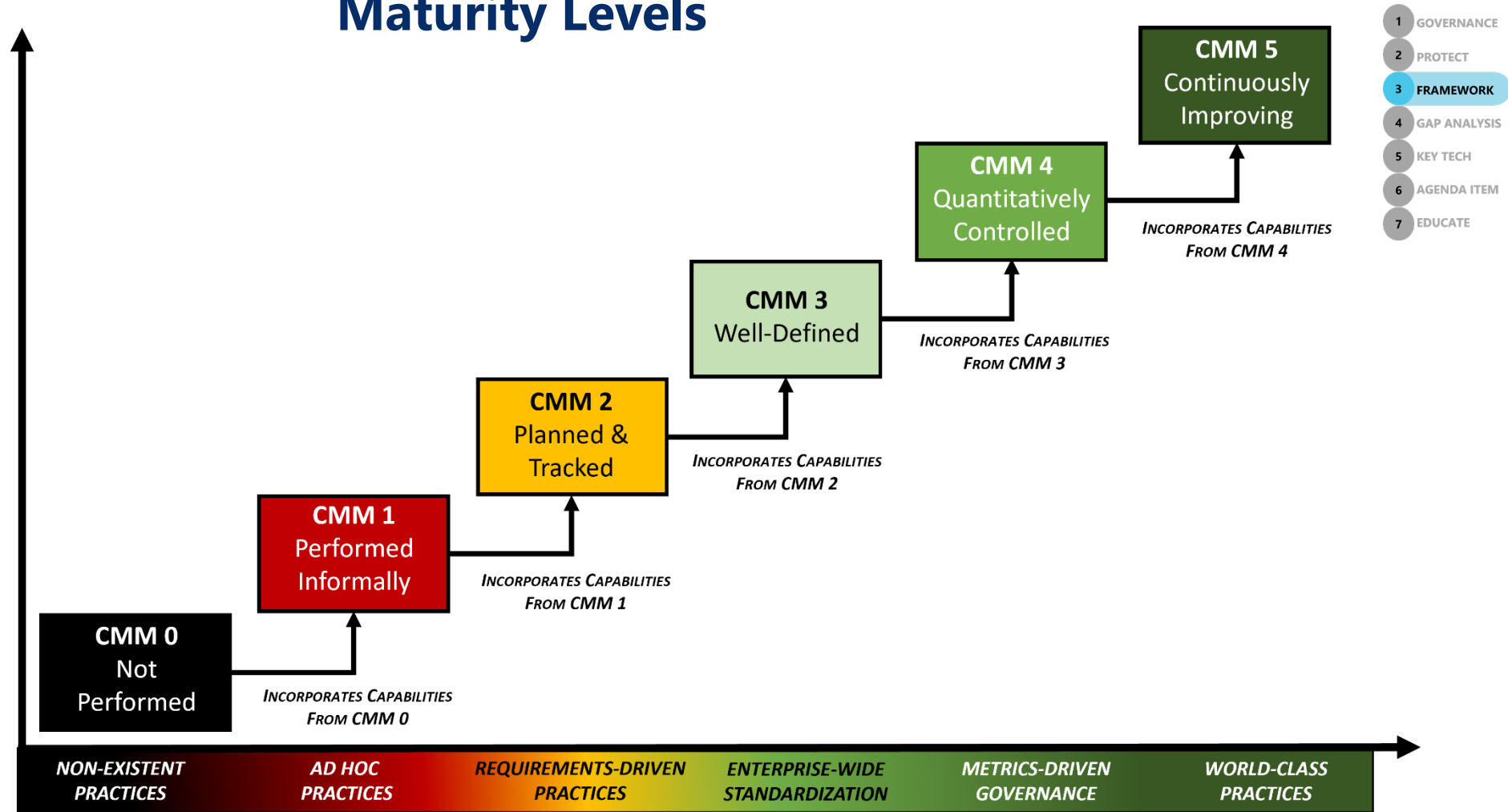
- Made up of 5 core functions.
- Each function is defined.
- Within each function is a set of assessable areas

NIST Cybersecurity Framework

Maturity Levels



COST & COMPLEXITY



MATURITY LEVEL (PEOPLE, PROCESSES & TECHNOLOGY)

Steps to implement a Cyber Security Framework

- 1 GOVERNANCE
- 2 PROTECT
- 3 FRAMEWORK
- 4 GAP ANALYSIS
- 5 KEY TECH
- 6 AGENDA ITEM
- 7 EDUCATE

Identify security Influences

- Business Objectives
- Risk Management Framework
- Government Requirements
- Other



Confirm Framework

E.g. NIST

- Identify
- Protect
- Detect
- Respond
- Recover



CYBERSECURITY FRAMEWORK VERSION 1.1



Identify Current State

- Scorecard
- Risk Assessment
- Gap analysis



Define Target Security Levels and Scorecard



Develop Uplift Roadmap



Progress Reports, Security Updates

reported into ICT Steering Committee, School Executive and Board.

4 – Undertake a Gap Analysis

to assess the Cybersecurity posture of the School

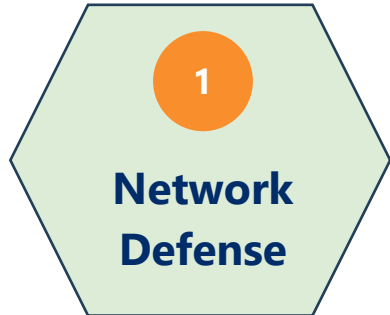
- 1 GOVERNANCE
- 2 PROTECT
- 3 FRAMEWORK
- 4 **GAP ANALYSIS**
- 5 KEY TECH
- 6 AGENDA ITEM
- 7 EDUCATE

GAP ANALYSIS STEPS

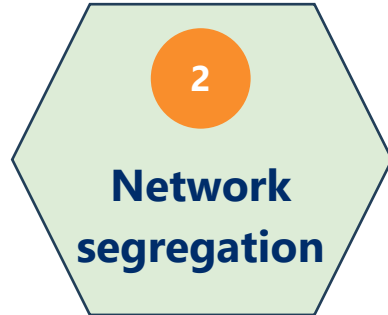
- 1 Identify Framework Core Functions
- 2 Define Desired State
- 3 Assess Current State
- 4 Identify Gaps
- 5 Prioritise Gaps
- 6 Develop & Implement Plans
- 7 Monitor, Track, Review Progress

5 – Key Technology Areas for a Cyber-Attack preparations

- 1 GOVERNANCE
- 2 PROTECT
- 3 FRAMEWORK
- 4 GAP ANALYSIS
- 5 KEY TECH
- 6 AGENDA ITEM
- 7 EDUCATE



Firewalls, Endpoint Security



Segregate staff, student, guest and infrastructure networks.



OS + App Software Maintenance

Patch OS & apps regularly



Minimise admin privileges



Strong Passwords, Multi-factor Authentication



Continuous Assessment

Vulnerability Tests, Penetration Tests



Threat Protection

Intrusion Detection, Suspicion Monitoring



Centralised Monitoring & Alerts

5 – Key Technology Areas for a Cyber-Attack preparations

- 1 GOVERNANCE
- 2 PROTECT
- 3 FRAMEWORK
- 4 GAP ANALYSIS
- 5 KEY TECH
- 6 AGENDA ITEM
- 7 EDUCATE



Regular Backups & Review
Immutable/Air-Gapped Copy



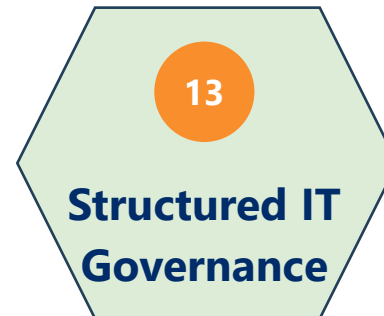
Recovery Testing



Clear Roles & Responsibilities



Conditional Access



Policies & Procedures
Disaster Recovery &
Business Continuity

6 – Make Security a Regular Agenda Item

- 1 GOVERNANCE
- 2 PROTECT
- 3 FRAMEWORK
- 4 GAP ANALYSIS
- 5 KEY TECH
- 6 AGENDA ITEM
- 7 EDUCATE



Establish ICT Steering Committee



Make Cyber Security an agenda item in ICT Steering Committee and Board Updates



Discuss identified gaps and risks (be transparent)



