CHRISTIAN
EDUCATION NATIONAL

Christian Schools ICT Network Professional Development Day

Thursday 10th October 2024

CHRISTIAN
EDUCATION NATIONAL

Christian Schools ICT Network Professional Development Day

Cyber Security

At Covenant

Presented by:
Paul Carnemolla, Mitch Green and the TechServe team

October 2024

Today's resources
and further information

Overview

- Cyber Security Threats and 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).

Sources: Exploitation Accounts For 29% of Education Sector Attacks - Infosecurity Magazine (infosecurity-magazine.com), Ransomware attacks on schools and colleges around the world (comparitech.com)

Education sector graphic

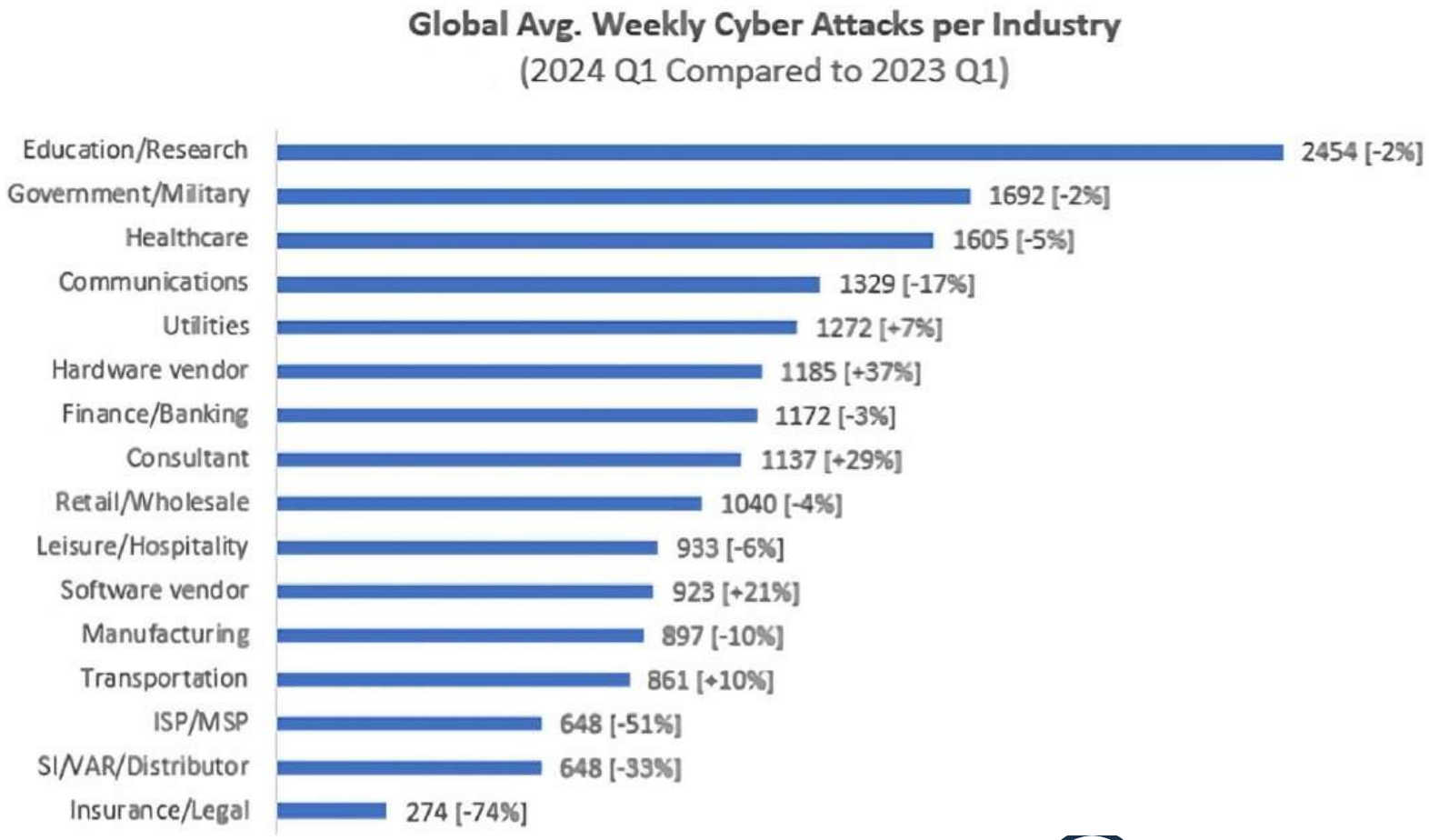


Image source: Check Point Software Technologies

Covenant Christian School
All knowledge through Christ

new era. TECHNOLOGY

Importance of Cyber Security

in educational institutions

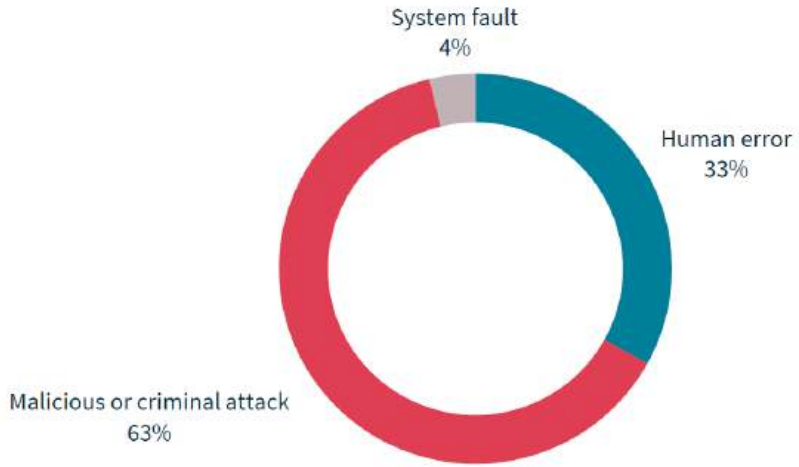
1. Protect Sensitive Data
2. Preserving Academic Integrity
3. Safeguarding Intellectual Property
4. Maintaining Operational Continuity
5. Protecting Financial Resources
6. Fostering Trust and Reputation
7. Promoting Digital Citizenship & Online Safety
8. Compliance with Regulations
9. Mitigating Cyber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

Covenant Christian School
All knowledge through Christ

new era. TECHNOLOGY

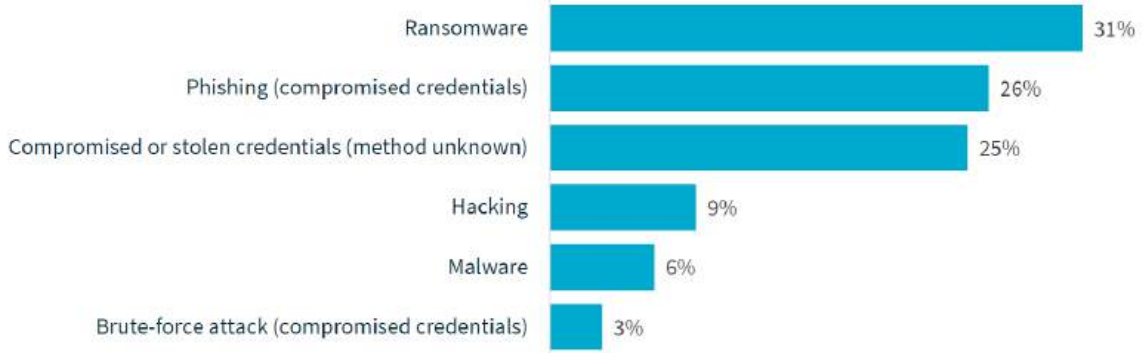
Sources of Data Breaches

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%

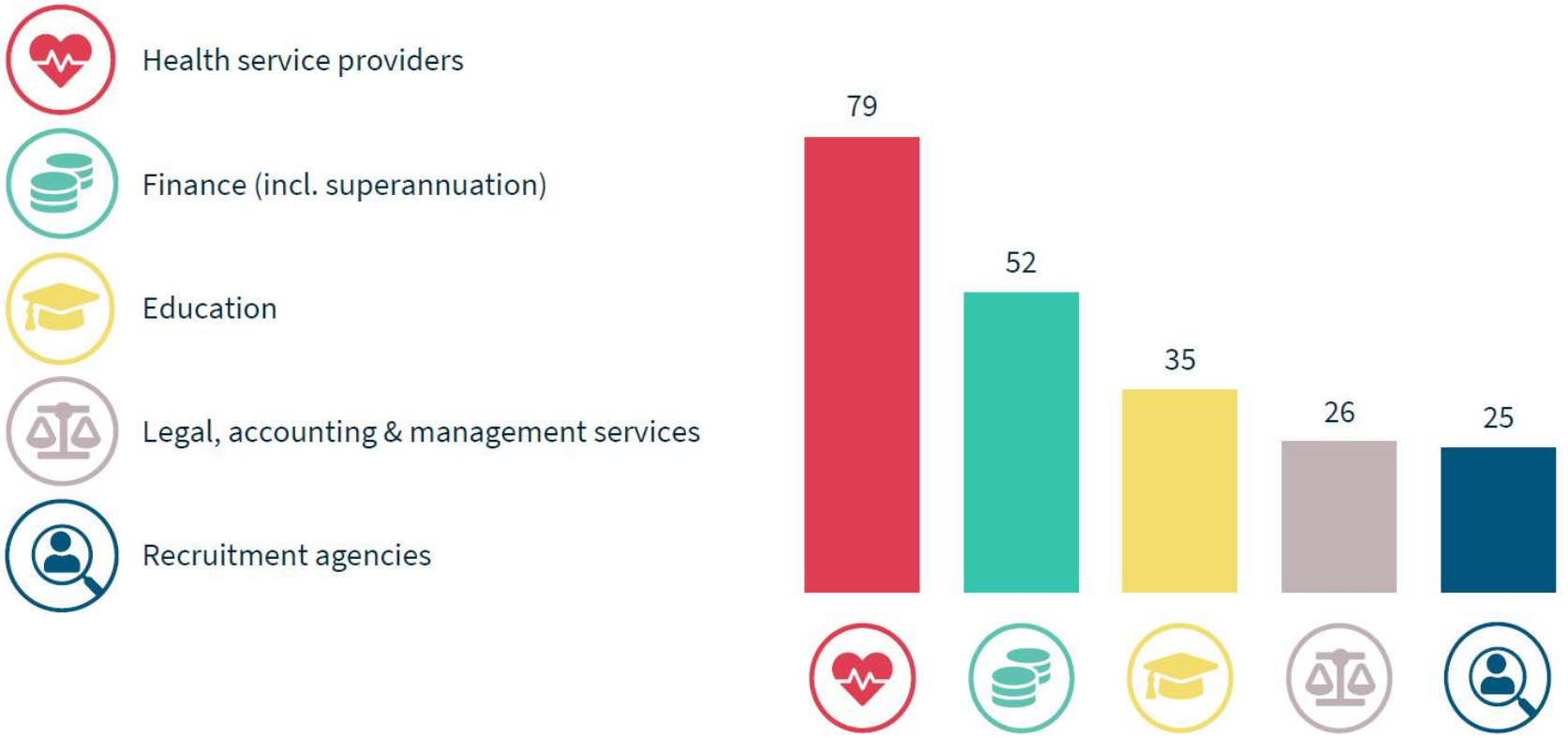
Source: [Notifiable Data Breaches Report: January to June 2022 | OAIC]

Covenant Christian School
All knowledge through Christ

new era. TECHNOLOGY

Notifiable Data Breach snapshot

Top 5 sectors to notify data breaches

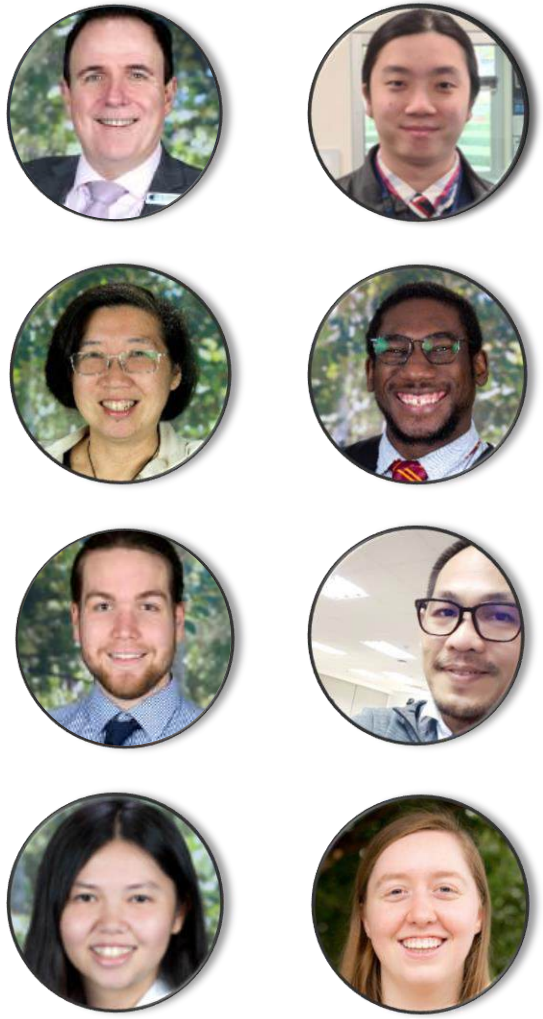


Source: [Notifiable Data Breaches Report: January to June 2022 | OAIC]

Project Timeline

The Covenant Story

Covenant ICT Team



	Role	Org	FTE
Paul Carnemolla	Director of ICT	New Era	0.5
Henry Woo	ICT Support	New Era	1
Justina Lowe	ICT Support	Covenant	0.8
Leon Dhemba	ICT Support	Covenant	1
Nicholas Sargent	ICT/AV 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	ICT/AV Support	Covenant	0.75

Covenant Christian School
All knowledge through Christ

new era. TECHNOLOGY

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

INCEPTION

2021 • Term 4

Penetration Test

- Internal
- External
- Wi-Fi

Disaster Recovery Planning

2021-2022 School Holidays

1st Internal Pen. Remediation

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

REFINING

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

Penetration Testing

Enhancing Cyber Security Through Penetration Testing

- School underwent a comprehensive Penetration Testing in Term 4 2021, covering:
  - Internal Penetration tests
  - External Penetration tests
  - Wi-Fi Penetration tests

Finding ID	Risk	Title	Remediation Timeframe	Status
INPT-1	Extreme	Account and privilege management is not adequate.	3-6 Months	Open
INPT-2	Extreme	Password hygiene is not adequate.	1-2 Months	Open
ENPT-1	High	Multi-factor authentication is not required for external access to Virtual Private Network.	1-2 Months	Open
ENPT-2	High	Users are susceptible to email-based phishing attacks.	Ongoing	Open
ENPT-3	High	Website is vulnerable to web cache poisoning.	N/A	Closed
INPT-3	High	Systems are vulnerable to null session attack.	1 Month	Open
INPT-4	High	Students have local administrative privileges and wide-reaching network access on	Covenant to confirm	Open
INPT-5	High	Domain is susceptible to Kerberoasting attacks.	1-2 Months	Open
WNPT-1	High	Wireless LAN is not logically segmented from wired LAN.	3 Months	Open
WNPT-2	High	No Wireless Intrusion Prevention System (WIPS) implemented.	1 Month	Open
ENPT-4	Moderate	DNS server vulnerable to zone transfer.	N/A	Closed
ENPT-5	Moderate	Issues with certificates used to validate host identity.	3 Months	Open
ENPT-6	Moderate	DMARC has not been implemented.	1 Month	Open
ENPT-7	Moderate	DKIM has not been implemented on primary mail domain.	1 Month	Open
INPT-6	Moderate	Credentials are cached on workstations that are constantly connected to Domain Control	1-2 Months	Open
INPT-7	Moderate	KRBTGT account password has not been changed for an extensive period of time.	2 Weeks	Open
INPT-8	Moderate	Directory Replication allowed to hosts other than Domain Controllers.	1-2 Months	Open
INPT-9	Moderate	Domain Administrators are not restricted to Domain Controllers.	2 Weeks	Open
INPT-10	Moderate	Administrators are assigned debug privileges.	2 Weeks	Open
INPT-11	Moderate	VMware vCenter missing critical security patches.	2 Weeks	Open
INPT-12	Moderate	Issues with certificates used to validate host identity.	1-2 Months	Open
INPT-13	Moderate	802.1X authentication not implemented on wired network.	6-12 Months	Open

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

Using Microsoft to reduce Security Risks

Multi-Factor Authentication – a multi-step account login process that requires users to enter more information than just a password.

Current : All staff are required to set up Multi-Factor Authentication (MFA) using their mobile phones or an additional device like an ipad. While onsite using a school device, MFA is not required.

Students do not normally have MFA enforced.

MFA for students would be preferable but students carrying mobile phones creates other risks.

Using Microsoft to reduce Security Risks

Conditional Access

Current : access is limited to Australian IP address via Geoblocking (restricting access to Internet content based upon the user's geographical location). This applies to both staff and students.

If Overseas access is required, an approval process has to be completed, then access to specified countries is allowed with MFA.

Using Microsoft to reduce Security Risks

Intune / Endpoint Manager

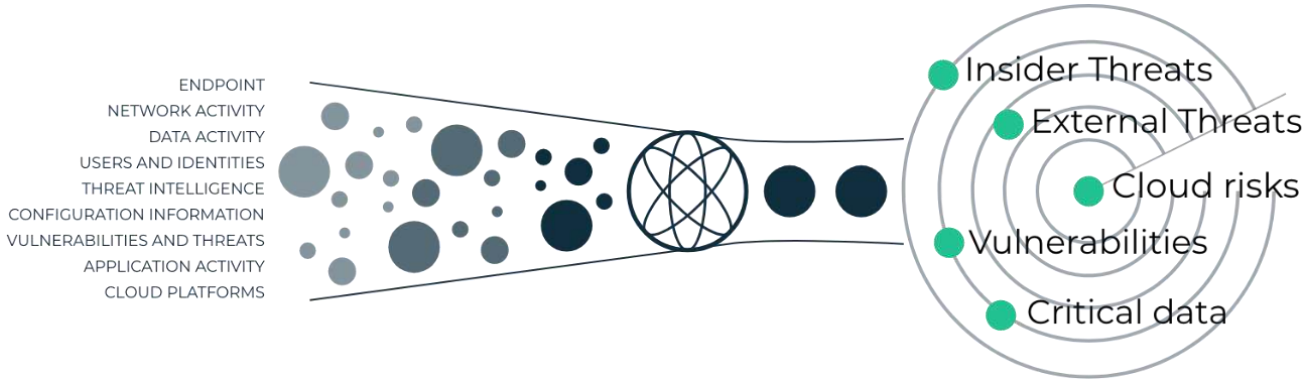
Current : Restrictions on programs that can be installed on school owned devices. Computers are set up with a predetermined set of programs. Only system administrators can install additional programs.
Requests for additional software goes through an approval process, then pushed out via Intune.
Staff can install apps from the Microsoft Store, but this is not available for students.

Desired : Restrict all installs of software except when managed through Intune.

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



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)

Covenant Christian School
All knowledge through Christ

new era. TECHNOLOGY

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

Covenant Christian School
All knowledge through Christ

new era. TECHNOLOGY

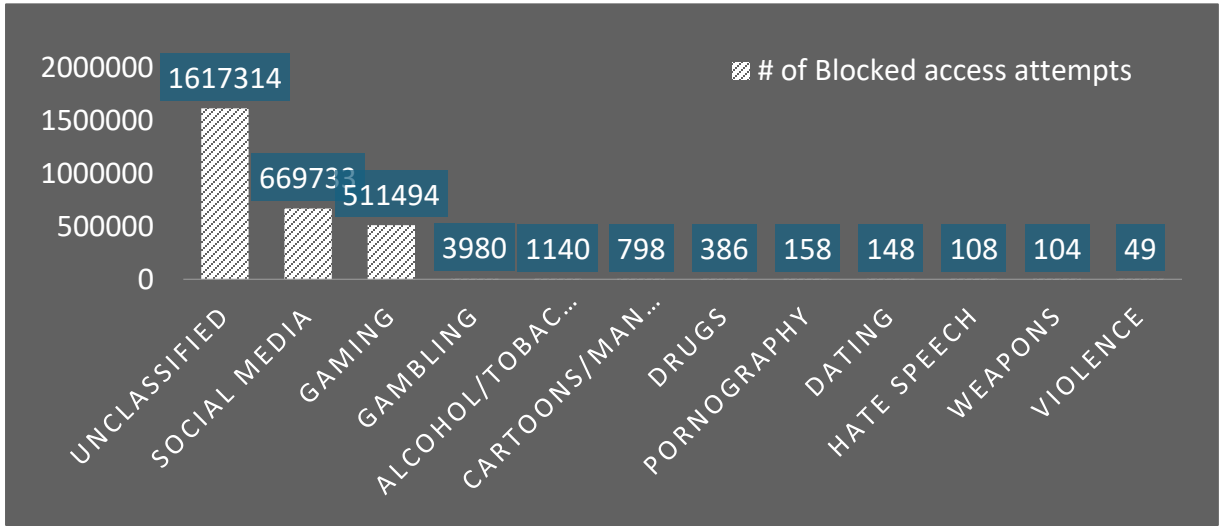
Linewize

What is it?