IT provides updates on framework implementation



Discuss emerging threats



Seek expert guidance and support, if required

7 – Educate Staff, Parents, and Students on Cyber Security

- 1 GOVERNANCE
- 2 PROTECT
- 3 FRAMEWORK
- 4 GAP ANALYSIS
- 5 KEY TECH
- 6 AGENDA ITEM
- 7 EDUCATE



Regular Training Sessions

- Staff
- Parents
- Students



Audience-Centric Approach

- Relevant Content for Roles



Focus Areas

- Password Security
- Phishing Awareness
- Social Engineering
- Safe Browsing
- Data Privacy
- Responsible Social Media Use



Promote Reporting & Communication



Acceptable Use of Resources

- School Equipment & Systems

7 – Educate Staff, Parents, and Students on Cyber Security

- 1 GOVERNANCE
- 2 PROTECT
- 3 FRAMEWORK
- 4 GAP ANALYSIS
- 5 KEY TECH
- 6 AGENDA ITEM
- 7 EDUCATE



Consistent Reinforcement

- Regular Cybersecurity Practice



Audience-Centric Approach

- Relevant Content for Roles



Addressing Cyberbullying



Teaching Digital Citizenship



Managing Screen Time

- Implementing Parental Controls



<https://www.esafety.gov.au/parents/issues-and-advice>

7 – Educate Staff, Parents, and Students on Cyber Security

- 1 GOVERNANCE
- 2 PROTECT
- 3 FRAMEWORK
- 4 GAP ANALYSIS
- 5 KEY TECH
- 6 AGENDA ITEM
- 7 EDUCATE

To educate staff, parents and students on Cybersecurity effectively:



Audience Relevance

- Tailored Content
- Role-Specific Information



Consistent Reinforcement

- Regular Cybersecurity Practice



<https://www.covenant.nsw.edu.au/parent-resources/technology-support/technology-advice-for-parents>

7 – Educate Staff, Parents, and Students

Application: KnowBe4

- 1 GOVERNANCE
- 2 PROTECT
- 3 FRAMEWORK
- 4 GAP ANALYSIS
- 5 KEY TECH
- 6 AGENDA ITEM
- 7 EDUCATE



Phishing Defense

- Regular Tests & Training
- Guard Against Social Engineering



Phishing Reporting

- Simplified Alert Process
- Webmail & Email Client Button



Assessment Measures


- Baseline & Follow-up Checks

Email exercise

Your delivery from EL is on its way

 Australia Post <noreply@notifications.auspost.com.au>
To: sjames@covenant.nsw.edu.au

[↩ Reply](#) [↩ Reply All](#) [→ Forward](#)

 If there are problems with how this message is displayed, click here to view it in a web browser.

From EL
Tracking number **338XH3358674**

Expected **Tuesday 23 Jul 2024 – Wednesday 24 Jul 2024***

We'll update the expected delivery date as your item progresses, so you can stay updated by [tracking your item](#).

We'll also send you a notification when the driver loads your item onto their vehicle on the day of delivery.


If nobody's home to sign for your delivery, we'll take it to a local Post Office and email you when it's available to pick up.

Here are your delivery options.

<https://click.notifications.auspost.com.au/u/?qs=cf6d70b4b54d73a7c180449e82a708cf532d41fb3c6af9faf01b0b6936e322e67fe207c8030f8f5a3a559006a86b64b8aaa1abbcedf4db8aaef22ed706cb86>
Click or tap to follow link.

Leave it in a safe place

From: AUSTRALIA POST <licas123740@skinlinecos.me>
Date: 8 December 2020 at 11:47:12 AEDT
To: sjames@covenant.nsw.edu.au
Subject: Failed to deliver



Your shipment number **51036609** has not yet been delivered for the following reason: **Incorrect address**
We invite you to correct your address, and pay the new shipping costs (**2,40 AUD**) on the following link to receive your package tomorrow.

[Click to correct your address](#)

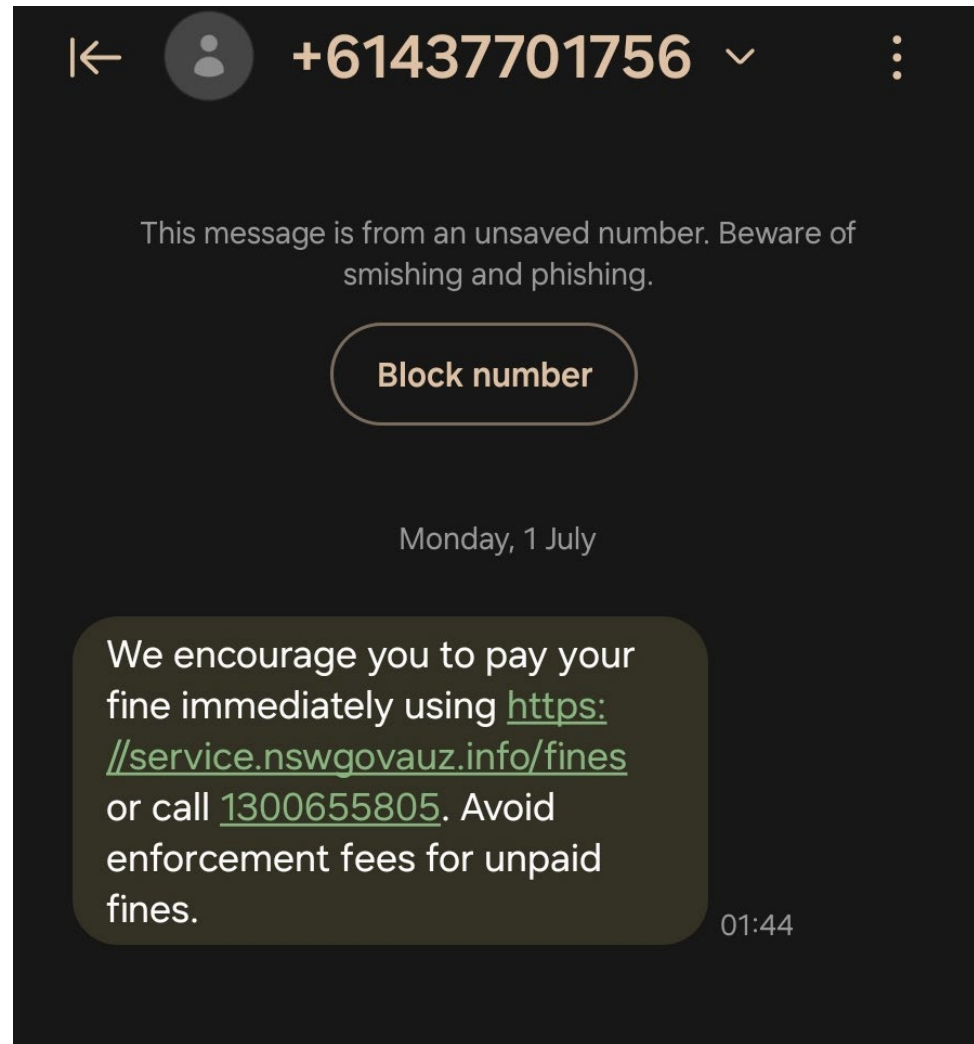
Thanks.