- Linewize is a suite of device management and security tools.
- Covenant uses Linewize School Manager, in conjunction with Linewize Connect.
- The Linewize suite integrates with Qustodio, granting parents a degree of control over School Managed devices outside of school hours.

Date and Time	Username	Blocked	Website	Website Path
2024-07-29 09:52:24		No	www.google...	/complete/search?q=temu&cp=0&client=mobile-gws-wiz-on-focus-serp&...
2024-07-29 09:48:25		No	www.google...	/complete/search?q=euro%20to%20inr&cp=0&client=mobile-gws-wiz-on...
2024-07-29 09:48:24		No	www.google...	/search?q=euro+to+inr&rlz=1C9BKJA_enAU1067AU1067&oq=eu&gs_lc...
2024-07-29 09:48:12		No	www.google...	/complete/search?q=smart%20watch&cp=0&client=mobile-gws-wiz-on-f...
2024-07-29 09:47:34		No	www.google...	/complete/search?q=smart%20watch&cp=0&client=mobile-gws-wiz-on-f...
2024-07-29 09:47:33		No	www.google...	/search?q=smart+watch&safe=active&hl=en-GB&rlz=1C9BKJA_enAU10...
2024-07-29 09:47:32		No	www.google...	/complete/search?q=g-shocsmart%20watch&cp=6&client=mobile-gws-w...
2024-07-29 09:47:32		No	www.google...	/complete/search?q=gsmart%20watch&cp=1&client=mobile-gws-wiz-ser...
2024-07-29 09:47:32		No	www.google...	/complete/search?q=g-smart%20watch&cp=2&client=mobile-gws-wiz-se...
2024-07-29 09:47:32		No	www.google...	/complete/search?q=g-shosmart%20watch&cp=5&client=mobile-gws-wi...
2024-07-29 09:47:32		No	www.google...	/complete/search?q=g-ssmart%20watch&cp=3&client=mobile-gws-wiz-s...
2024-07-29 09:47:32		No	www.google...	/complete/search?q=g-shsmart%20watch&cp=4&client=mobile-gws-wiz-...
2024-07-29 09:47:32		No	www.google...	/complete/search?q=smart%20watch&cp=0&client=mobile-gws-wiz-serp...
2024-07-29 09:47:31		No	www.google...	/complete/search?q=g-shocksmart%20watch&cp=7&client=mobile-gws-...
2024-07-29 09:44:04		No	www.google...	/complete/search?q=g-shock%20smart%20watch&cp=0&client=mobile-...
2024-07-29 09:44:02		No	www.google...	/search?q=g-shock+smart+watch&safe=active&sca_esv=4c9d44f7b0b8...
2024-07-29 09:43:52		No	www.google...	/complete/search?q=g%20shock%20watches&cp=0&client=mobile-gws-...
2024-07-29 09:43:47		No	www.google...	/search?q=g+shock+watches&rlz=1C9BKJA_enAU1067AU1067&oq=g+...
2024-07-29 08:30:44		No	www.bing.c...	/search?q=whats+the+area+of+a+rectangle+measuring+13+in&qs=ds&f...

Student network traffic as seen in School Manager



Summary of access attempts blocked by Linewize (01/06/24-30/06/24)

Covenant Christian School
All knowledge through Christ

new era. TECHNOLOGY

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.

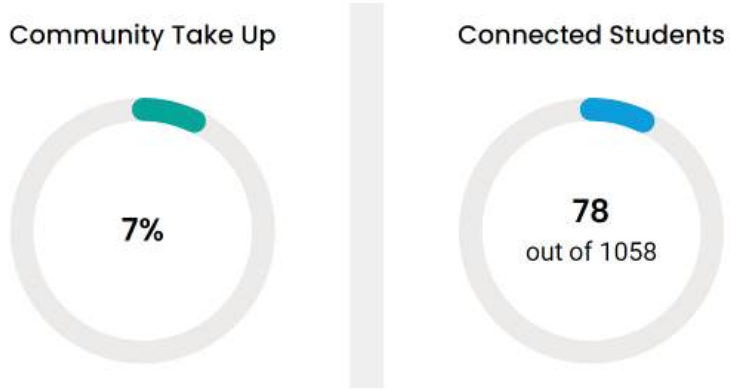


Diagram of active parent integrations

Covenant Christian School
All knowledge through Christ

new era. TECHNOLOGY

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.

Linewize

Report

Hi there,

This is the weekly student wellbeing report for device

covenantcs.nsw.linewize

July 8, 2024 - July 14, 2024

Total users with red flag indicators : 6

Username	Red Flags	Hits
[redacted]	VPN	19
[redacted]	Adult Content	6
[redacted]	Adult Content	5
[redacted]	Adult Content	1
	VPN	1
[redacted]	VPN	1

Top Suicidal Red Flag Users: 0

No Users At Risk

Top Adult Content Users: 3

Username	Hits
[redacted]	6
[redacted]	5
[redacted]	1

Top VPN Users: 4

Username	Hits
[redacted]	19
[redacted]	1

Top applications and websites	Data transferred

Applications and websites visited : 440

Top applications and websites	Data transferred
YouTube	23.3 GB
Microsoft	9.0 GB
Office 365	2.1 GB
Scratch MIT	1.0 GB
Microsoft Teams	585.9 MB
Linewize	487.5 MB
Bing	433.0 MB
Windows Updates	348.2 MB
Outlook	155.5 MB
Google Play	151.1 MB

Requests filtered : 936

Top filtered users	Hits
[redacted]	302
[redacted]	88
[redacted]	83
[redacted]	62
[redacted]	57
[redacted]	55
[redacted]	53
[redacted]	46

Top Filtered Websites	Hits
facebook.net	57
githubusercontent.com	35
gamepass.com	28
linkedin.com	23
got-to-be.net	21
clarity.ms	14
dotmetrics.net	13
pinimg.com	13
disqus.com	12
get-my-push.xyz	12

Thank you,
Linewize Team

Covenant Christian School
All knowledge through Christ

new era. TECHNOLOGY

Other Key Projects

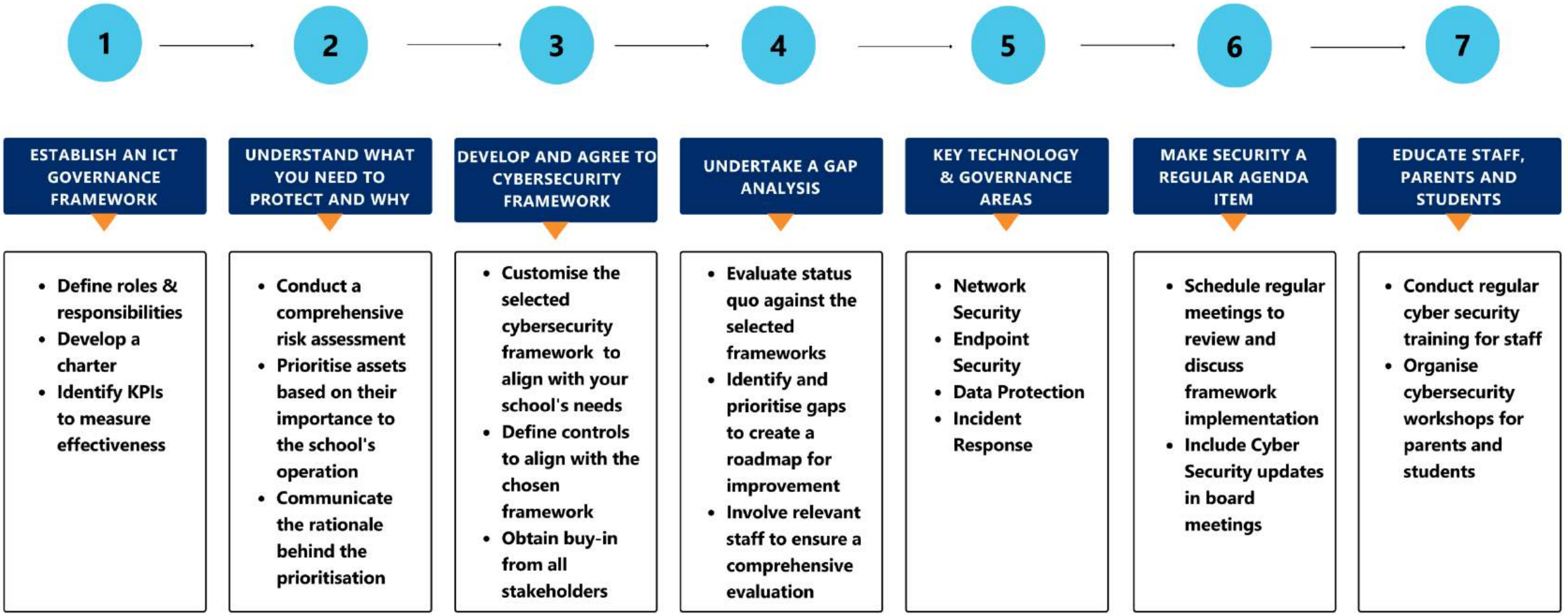
- KnowBe4 Security Awareness Training and regular Phishing campaigns
- Data Classification
- Security Improvements:
  - Enhanced network segregation
  - 802.1x network authentication for wired network
- Security Questionnaire for Third-Party Vendors
- Cyber Security Incidence Response Plan
- Microsoft 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

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

1. Define the Purpose and Scope
2. Identify Stakeholders
3. Establish IT Steering Committee
4. Define Decision-Making Processes
5. Establish Governance Policies & Procedures
6. Implement Monitoring & Reporting Mechanisms
7. Review & Continuous Improvement

2 – What to Protect and Why?