Correct your address before 05:59 PM to receive it tomorrow

This is an automated message - please do not reply directly to this email

Email ID sjames@covenant.nsw.edu.au

SMS exercise



7 – Educate Staff, Parents, and Students

KnowBe4 Baseline Phishing Test and Initial Assessment

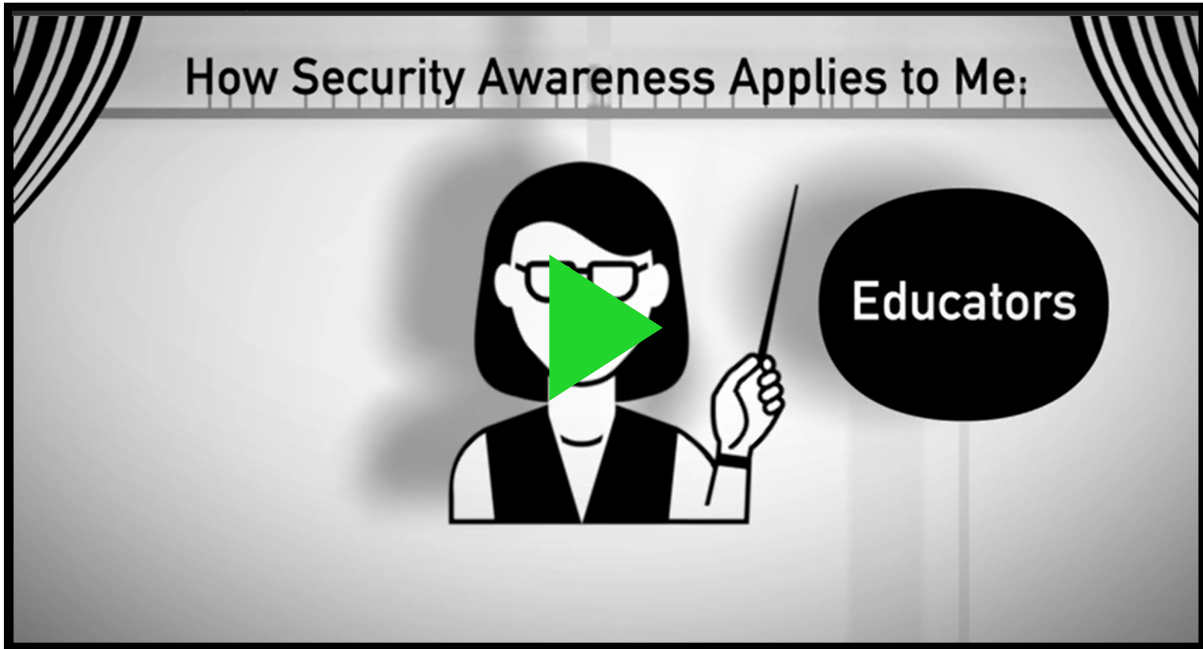
- Assess organisation awareness.
- Establish
- Establish a baseline in order to determine training focus and measure progress:
 - Baseline phishing test.
 - Baseline assessment (CHECK WORDING)

- 1 GOVERNANCE
- 2 PROTECT
- 3 FRAMEWORK
- 4 GAP ANALYSIS
- 5 KEY TECH
- 6 AGENDA ITEM
- 7 EDUCATE

7 – Educate Staff, Parents, and Students

KnowBe4 Training Module

- 1 GOVERNANCE
- 2 PROTECT
- 3 FRAMEWORK
- 4 GAP ANALYSIS
- 5 KEY TECH
- 6 AGENDA ITEM
- 7 EDUCATE



Security Culture Survey

1. It is normal in our organization for people to send sensitive materials by email to get work done efficiently.

Strongly Disagree Disagree Neither Agree Nor Disagree Agree Strongly Agree

2. I think that adherence to information security policies is especially important for those dealing with sensitive data, while others can be more relaxed.

Strongly Disagree Disagree Neither Agree Nor Disagree Agree Strongly Agree

3. The people in our organization who are experts on computer issues are often difficult to reach.

Strongly Disagree Neither Agree Strongly

Preparing a Cyber Security *incident response plan*



Incident Management



INCIDENT



PROCESS



DETECTION



ANALYSIS

- A cyber incident is any attempted or actual unauthorised access.



**INITIAL
SUPPORT**



RESTORE



REPORTING

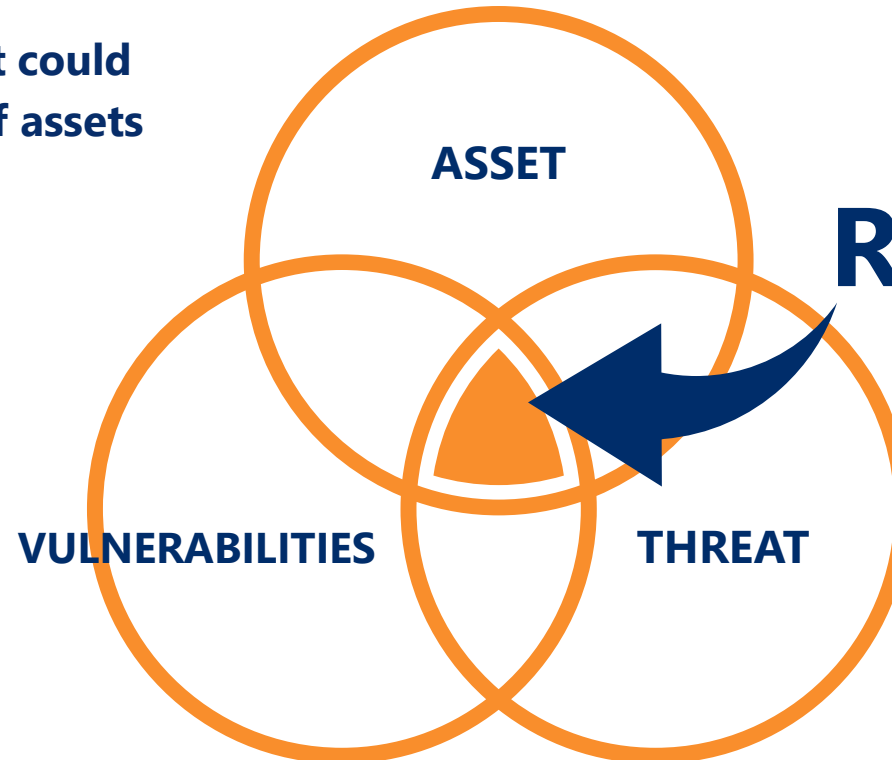
- The goal of incident response is to detect and halt attacks.

Risk Management Terms

ASSET | Anything of value

VULNERABILITIES | Weakness or flaw that could be exploited

THREAT | Something that could lead to a loss of assets



RISK | Potential for loss/damage of an asset when a threat exploits a vulnerability

Risk Management

- It is not realistic to protect all systems equally.
- Risk management aims to **mitigate**, not eliminate risks.





Critical Steps for Cyber Security Incident Response Planning



IDENTIFY ASSETS & RISKS



DEVELOP INCIDENT RESPONSE PLANS & SUPPORT TEAMS



EXECUTE PLAN WITH EXECUTIVE ENDORSEMENT



PLAN WITH YOUR PEOPLE



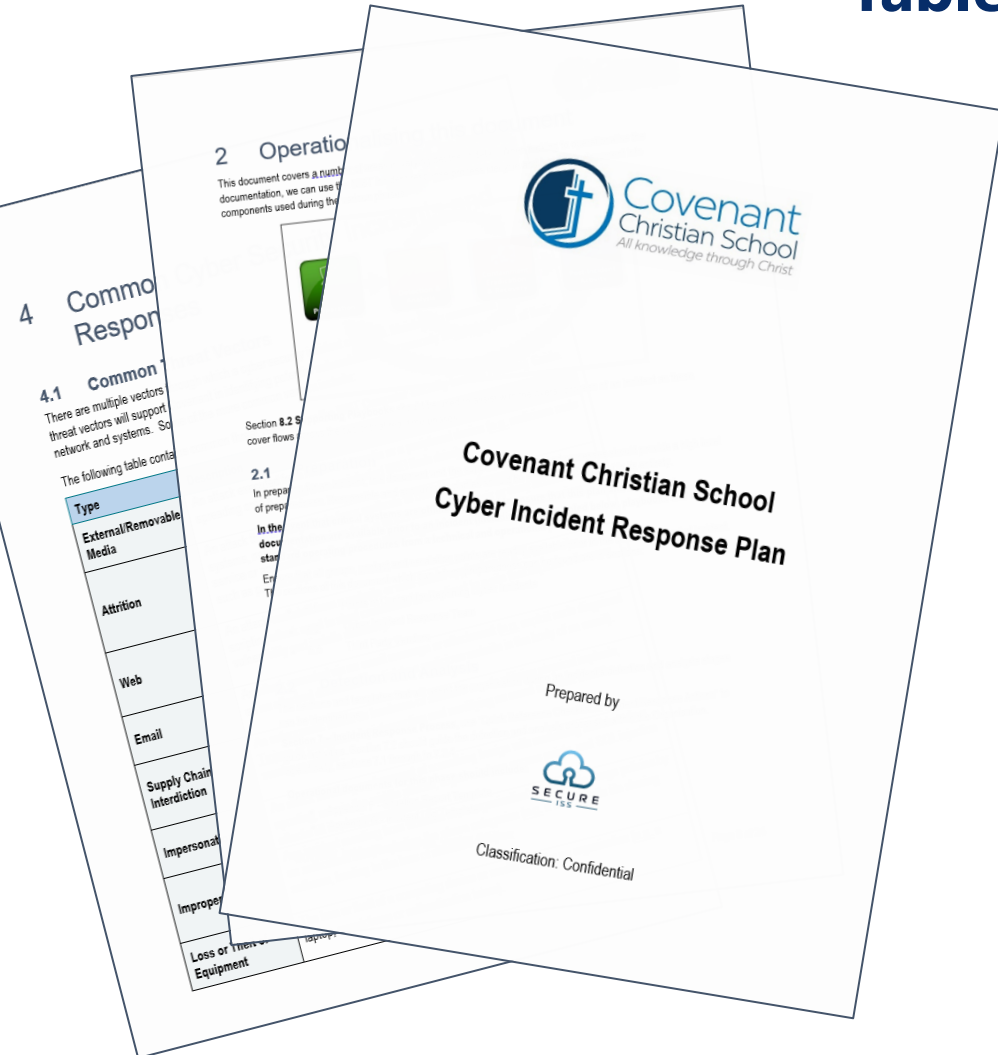
REASSESS & REFINE

- IDENTIFY
- DEVELOP
- ENDORSEMENT
- PLAN
- REASSESS

Cyber Incident Response Plan

Table of Contents to include:

- IDENTIFY
- DEVELOP
- ENDORSEMENT
- PLAN
- REASSESS



Document control
Version history
Release approval

1 Introduction

- 1.1 Context
- 1.2 Purpose
- 1.3 Authority
- 1.4 Review

2 Operationalising this document

- 2.1 Preparation
- 2.2 Detection and Analysis
- 2.3 Containment, Eradication and Recovery
- 2.4 Post Incident Activity

3 Terminology and Definitions

- 3.1 What is a cyber security event?
- 3.2 What is a cyber security incident?
- 3.3 Information and Data Classification
 - 3.3.1 Very Sensitive Data
 - 3.3.2 Sensitive Data
 - 3.3.3 Private Data
 - 3.3.4 Public Data
 - 3.3.5 Systems and Data Classification

4 Common Cyber Security Incidents and Responses

- 4.1 Common Threat Vectors
- 4.2 Common Cyber Incidents

5 Roles and Responsibilities

- 5.1 Points of Contact for Reporting Cyber Incidents

5.1.1 Escalation

- 5.2 Cyber Incident Response Team (CIRT)
- 5.3 Critical Incident Coordinating Team (CICT)

5.4 Board of Trustees

5.5 Third Party Vendors

5.6 Incident Notification and Reporting

- 5.6.1 Legal and Regulatory Requirements
- 5.6.2 Cyber Insurance

6 Communications

- 6.1 Internal Communications
- 6.2 External Communications
- 6.3 Supporting documentation
- 6.4 Document Storage

7 Incident Response Process

- 7.1 Detection, Analysis, Classification, Activation
- 7.2 Containment, Evidence Collection & Remediation
- 7.3 Recovery

8 Playbooks and Supporting Procedures

Identify Assets and Risks

- IDENTIFY
- DEVELOP
- ENDORSEMENT
- PLAN
- REASSESS

Identify data to protect and its location, prioritise valuable assets, address vulnerabilities, conduct penetration tests, and understand financial risks.

Threat Classification Overview:

- Confidentiality
- Integrity
- Availability



Operational Continuity

- IDENTIFY
- DEVELOP
- ENDORSEMENT
- PLAN
- REASSESS

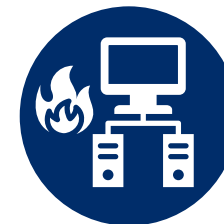
- Ensure essential school and business functions and processes continue
- Minimise downtime
- Avoid negative impacts
- Swift Restoration of IT Systems



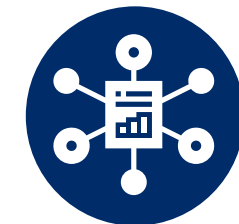
Assess the School's Backup Strategy & Create a Written Backup Plan



Develop a Business Continuity Plan (BCP)



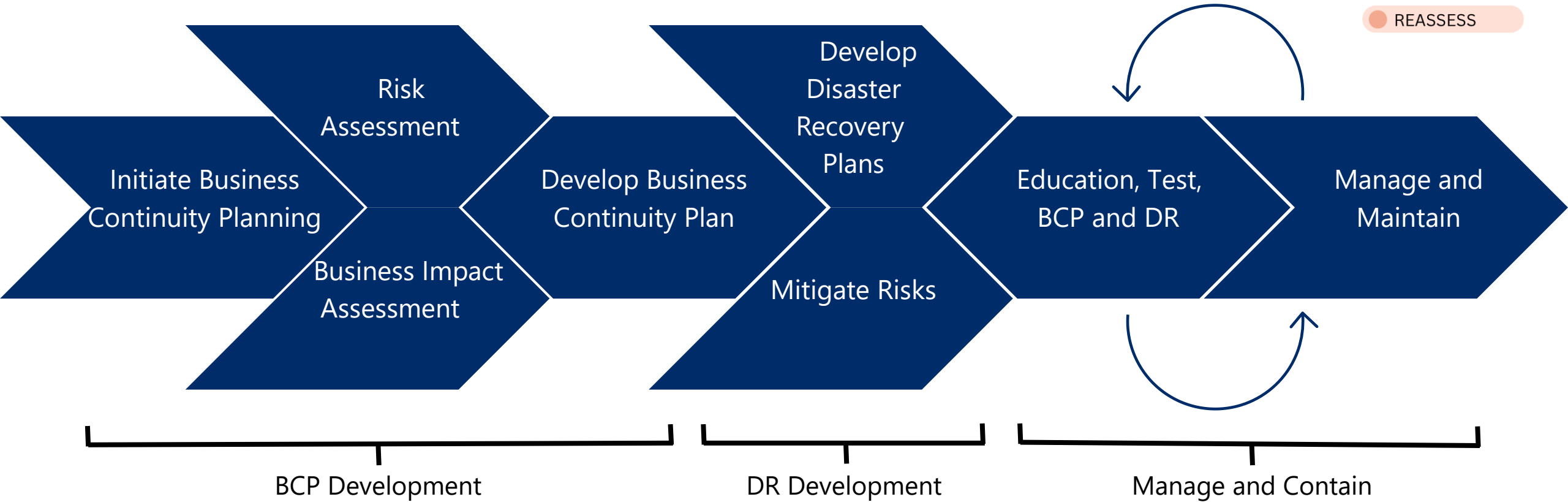
Develop Disaster Recovery Plans (DR)



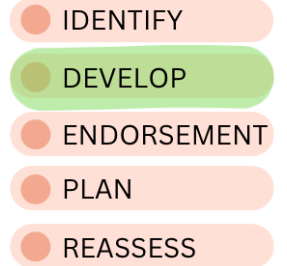
Base structure on chosen Framework. i.e. CIS.

Disaster Recovery and Business Continuity

- IDENTIFY
- DEVELOP
- ENDORSEMENT
- PLAN
- REASSESS



Incident Response Team Model



- Specialised team focused on rapid response to critical incidents
- Minimise damage, restore operations and protect assets
- Comprised of key stakeholders across the school
- Brings together technical, operational, and communication expertise

CIRT – **C**ritical **I**ncident **R**esponse **T**eam

CIST – **C**ritical **I**ncident **C**oordinating **T**eam

Board – School Board

Incident Response Team Model

Critical Incident Response Team - CIRT

- IDENTIFY
- DEVELOP
- ENDORSEMENT
- PLAN
- REASSESS

- Responsible for managing and responding Cyber Security incidents.
- Identify, contain, mitigate, and recover.
- Executes the incident response plan and coordinates technical actions.
- Minimise damage and protect the school's data and digital assets.