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

Data and Information → **IT Infrastructure** → **Application and Software** → **Physical Assets** → **Regulatory Compliance**

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

Covenant Christian School
All knowledge through Christ

new era. TECHNOLOGY

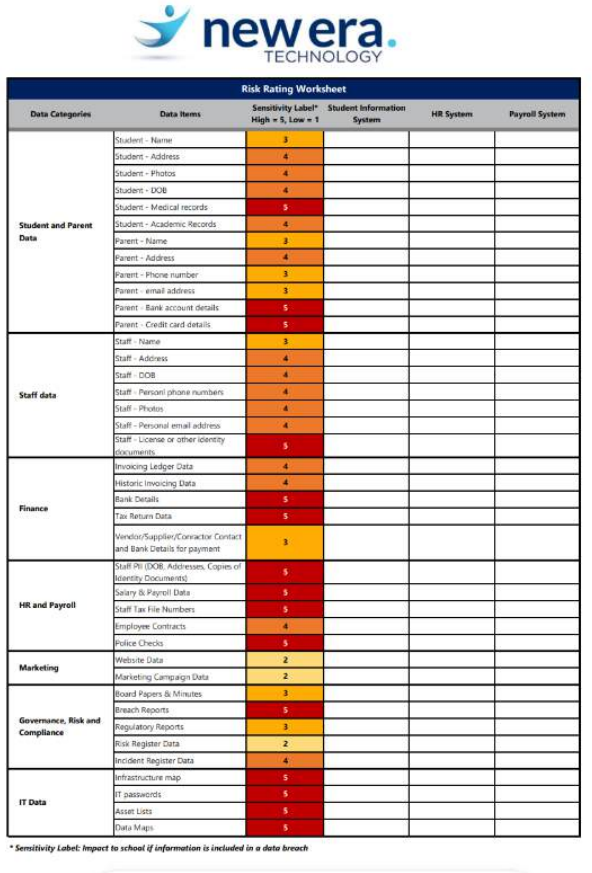
Cyber Risk Assessment

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 - Personl phone numbers	4
	Staff - Photos	4
	Staff - Personal email address	4
	Staff - License or other	5

Data Classification Activity



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			
	Parent - Bank account details	5			
	Parent - Credit card details	5			
Staff data	Staff - Name	3			
	Staff - Address	4			
	Staff - DOB	4			
	Staff - Personl phone numbers	4			
	Staff - Photos	4			
	Staff - Personal email address	4			
	Staff - License or other identity documents	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 PII (DOB, Addresses, Copies of Identity Documents)	5			
	Salary & Payroll Data	5			
	Staff Tax File Numbers	5			
	Employee Contracts	4			
	Police Checks	5			
Marketing	Website Data	2			
	Marketing Campaign Data	2			
Governance, Risk and Compliance	Board Papers & Minutes	3			
	Breach Reports	5			
	Regulatory Reports	3			
	Risk Register Data	2			
	Incident Register Data	4			
IT Data	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

Or go to this link and click

"View Data Classification Exercise":

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

Covenant Christian School
All knowledge through Christ

new era. TECHNOLOGY

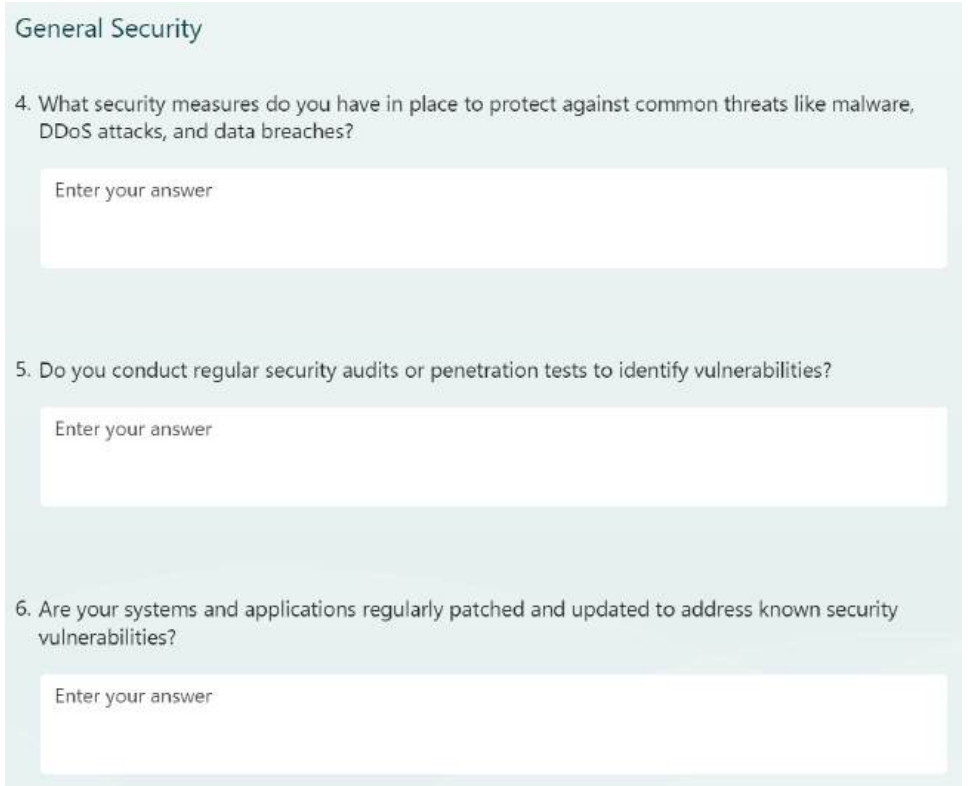
Cyber Risk Assessment

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":

Covenant Christian School
All knowledge through Christ

new era. TECHNOLOGY

3 – Develop and Agree to a Cyber Security Framework

Cyber Security Frameworks

Essential 8 Maturity Model Australian Cyber Security Centre (ACSC)

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

NIST Cybersecurity Framework

IDENTIFY	PROTECT	DETECT	RESPOND	RECOVER
Asset Management	Access Control	Anomalies and Events	Response Planning	Recovery Planning
Business Environment	Awareness and Training	Security Continuous Monitoring	Communications	Improvements
Governance	Data Security	Detection Processes	Governance	Communications
Risk Assessment	Info Protection, Processes and Procedures		Analysis	
Risk Management Strategy	Maintenance		Mitigations	
	Protective Technology		Improvements	

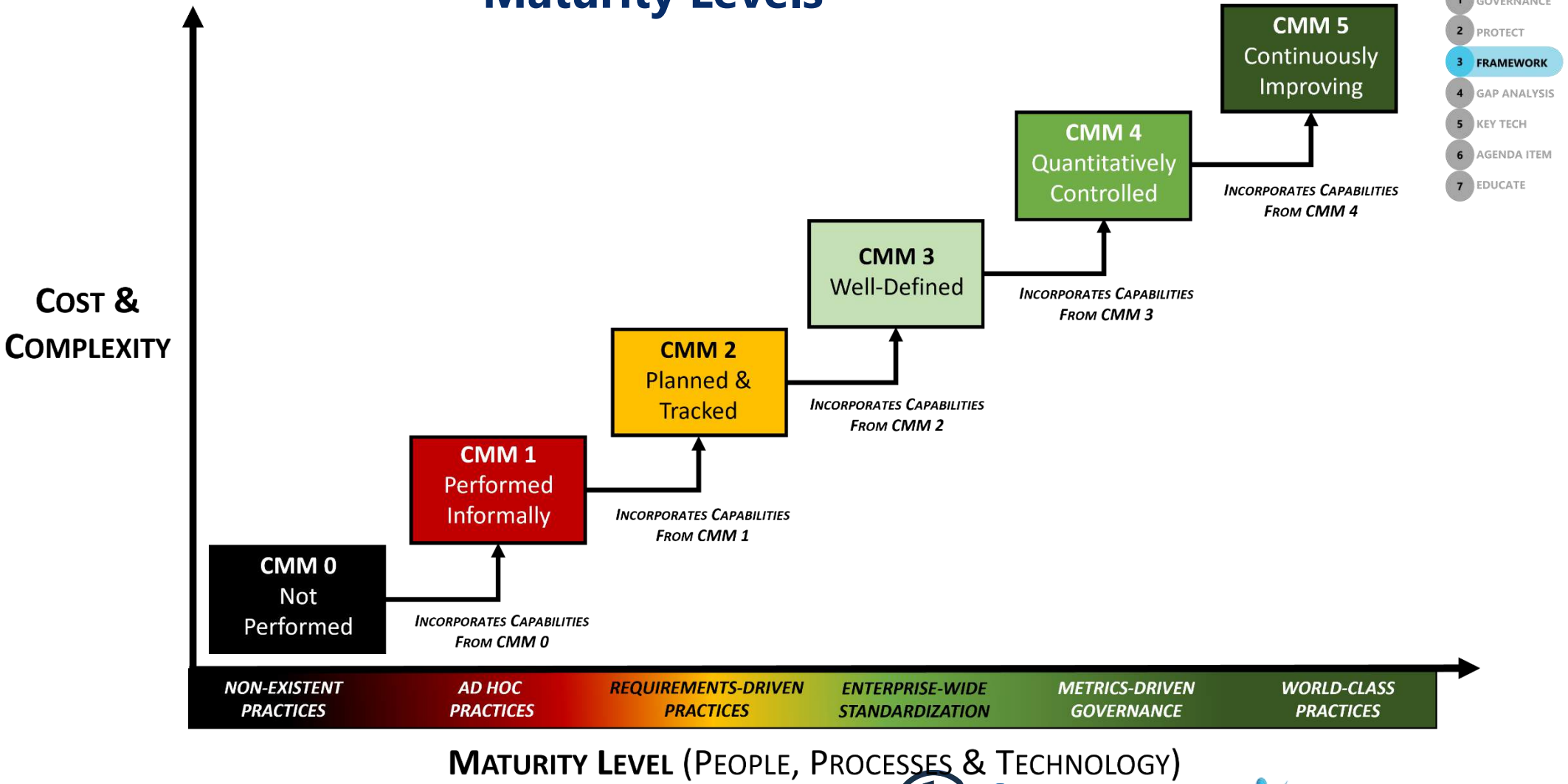
- Made up of 5 core functions.
- Each function is defined.
- Within each function is a set of assessable areas

Covenant Christian School
All knowledge through Christ

newera. TECHNOLOGY

NIST Cybersecurity Framework

Maturity Levels



Covenant Christian School
All knowledge through Christ

new era. TECHNOLOGY

Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

new era. TECHNOLOGY

The Essential 8
A Comprehensive Overview

Mitch Green

October 10, 2024

Introductions

New Era Technology

Mitch Green – Director of Solutions

10 years with New Era Technology

Covenant Christian School
All knowledge through Christ

new era. TECHNOLOGY

Mitch Green

Director of Solutions

TPG Telecom – Network operations

AGL Energy – Network and Security

Countrytell Community Broadband – Network Architect

New Era Technology – Specialist Engineering Lead

New Era Technology – National Infrastructure Manager

New Era Technology – Director of Solutions

B. IT - Network Engineering

Grad Cert – Business Analytics

RMIT – Cyber Security Strategy and Risk

Cisco – Network Security

Cisco – Enterprise Infrastructure

APAC Cyber Security Strategy

Our Approach

Support customers on their cybersecurity journey – wherever they may be today

Support the broad range of **existing security solutions** in place across APAC

Provide competitive and **integrated solutions**

Utilise frameworks such as the **Essential 8** to educate customers about security

Adaptable to meet the **needs** of a wide range of customer types and sizes

Provide a **common direction** for our region moving forward

APAC Cyber Security Strategy

What do our customers require?