CIRT Role	Name	Contact Details
CIRT Leader* Incident Controller Executive support & school liaison **CFC Response App user**	Business Manager	Email Phone
CIRT Leader* Incident Controller Executive support & school liaison	Deputy Principal	Email Phone
CIRT Leader* Incident Controller Cyber planning & operations **CFC Response App user**	Director of ICT	Email Phone
CIRT Leader* Investigation, analysis, containment, eradication, system administration, incident & evidence logs, situation report, restoration & recovery. **CFC Response App user**	IT Manager	Email Phone
CIRT Member Investigation, analysis, containment, eradication, systems administration, restoration & recovery	IT Team Member	Email Phone
CIRT Member Logistics support	Senior Executive Assistant	Email Phone
CFC Underwriting – CFC Response Incident response, digital forensics, ransom negotiation, system recovery, hardware replacement, legal advisory services (incl. regulatory compliance), etc. as detailed in policy certificate.	Cyber Insurer / Broker CFC	Email Phone Website
Outsourced Security Operations Centre (SOC); detection, intelligence and analysis, technical advice, evidence collection, critical incident containment.	Secure ISS Manager	Email Phone Website
Network/ system/ application support (Members should be added to the CIRT based upon incident impact and scope).	Third Party Vendors MSP, Network Provider	Email Phone Website

Incident Response Team Model

Critical Incident Coordinating Team- CICT

- IDENTIFY
- DEVELOP
- ENDORSEMENT
- PLAN
- REASSESS

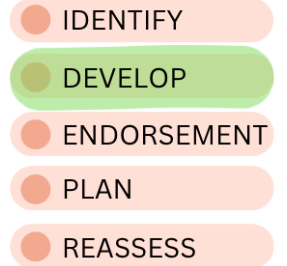
- Provide strategic oversight, direction and support to the CIRT.
- Stakeholder engagement and communications.
- Resource and capability demand.
- Coordinates communication and decision-making across various departments

CICT Role	Name	Contact Details
CICT Leader* / Incident Controller	Principal	Email Phone
CICT Leader* / Incident Controller	Deputy Principal	Email Phone
CICT Leader* / Incident Controller	Business Manager	Email Phone
CICT Checkpoint Coordinator	Head of Junior School	Email Phone
CICT Checkpoint Coordinator	Head of Secondary School	Email Phone
CICT Coordinator	Director of Student Wellbeing	Email Phone
CICT Internal & External Comms. Coordinator	Senior Executive Assistant	Email Phone

* If the Principal is not available, the Deputy Principal or Business Manager becomes CICT Leader / Incident Controller

Incident Response Team Model

School Board



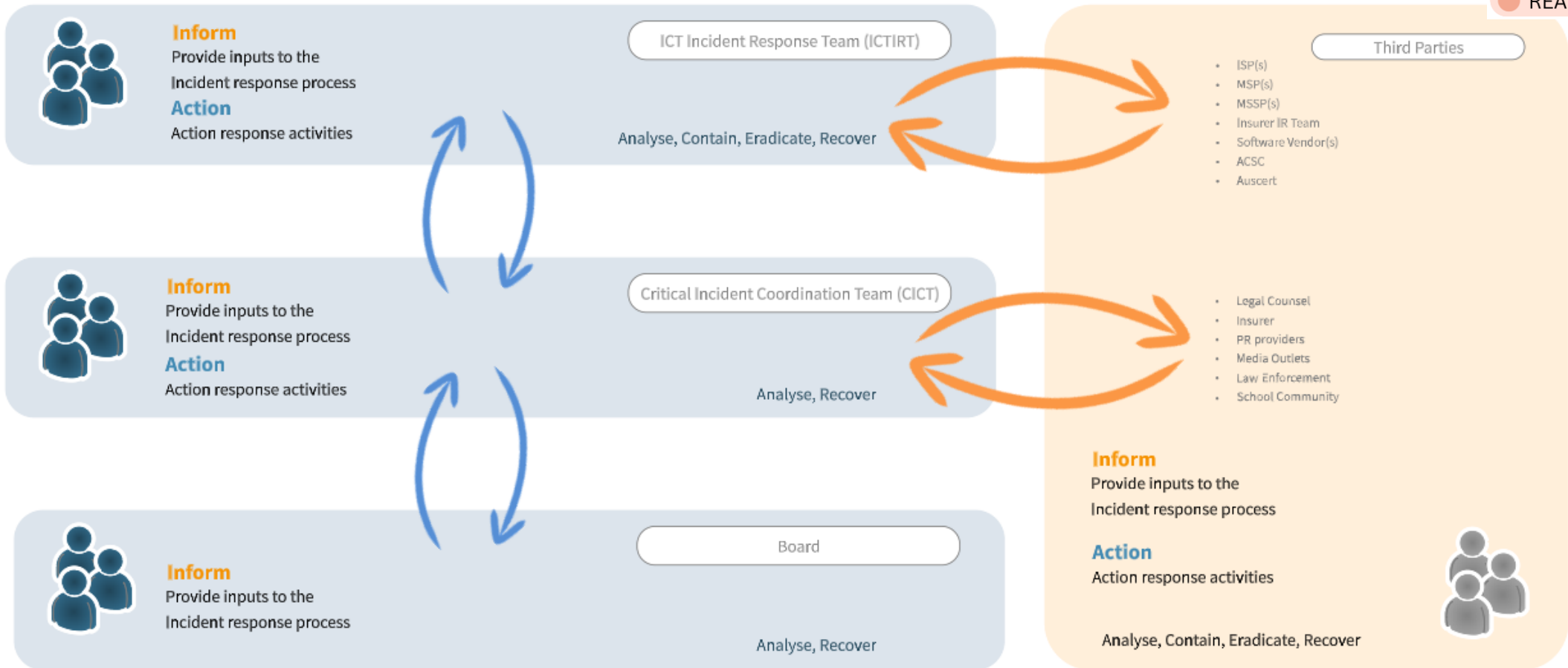
Although not actioning response activities, Board will assist the CICT in guiding response activities particular during containment and recovery phases.

Questions that the Board should be prepared to provide guidance to:

- How does the Board determine the risk appetite in relation to the reputational damage that a data breach may cause?
- How does the Board quantify the reputational damage an event may have on the school?
- In the event of a ransom demand, will the organisation consider payment?

Incident Response Team Model

- IDENTIFY
- DEVELOP
- ENDORSEMENT
- PLAN
- REASSESS



Communication with School Community in the event of an outage

- IDENTIFY
- DEVELOP
- ENDORSEMENT
- PLAN
- REASSESS

Contents of Scheduled Report	2 reports which produce current Student, Parent and Staff contact details and key communication information.
Recipients of the Report	Business Manager, Director of ICT, ICT Manager (sent to roles not individuals)
Schedule and Frequency	Fortnightly
Data Transfer to Encrypted USB / Secure Storage	Work in progress
Designated Platform for Bulk Email Dissemination	SendGrid
Designated Platform for Bulk SMS Delivery	SMS Central

Covenant Incident Response Plan

Extract: Playbooks

The playbooks provide high-level guidance for responding to cyber incidents and are not intended to be exhaustive. Many technical tasks referenced require separate internal procedures. These playbooks support the activities of the Covenant IT team, CIRT, CICT and third parties. Responsible parties are assigned to tasks in the Playbooks. The actual persons undertaking the tasks may vary depending on individual situations.

Note: Phishing, Malware & DoS attacks are often pre-cursors to a Data Breach or Ransomware.