Essential

- **Tactical conversation** around security
- Education on cyber security fundamentals
- Clarity and guidance on Essential 8 maturity
- Practical measures to improve cyber security
- Build upon existing New Era managed services

Strategic

- **Strategic conversation** around security
- Governance, risk and compliance
- Alignment with security frameworks – NIST, ISO etc
- Policy development and implementation
- Reviewing and securing business processes
- Proactive monitoring and cyber response services
- Trusted security advisor – ongoing engagement

APAC Cyber Security Strategy

Tailored delivery model for different customer types

Essential	Strategic
Locally Developed & Delivered	Locally Delivered in Partnership with SecureBlu by new era.
• Accredited Essential 8 security assessment • Product led • Pre-defined security product bundles • Readiness for Essential 8 maturity up to M1 • Sold directly by existing sales teams	• Detailed security assessment • Consulting led • Security strategy & roadmap development • Bespoke to suit complex clients & environments • Essential 8 maturity M1+ • Alignment with other frameworks re SOCI, ISO etc • Regular vCISO engagement • Presales support from SecureBlu team

What is the Essential 8?

8 practical strategies for mitigating cyber incidents

- The Australian Cyber Security Centre (ACSC) is our country's first line of defence against cybercrime and is the Australian Government's lead on national cyber security
- The ACSC and New Era recommend organisations implement The Essential 8 as a **Baseline**
- The strategy to implement the Essential 8 and to which maturity level needs to be customized to each organisations risk profile and adversaries
- New Era Technology are recommending all customers adopt the Essential 8 framework and intend on guiding and supporting our customers to reach the appropriate Maturity level

Covenant Christian School
All knowledge through Christ

new era. TECHNOLOGY

What is the Essential 8?

8 practical strategies for mitigating cyber incidents

- Developed by the Australian Signals Directorate (ASD)
- Focuses on securing Microsoft Windows environments
- Progressive maturity model: Level 0, 1, 2, 3
- Can be implemented using a range of technologies/solutions

Covenant Christian School
All knowledge through Christ

new era. TECHNOLOGY

Why is the Essential 8 important?

8 practical strategies for mitigating cyber incidents

- **A Real threat to Everyone** - All industries are being targeted
- **Cost** – Cyber Crime is costing the Australian Economy more than $1 Billion annually in direct costs
- **Reputational Damage** – trust of clients and staff

Covenant Christian School
All knowledge through Christ

new era. TECHNOLOGY

Why is the Essential 8 important?

8 practical strategies for mitigating cyber incidents

- **Insurance**

  Premiums reduced when cyber security controls are implemented

The Essential 8: Key Strategies for Cyber Security

User Application Hardening

Patching Applications

Configure Microsoft Macro Settings

Application Control

Proactively Prevent Cyber Attacks

Multi-Factor Authentication

Patch Operating Systems

Restrict Admin Privileges

Minimise the Impact of Cyber Attacks

Daily Backups

Ensure Data Recovery and System Availability

Essential 8 Mitigation Strategies

Description

Mitigation Strategy	Description
Multi-factor Authentication	Implement multi-factor authentication to enhance the security of user accounts.
Regular Backups	Regularly back up important data and verify the integrity and availability of backup copies.
Patch Applications	Regularly apply patches and updates to close security gaps in software applications.
Patch Operating Systems	Regularly apply patches and updates to secure the underlying operating systems.
Application Control	Only allow approved applications to run, preventing the execution of unauthorized or malicious software.
Configure MS Office Macros	Adjust settings to secure Microsoft Office macros, preventing malicious code execution.
User Application Hardening	Configure applications securely, manage user permissions, and apply best practices to reduce vulnerabilities.
Restrict Administrative Privileges	Implement the principle of least privilege, restricting access to critical systems and functions.

Maturity Levels

Example

Applicability & Effectiveness	Level 1	Level 2	Level 3
Application Control	✓	✓	−
Patching Applications	✓	✓	✓
Configure Microsoft Macro Settings	✓	✓	✓
User Application Hardening	✓	✓	−
Restrict Admin Privilege	✓	✗	✗
Patch Operating System	✓	✓	✓
Multi-Factor Authentication	✓	−	−
Daily Backups	✓	✓	−

ASCS Maturity Levels

Maturity Level 1	**Partially** meets the objectives of the mitigation strategy
Maturity Level 2	**Largely** meets the objectives of the mitigation strategy
Maturity Level 3	**Completely** meets the objectives of the mitigation strategy

The Essential 8: Key Strategies for Cyber Security

ACSC Maturity Levels	
Maturity Level 1	**Partially** meets the objectives of the mitigation strategy
Maturity Level 2	**Largely** meets the objectives of the mitigation strategy
Maturity Level 3	**Completely** meets the objectives of the mitigation strategy

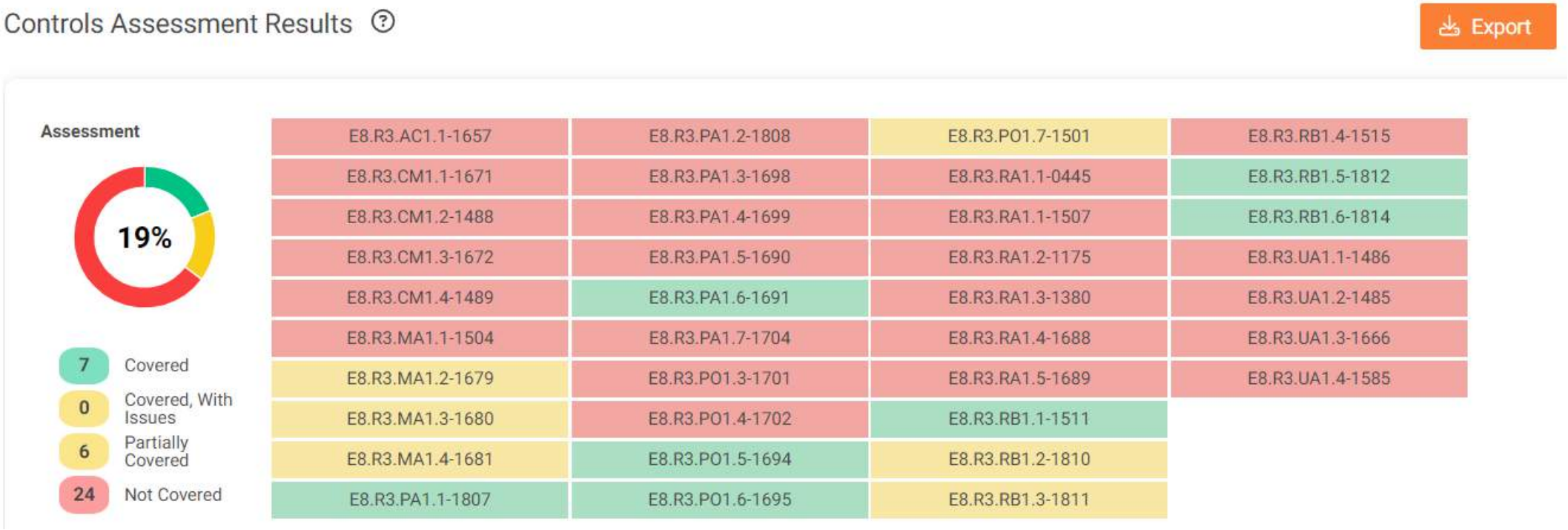
Maturity Level Examples

Mitigation Strategy	Level	Backup Frequency	Backup Storage Method	Backup Retention Period	Full Restoration Testing	Partial Restoration Testing
Daily Backups	Level 1	Monthly	Not specified	1-3 months	Not specified	Annually or more frequently
	Level 2	Weekly	Stored offline or online in a way that prevents alteration or deletion	1-3 months	At least once	Bi-annually or more frequently
	Level 3	Daily	Stored offline or online in a way that prevents alteration or deletion	3 months or greater	At least once upon setup and after any major infrastructure updates	Quarterly or more frequently

New Era Technology

Essential 8 Audit

EXAMPLE:



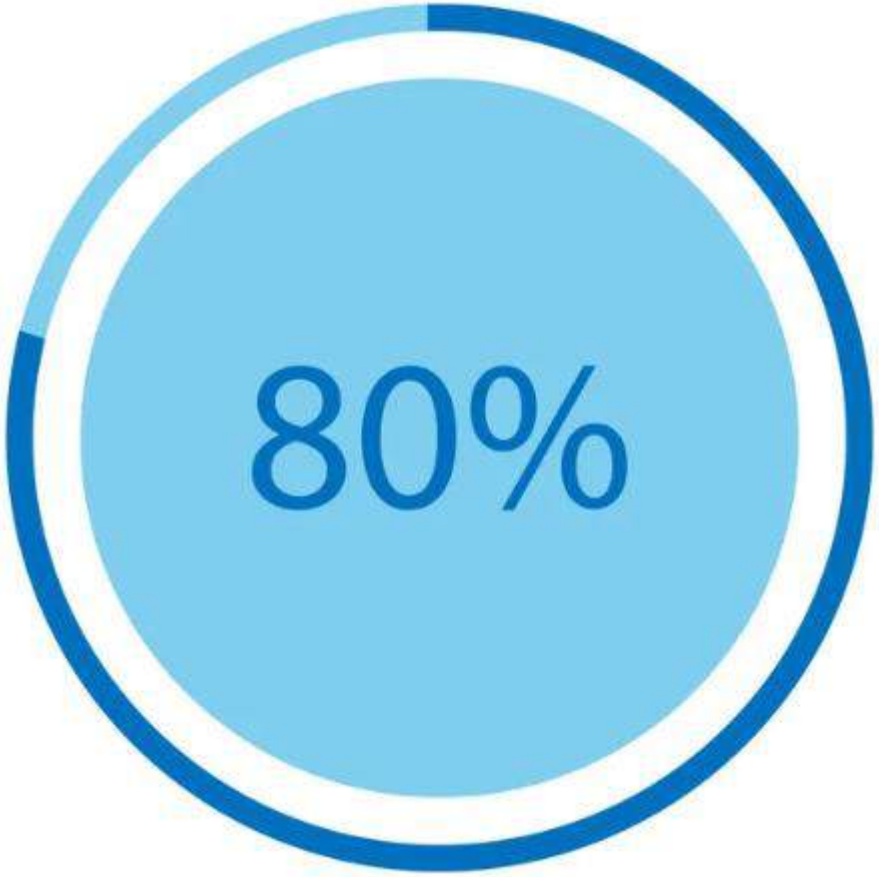
Covenant Christian School
All knowledge through Christ

new era. TECHNOLOGY

New Era Technology

Essential 8 Audit

Covenant Christian School
All knowledge through Christ



- **Restrict Office Macros** – Require use by Covenant, needs to be controlled and documented for justification
- **Removal of unsupported operating systems** – Patching and vulnerability implications
- **Web browser –** restrictions on IE and web adverts

Covenant Christian School
All knowledge through Christ

new era. TECHNOLOGY

The Essential 8: Key Strategies for Cyber Security

Recap

- The Essential 8 are guideline strategies to stop cyber-attacks. These guidelines are set by the ACSC (Australian Government)
- New Era advise that these controls are a MUST for every organization
- Cyber attacks are real and effect everyone – we all must pay attention
- New Era can assist you on your E8 journey

4 – Undertake a Gap Analysis

to assess the Cybersecurity posture of the School

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**

Covenant Christian School
All knowledge through Christ

new era. TECHNOLOGY

5 – Key Technology Areas

for a Cyber-Attack preparations

1

Network Defense

Firewalls, Endpoint Security

2

Network segregation

Segregate staff, student, guest and infrastructure networks.