Incident Response Overview – Malware Playbook

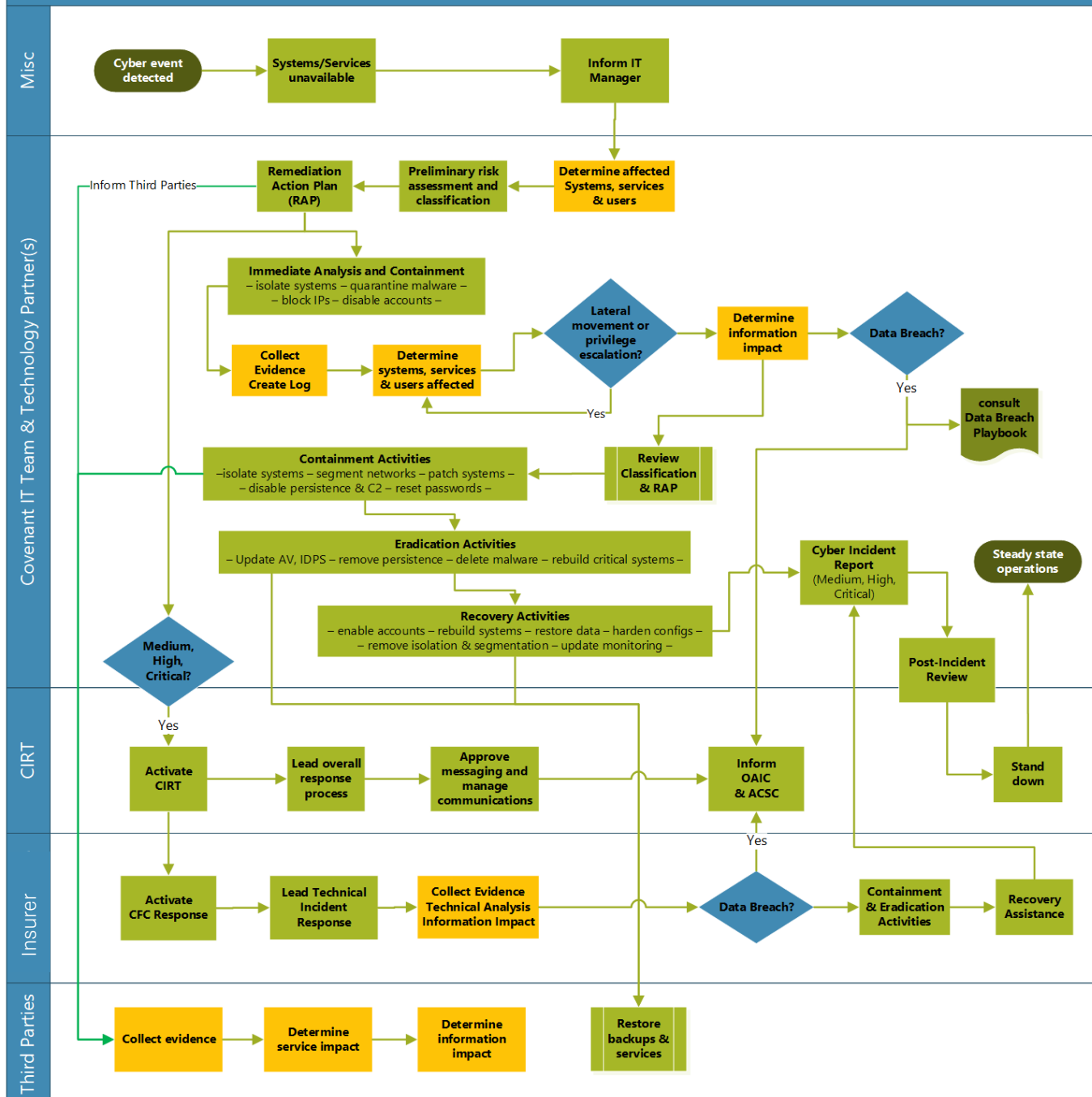


Table-Top Exercises

- Simulated cyber attack
 - Training of key staff.
 - Stress testing the Cyber Security Incident Response Plan.
- Table-top exercise: DDOS and Malware, Phishing and Ransomware

Friday, 13th October 2:00pm

- The day has been like any other...

- 2:00pm

Multiple emails have been forwarded by school staff members, requesting input into their legitimacy.

We know of at least 13.



Critical Microsoft Authenticator Update

Dear [REDACTED],

We respectfully request that you upgrade your Microsoft Authenticator app to the most recent version in order to protect the security of your account and to continue offering you a seamless authentication experience.

This update is necessary to improve the app's security features and guarantee the continuous security of your account. You will also be able to take advantage of the most recent additions and enhancements thanks to it.

Scan the QR Code to update your microsoft authenticator application



Thank you for being a valued customer!

© 2023 Microsoft Corporation. All rights reserved.

Microsoft Corporation, Two Microsoft Way, Redmond, CA 98634

Friday, 13th October Actions from 2:00pm

- Forward email in its entirety to SOC/SIEM Secure-ISS for forensics.
- Check KnowBe4 phishing portal to confirm it is not a campaign.
- Check Exchange admin centre to determine recipients with message trace.
- Check with recipients as to what actions they took.
- KnowBe4 recall from all mailboxes.

Friday, 13th October 2:30pm

- 2:30pm

A significant number of helpdesk tickets have been lodged in relation to laptops running slowly and crashing! These are across both students and faculty members.

- 2:45pm

The Sophos console is “lighting up like a Christmas tree” with a number of alerts in relation to Malware being stopped and potentially unwanted applications being installed.

Friday, 13th October Actions from 2:30pm

- Check Microsoft Security and Compliance centre for potentially compromised users.
- Ask Senior Engineer to investigate.
- As timing is close to finish time on Friday, capacity to reach out to staff is limited. The Business Manager and Deputy Principal engaged to handle staff communications and information gathering.
- Ask Secure ISS about malware – what is the risk level? How do we deal with the malware? Is it exploiting a vulnerability that needs to be patched?
- Spreadsheet created to track affected users and their actions.
- Notify CFC (insurance provider) via app for their awareness only.

Friday, 13th October 5:30pm

- 5:30pm

Secure-ISS have detected significant SPAM emails originating from a number of school email addresses.

- 6:00pm

A user, (the Front Office Manager) has reported suspicious activities in their OneDrive and emails. With what looks to be deletions occurring. Can IT take a look?

Friday, 13th October 6:00pm

- 6:00pm

Another user (Director of Student Wellbeing) has sent through another suspicious email.

..." Hi Rob,

ABC Alphabet Schools has recently updated the COVID19 policy regarding illness and work from home policies. As this situation is evolving we require all staff to lead by example and assist in keeping our community safe. This policy is in force tomorrow.

Please review the attached document, sign and return to your supervisor within 24 hours."

Friday, 13th October 8:00pm

- 8:00pm

Secure-ISS have detected indicators of compromise (IOCs) within the School environment related to a recent phishing attack. This attack looks to be targeting the Australian education.

- 8:30pm

After further threat hunting, Secure-ISS have detected several compromised accounts.

Friday, 13th October from 8:00pm - Actions

- Email from Deputy Principal to notify staff that all accounts (except essential IT accounts) will be disabled and not able to be accessed for a period of time. Mobile phone number to be used for all enquiries.
- ICT Team to disable accounts.
- Those accounts still active will have passwords reset.
- Cyber Insurers notified. It is expected they will take the lead on future actions.
- CICT (Critical Incident Coordinating Team) activated.
- Communication to parent community.
- Student accounts disabled.
- Year 12 account mass password reset.

Saturday, 14th October 6:30pm

- 6:30pm

An extortion note (\$48K) has been sent to the school.

Emails sent through to all targeted users and:

admin@abcalpha.nsw.edu.au

enrolments@abcalpha.nsw.edu.au

danceacademy@abcalpha.nsw.edu.au

sportsacademy@abcalpha.nsw.edu.au

!!!!!!!IMPORTANT INFORMATION!!!!!!!

We have discovered and exploited significant weaknesses in your organisation, allowing us to take control of several user accounts.

As a result, we have taken large amount of your data including sensitive student information and personal details of parents and staff. Scanned copies of passports and drivers licenses are included!

We demand payment of 0.5 Bitcoins, or we will begin selling the data on the Dark Web. If you do not have access to Bitcoins, Google Binance, then purchase 0.5 Bitcoins and transfer to the Bitcoins address specified below.


Thank You

Time to pay the Bitcoins

00:47:59:00
Days Hours Mins Secs

Please transfer Bitcoins to this address.

[d3mbHT7k5xpLwRgZ8MiWtj7Wu8SxQgk8VNPqBTwmRd2](https://www.blockchain.com/transaction/d3mbHT7k5xpLwRgZ8MiWtj7Wu8SxQgk8VNPqBTwmRd2)



Monday, 16th October 8:30am

- 8:30am

Another extortion note (\$2.6M) has been sent to the school.

!!!!!!!IMPORTANT INFORMATION!!!!!!!

We have now taken control of your primary education system, thanks to poor security practices by your staff.
We have exfiltrated the entire database of your Edumate platform.

We demand payment of 53 Bitcoins, or we will begin selling the data on the Dark Web.
If you do not have access to Bitcoins, Google Binance, then purchase 53 Bitcoins and transfer to the Bitcoins address specified below.

Thank You


Time to pay the Bitcoins

00:71:59:00

Days Hours Mins Secs

Please transfer Bitcoins to this address.

d3mbHT7k5xpLwRgZ8MiWtj7Wu8SxQgk8VNPqBTwmRd2



Key Learnings from Table-Top Exercise

- Staff are our last line of defense.
 - KnowBe4 phishing training is crucial to ensure we are protected and are updated with latest attack strategies.
- Time is of the essence – delegate activities broadly amongst the team.
- Ensure hard copies of IRP (Incident Response Plan) and key documentation are readily accessible.
- Enabled additional functionality in KnowBe4.
- Reach out to cyber insurers earlier to keep them in the loop.
- Engage Secure-ISS early to assist with forensics.
- Utilise the Deputy Principal (Heads of School as backup) and the Business Manager in staff communications diverting away from the ICT Team.
- Utilise emergency communication mechanisms with staff and parents when school accounts are inaccessible.

Things to consider....

- Is cyber security a regular agenda item at Executive / Board level meetings?
- Is cyber security an integral part of budgeting and forecasting?
- Do we have a documented and easily accessible IRP (Incident Response Plan)?
- Do we have formalised incident response teams? CICT / CIRT (Critical Incident Coordinating Team / Cyber Incident Response Team)
- Is our insurance up-to-date?
- Do we have the required policies and procedures documented, communicated and readily accessible?
- Who is responsible for alerting the Principal to a suspected cyber-attack?
- Do our staff undertake regular cyber security training?
- Do our staff know who to contact if they receive suspicious emails?
- Who will be the contact person to deal with external communications, including to parent/student community, media?
- How do we ensure our cyber security with casual staff, contractors, volunteers who require access to school systems?

Exercise in a Box – Table Top Exercises

<https://www.cyber.gov.au/resources-business-and-government/exercise-in-a-box>



Third Party Software Compromise - Participant Briefing

1.1 Scenario overview

This scenario investigates the risks around using third party software and the controls your organisation has in place to mitigate the impact of a third party supplier being compromised. In particular, the exercise looks at password controls, the ability to detect and respond to a compromise and the ability to cope with disruption to key services.

1.2 Objectives

The objective of this exercise is to explore how your organisation would respond to the compromise of a third party supplier. Discussions will cover the detection and response capability of your organisation, processes for dealing with service disruption, and policies in place to prevent stolen credentials being used to compromise network services. The outcomes of discussions around the events in this scenario can be an opportunity to identify areas for improvement. This exercise has the following aims:

- Understand risk associated with third party software
- Identify areas for improvement in password and authentication policy
- Clarify which network services are publically exposed
- Understand detection and response capability of organisation
- Determine processes for dealing with key services being unavailable
- Build trusted relationships and develop shared understanding between key stakeholders
- Prepare and train key staff to think about what risks they are exposed to
- Operate in a no fault environment to check and test cyber security defences and capabilities

1.3 Guidance for participants

This scenario is intended to help you understand how your organisation currently manages the risk of third party software, password policies and detection and response capabilities. Each part of this scenario is based on a realistic attack, in which your organisation's network is compromised using credentials stolen from a third party supplier. Understanding the risks associated with third party software is important. Having a strong detection and response capability, along with a password policy that encourages the



Third Party Software Compromise – Facilitator Prompts

This document should be used alongside the scenario events (injects) and discussion points which are delivered in the service. The additional questions below are to help get conversations started or explore some areas of interest in more detail. This should be reviewed before the scenario is run, and referred to throughout.

Section 1: Third Party Supplier Compromise

Facilitator guidance

The scenario starts with an online third party e-commerce tool that the organisation uses being compromised. If an e-commerce tool does not feel relevant to your organisation, the use of another online tool or cloud service that feels more appropriate can be substituted. The questions posed will still be relevant.

The compromised company has had all of their username and passwords stolen. This section aims to determine if the user has considered the risk of using third party software and if there are any policies in place to deal with a compromise.

Facilitator Prompts

1. Have you considered the benefits and risks of using third party service suppliers?
 - What are the risks to your organisation?
 - How much of your sensitive data do they have access to?
2. What processes do you have in place to respond to the compromise of a third party supplier you use?
 - What is your immediate response? Can the compromised accounts still be accessed? Should access to services be revoked?
 - Do you have a process to determine which of your services are most at risk following the compromise of a given third party? Will passwords be changed? Who will do this?
3. How can you determine which users' credentials have been stolen?
 - Do you keep accurate records of users in your organisation who have access to third party business services? Do you have a procedure to investigate where accounts on these services have been compromised?



Scribe sheet – Scenario:

Exercise Start Date: _____ Time: _____ Attendees: _____

Name: _____	Role: _____
Name: _____	Role: _____
Name: _____	Role: _____
Name: _____	Role: _____
Name: _____	Role: _____

2 | Threatened leak of sensitive data - Scribe sheet

Inject 1:

We have a number of exercises to choose from that include:



Discussion based exercises:

- A ransomware attack delivered by phishing email
- Mobile phone theft and response
- Being attacked from an unknown Wi-Fi network
- Insider threat leading to a data breach
- Third party software compromise
- Bring Your Own Device (BYOD)
- Threatened leak of sensitive data
- Supply chain risks
- Home and remote working
- Managing a vulnerability disclosure
- Supply chain software
- Supply chain ransomware attack



Micro-exercises:

- Responding to ransomware attacks
- Identifying and reporting a suspected phishing email
- Using passwords
- Connecting securely
- Securing cloud productivity suites
- Securing video conferencing services

Simulation exercises:

- A simulation exercise mimicking a cyber threat present on your organisation's network

Key Takeaways

- Operational Continuity:
 - Disaster Recovery
 - Business Continuity Plan
- Incident Response Team Model:
 - CIRT – Critical Incident Response Team
 - CIST – Critical Incident Coordinating Team
 - Responsibility: Notification, reporting and communication strategies
- Ongoing refinement, training, and reassessment

Reporting to the Board



Board Reporting Challenges

- Too much information or too little information
- Clear non-technical communication
- Articulating IT risks, vulnerabilities, and potential impacts
- Aligning IT strategy with organisational goals
- Managing cyber security and data privacy concerns

Board Reporting

Cyber Security actions based – November 2021

- Reporting was brief and dot points sufficed.
- Cyber Security tasks were undertaken as-and-when necessary.

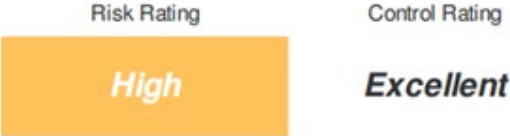
- Cyber Security continues to be focused on across multiple projects, including:
 - The implementation of the cloud immutable backup systems has been finalised and the daily tape backups have been retired. Weekly tape backups will continue and are held on site.
 - An external penetration tester has been selected and the testing is scheduled to run from 19 Oct - 1 Nov
 - TechServe has run a phishing campaign, which involves sending fake emails to staff, and are currently collating the results. The team received about 40 tickets and 15 walk-up queries seeking advice about the email, indicating a high level of awareness among staff.
 - Audits of passwords, licensing, and security best practice continue as part of the annual Security Uplift.