3

OS + App Software Maintenance

Patch OS & apps regularly

4

Access Control

Minimise admin privileges

5

Secure Authentication

Strong Passwords,
Multi-factor Authentication

6

Continuous Assessment

Vulnerability Tests,
Penetration Tests

7

Threat Protection

Intrusion Detection,
Suspicion Monitoring

8

Centralised Monitoring & Alerts

Covenant Christian School
All knowledge through Christ

new era. TECHNOLOGY

5 – Key Technology Areas

for a Cyber-Attack preparations

9

Backup Best Practices

Regular Backups & Review
Immutable/Air-Gapped Copy

10

Recovery Testing

11

Clear Roles & Responsibilities

12

Conditional Access

13

Structured IT Governance

Policies & Procedures
Disaster Recovery & Business Continuity

Covenant Christian School
All knowledge through Christ

new era. TECHNOLOGY

6 – Make Security a Regular Agenda Item

- **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

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

Covenant Christian School
All knowledge through Christ

new era. TECHNOLOGY

7 – Educate Staff, Parents, and Students

Application: KnowBe4

What is KnowBe4?

- Training platform that helps improve an organisation's overall security culture and reduce human risk

Key Features:

- Security Awareness Training
- Simulated Phishing Attacks
- Automated Training Campaigns

KnowBe4

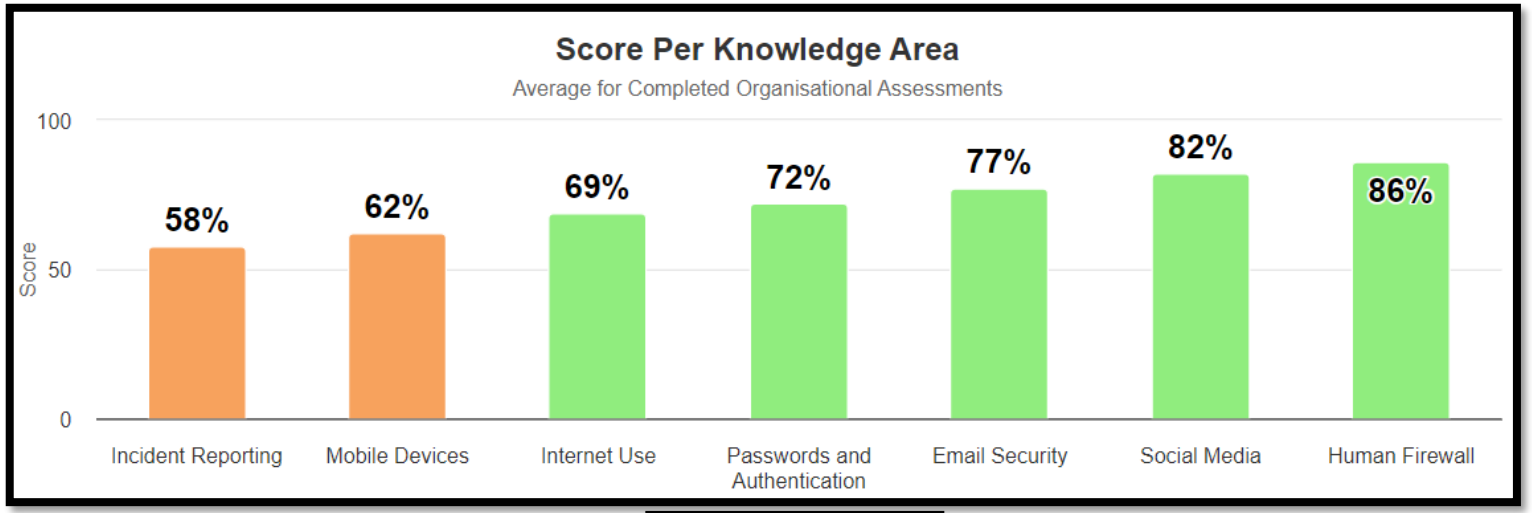
Covenant Christian School
All knowledge through Christ

new era. TECHNOLOGY

7 – Educate Staff, Parents, and Students

Why KnowBe4 ?

- Assess and measures school's awareness
- Tools to report and remove phishing emails
- Establish a baseline in order to determine training focus and measure progress:
  - Baseline phishing test.
  - **S**ecurity **A**wareness **P**roficiency **A**ssessment.

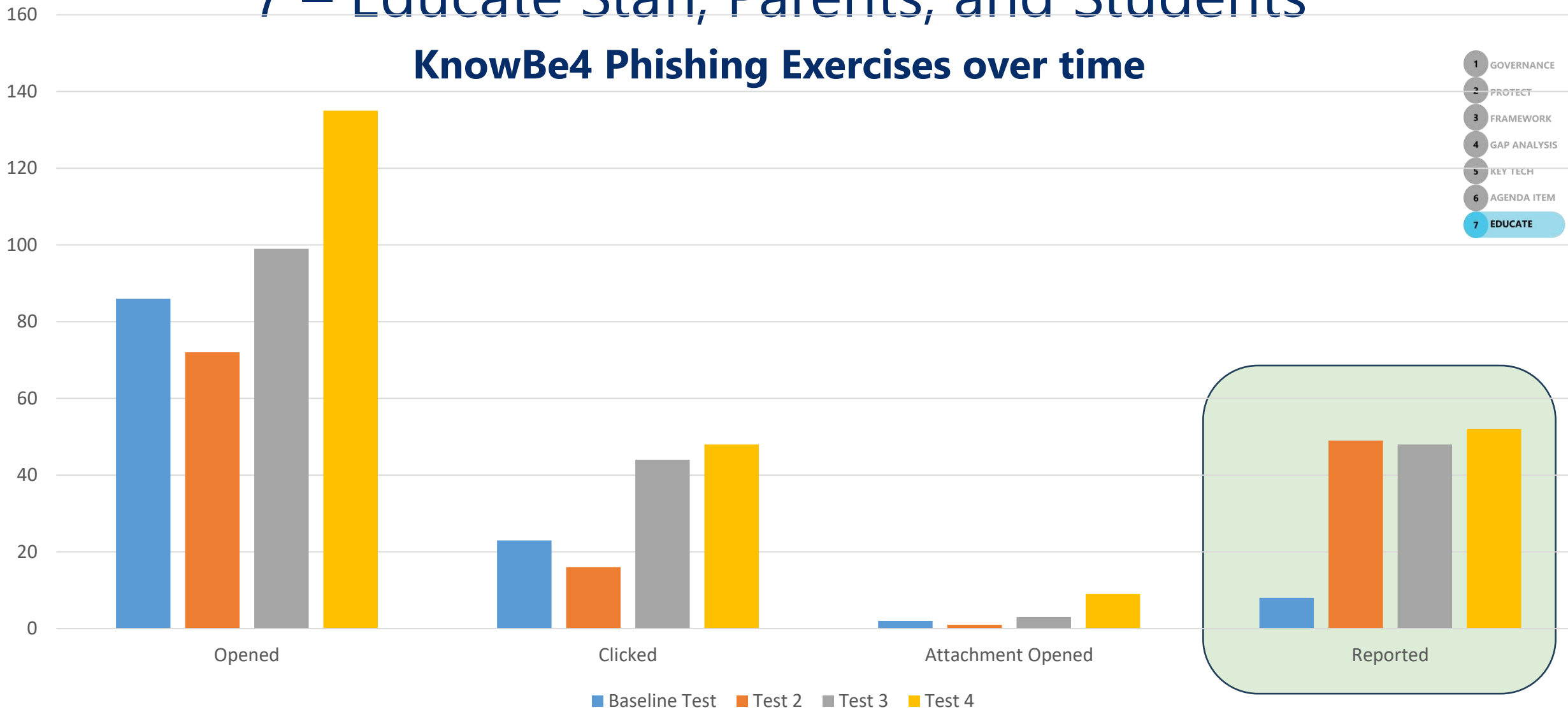


SAPA Results

Covenant Christian School
All knowledge through Christ

new era. TECHNOLOGY

7 – Educate Staff, Parents, and Students



7 – Educate Staff, Parents, and Students

KnowBe4 Phishing Campaign Reports

168 Recipients	99.4% 167 Delivered	52.1% 87 Opened	14.4% 24 Clicked	0% 0 QR Code Scanned	0% 0 Replied	1.2% 2 Attachment Opened	0% 0 Macro Enabled	0% 0 Data Entered	4.8% 8 Reported	0.6% 1 Bounced

Term 2 2023 to Term 2 2024

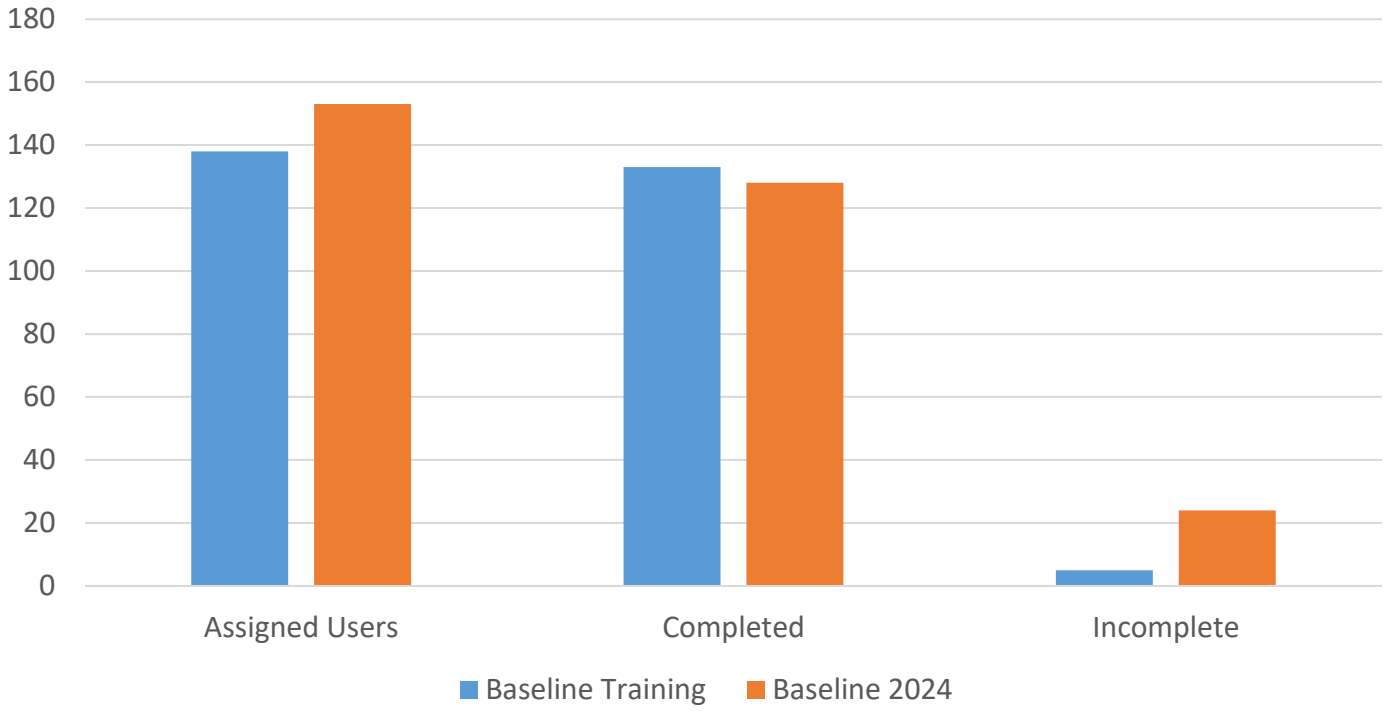
176 Recipients	100% 176 Delivered	77.3% 136 Opened	27.8% 49 Clicked	0% 0 QR Code Scanned	0% 0 Replied	5.1% 9 Attachment Opened	0% 0 Macro Enabled	0% 0 Data Entered	29.5% 52 Reported	0% 0 Bounced

Covenant Christian School
All knowledge through Christ

new era. TECHNOLOGY

7 – Educate Staff, Parents, and Students

KnowBe4 Training stats over time



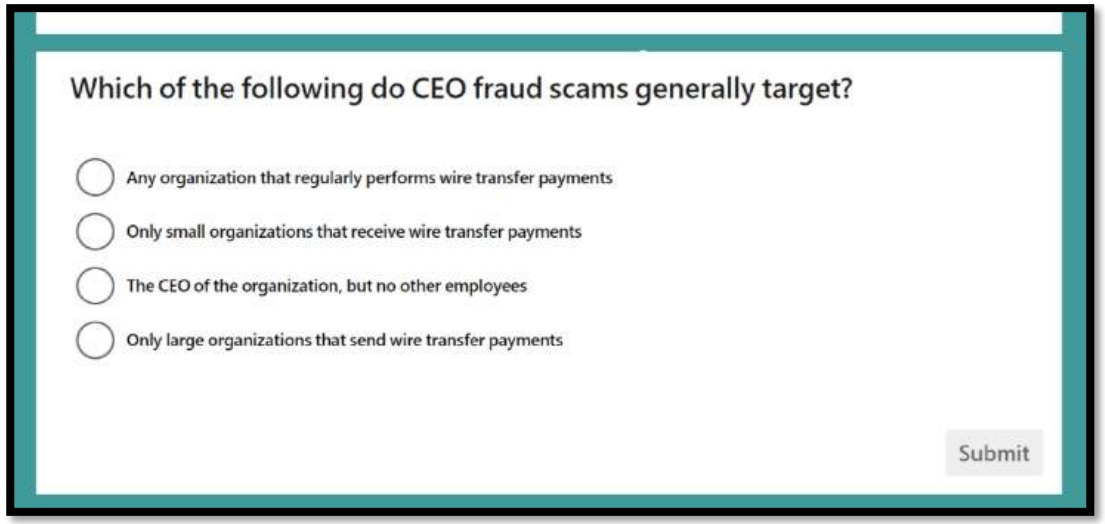
138	3.6%	2.2%	0.7%	96.4%	3.6%
All Users	5 Incomplete	3 Not Started	1 In Progress	133 Completed	5 Overdue

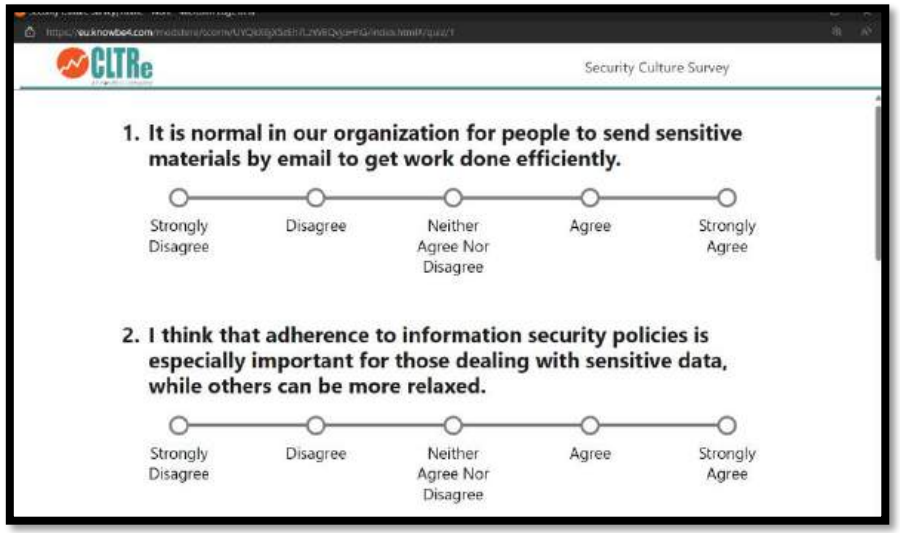
Covenant Christian School
All knowledge through Christ

new era. TECHNOLOGY

7 – Educate Staff, Parents, and Students

KnowBe4 Training Modules





Covenant Christian School
All knowledge through Christ

new era. TECHNOLOGY

Training Demo

- https://eu.knowbe4.com/ui/users/login

A Cyber Security Incident Response Plan

Why do we need one?

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

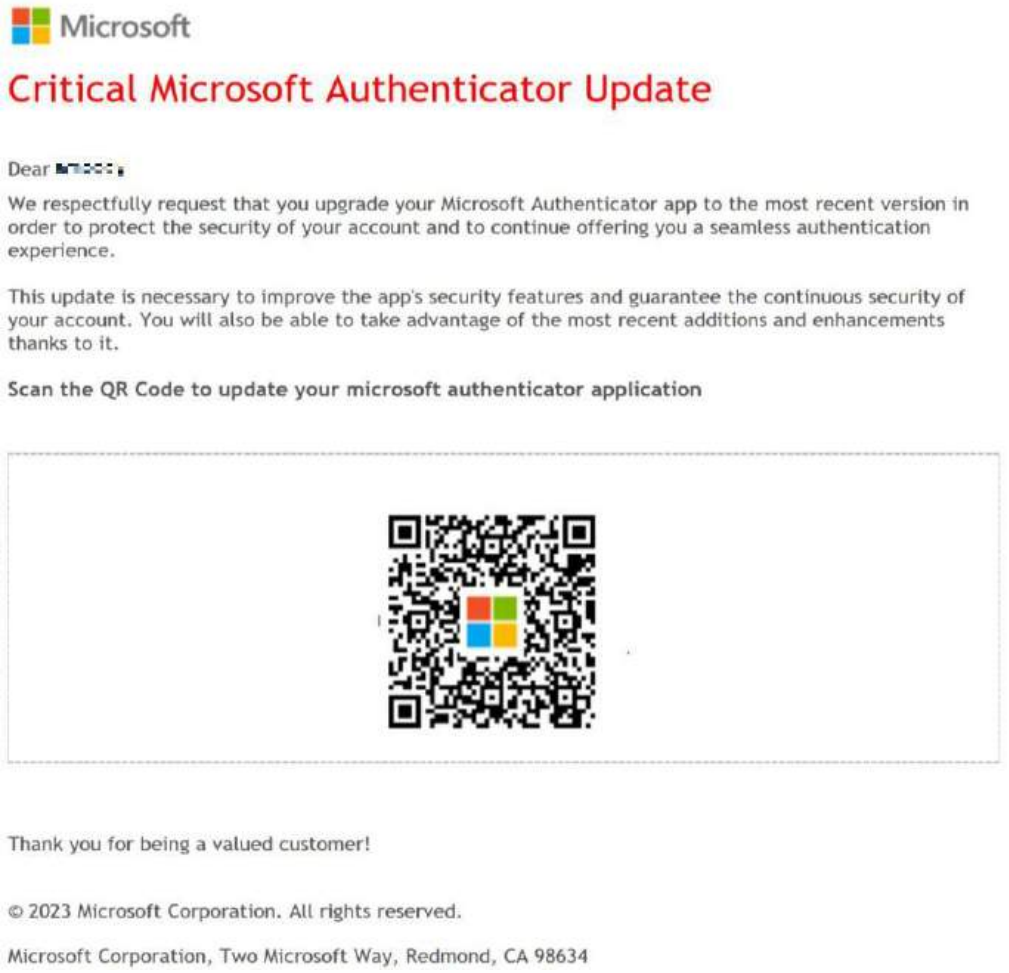
Friday, 13th October 2:00pm

- 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.



Microsoft

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!

Microsoft Corporation, Two Microsoft Way, Redmond, CA 98634

Covenant Christian School
All knowledge through Christ

new era. TECHNOLOGY

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.