Board Reporting for the Future

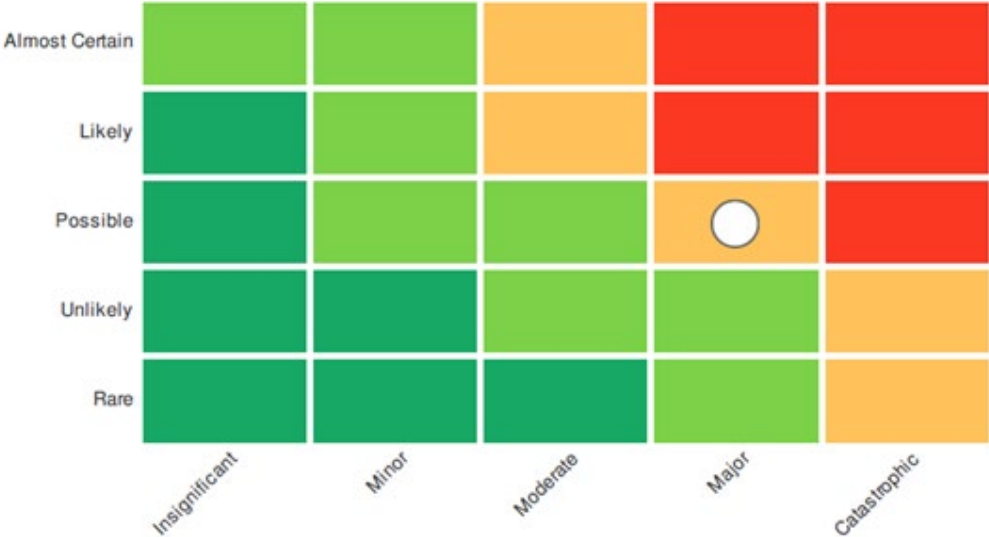
- Framework based reporting
 - Essential Eight
 - NIST
- Cyber risk register

Cyber Risk Register Reporting

Likelihood vs Consequence = Risk Rating



Risk Rating
(Likelihood vs Consequence)



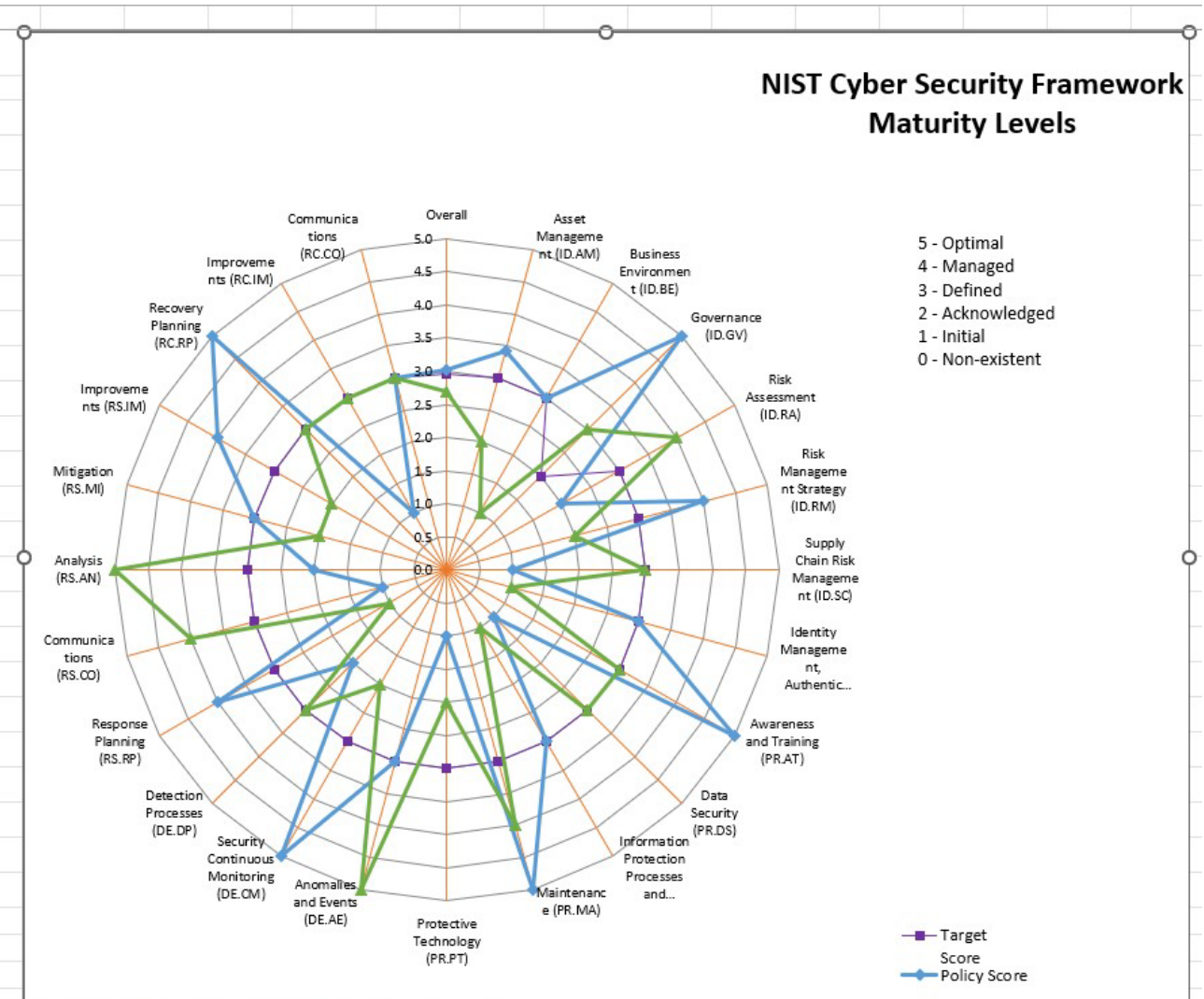
Cyber Risk Register Reporting

Risk	Cause	Likelihood	Consequence	Risk Rating	Mitigation Plan
Password compromise	Phishing email	Likely	Compromised account is lost to intruder (Moderate)	High	Implement staff training in high-risk emails
Data leak	Mixing personal and professional use of work device	Possible	Unauthorised access to data (Moderate)	Moderate	Implement strict policies and guidelines regarding personal use or business devices
Mobile data	Digital media isn't backed up	Likely	Loss of business assets (Minor)	Moderate	Compile a register of key assets and ensure routine back-up
Cloud vendor network compromise	Vendor has failed to use encrypted cloud communication	Rare	Information and assets transferred by vendor is compromised (Catastrophic)	High	Ensure vendor terms and conditions are reviewed to ensure encryption and best practice.

NIST Cyber Security Framework Maturity Level

Radar Chart

NIST CSF 1.1 Categories		2022		
		Target Score	Policy Score	Practice Score
Overall		3.00	3.02	2.70
IDENTIFY (ID)	Asset Management (ID.AM)	3.00	3.42	2.00
	Business Environment (ID.BE)	3.00	3.00	1.00
	Governance (ID.GV)	3.00	5.00	3.00
	Risk Assessment (ID.RA)	3.00	2.00	4.00
	Risk Management Strategy (ID.RM)	3.00	4.00	2.00
	Supply Chain Risk Management (ID.SC)	3.00	1.00	3.00
PROTECT (PR)	Identity Management, Authentication and Access Control (ID.AM)	3.00	3.00	1.00
	Awareness and Training (PR.AT)	3.00	5.00	3.00
	Data Security (PR.DS)	3.00	1.00	3.00
	Information Protection Processes and Procedures (PR. DS)	3.00	3.00	1.00
	Maintenance (PR.MA)	3.00	5.00	4.00
DETECT (DE)	Protective Technology (PR.PT)	3.00	1.00	2.00
	Anomalies and Events (DE.AE)	3.00	3.00	5.00
	Security Continuous Monitoring (DE.CM)	3.00	5.00	2.00
RESPOND (RS)	Detection Processes (DE.DP)	3.00	2.00	3.00
	Response Planning (RS.RP)	3.00	4.00	1.00
	Communications (RS.CO)	3.00	1.00	4.00
	Analysis (RS.AN)	3.00	2.00	5.00
	Mitigation (RS.MI)	3.00	3.00	2.00
RECOVER (RC)	Improvements (RS.IM)	3.00	4.00	2.00
	Recovery Planning (RC.RP)	3.00	5.00	3.00
	Improvements (RC.IM)	3.00	1.00	3.00
	Communications (RC.CO)	3.00	3.00	3.00



Conclusion and *next steps*



Conclusion and next steps

- Recap of key takeaways
- Importance of ongoing Cyber Security vigilance
- Encouraging collaboration and sharing best practices
- Next steps for improving Cyber Security preparedness

Today's resources
and further information



Contact Details
*Paul Carnemolla &
Solomon James*



Paul Carnemolla



Solomon James