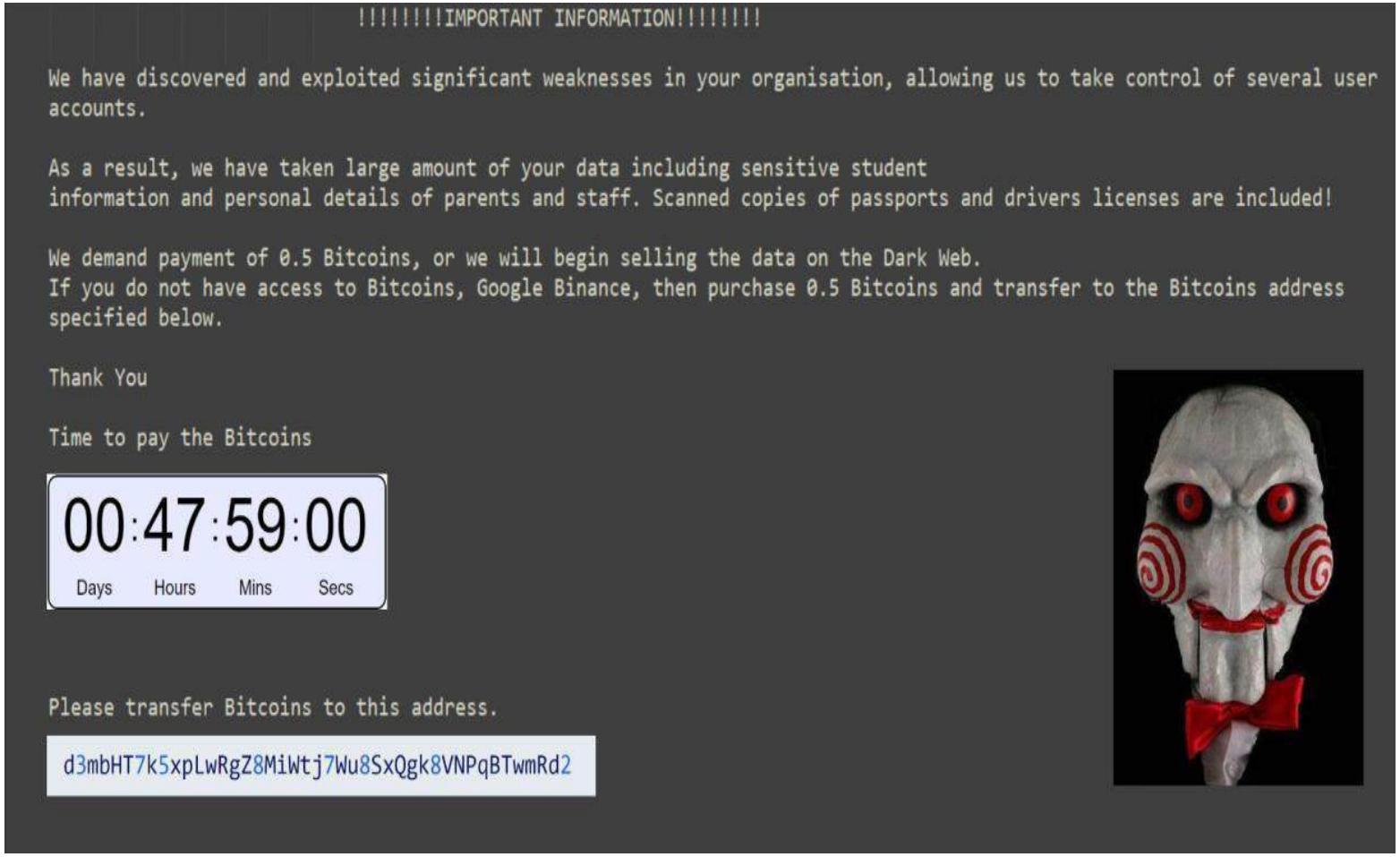
Emails sent through to all targeted users and:

admin@abcalpha.nsw.edu.au

enrolments@abcalpha.nsw.edu.au

danceacademy@abcalpha.nsw.edu.au

sportsacademy@abcalpha.nsw.edu.au



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

Covenant Christian School
All knowledge through Christ

new era. TECHNOLOGY

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

Australian Government
Australian Signals Directorate
ACSC Australian Cyber Security Centre

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

Australian Government
Australian Signals Directorate
ACSC Australian Cyber Security Centre

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?

Australian Government
Australian Signals Directorate
ACSC Australian Cyber Security Centre

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

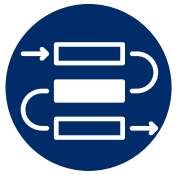
Simulation exercises:

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

Preparing a Cyber Security *incident response plan*

Incident Management

INCIDENT



PROCESS

DETECTION

ANALYSIS

INITIAL SUPPORT

RESTORE

REPORTING

- A cyber incident is any attempted or actual unauthorised access.
- The goal of incident response is to detect and halt attacks and limit the damage.

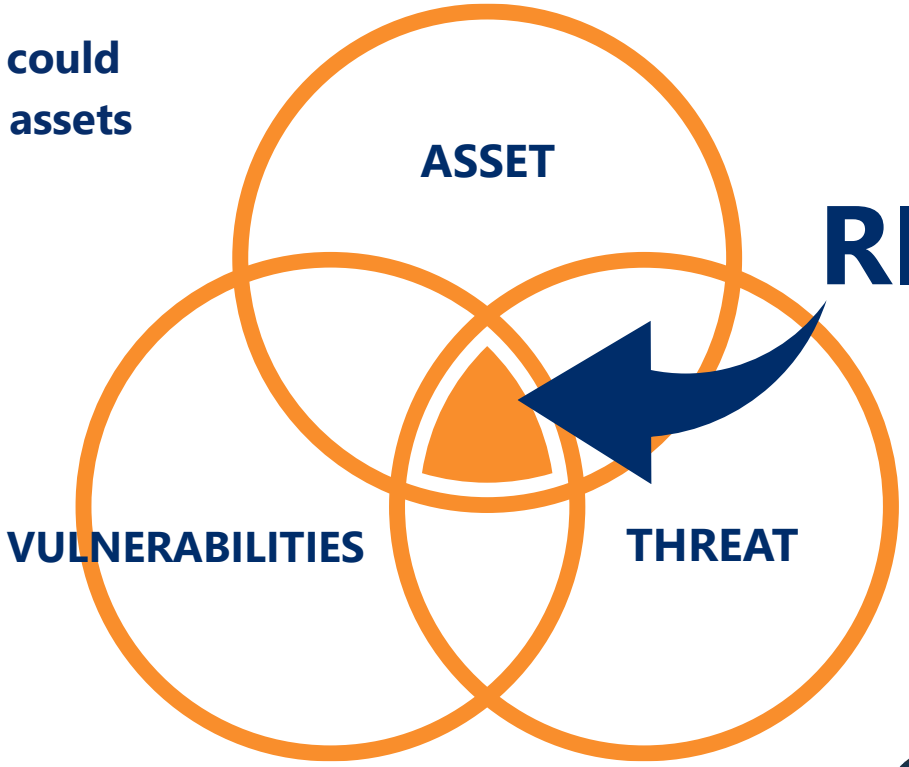
Risk Management

Terms

ASSET | **Anything of value**

THREAT | **Something that could lead to a loss of assets**

VULNERABILITIES | **Weakness or flaw that could be exploited**



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

Risk Management

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

Critical Steps for Cyber Security Incident Response Planning

- IDENTIFY
- DEVELOP
- ENDORSEMENT
- PLAN
- REASSESS

IDENTIFY ASSETS & RISKS

DEVELOP INCIDENT RESPONSE PLANS & SUPPORT TEAMS

EXECUTE PLAN WITH EXECUTIVE ENDORSEMENT

PLAN WITH YOUR PEOPLE

REASSESS & REFINE

Cyber Incident Response Plan

Table of Contents to include:

- IDENTIFY
- DEVELOP
- ENDORSEMENT
- PLAN
- REASSESS

Covenant Christian School
All knowledge through Christ

new era. TECHNOLOGY

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

Covenant Christian School
All knowledge through Christ

new era. TECHNOLOGY

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)

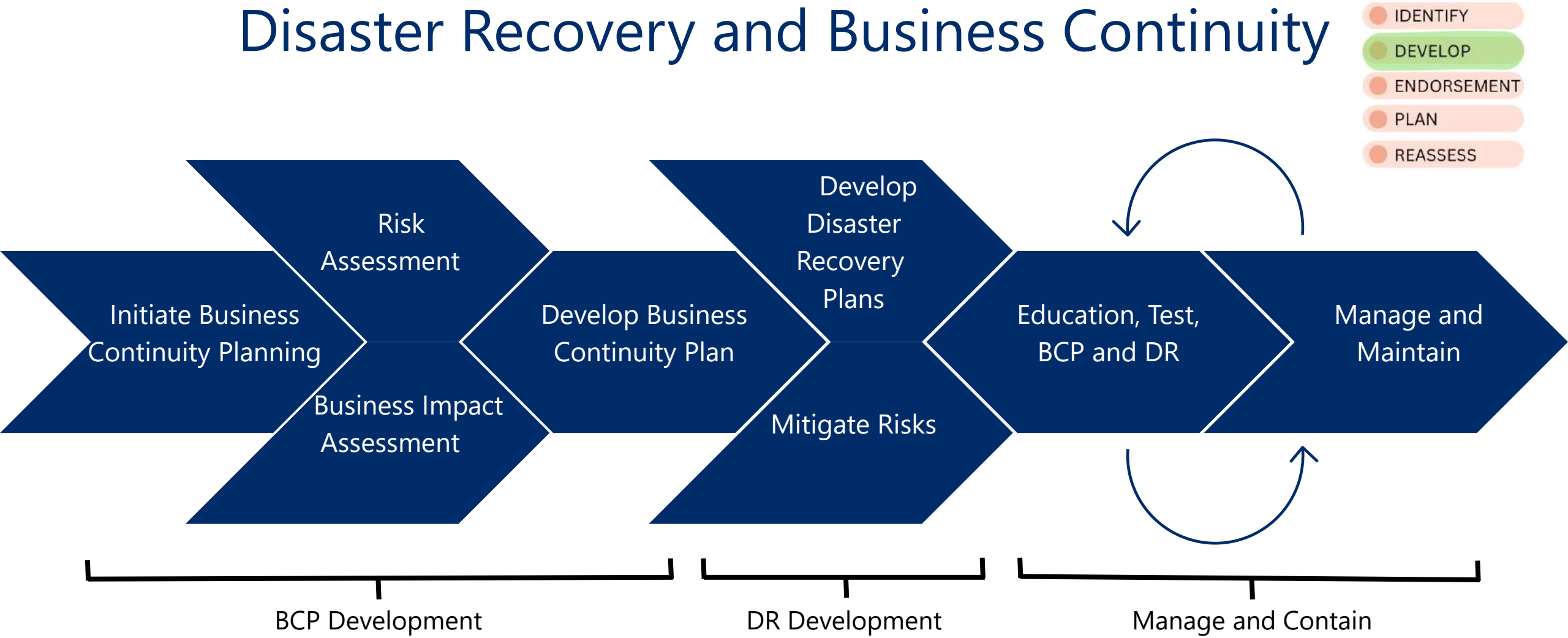
Develop Disaster Recovery Plans (DR)

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

Covenant Christian School
All knowledge through Christ

new era. TECHNOLOGY

Disaster Recovery and Business Continuity



Covenant Christian School
All knowledge through Christ

new era. TECHNOLOGY

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 **I**ncident **R**esponse **T**eam - **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

Covenant Christian School
All knowledge through Christ

new era. TECHNOLOGY

Incident Response Team Model

Critical **I**ncident **C**oordinating **T**eam- **CICT**

IDENTIFY
DEVELOP
ENDORSEMENT
PLAN
REASSESS

- Provide strategic oversite, 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

Covenant Christian School
All knowledge through Christ

new era. TECHNOLOGY

Incident Response Team Model

School Board

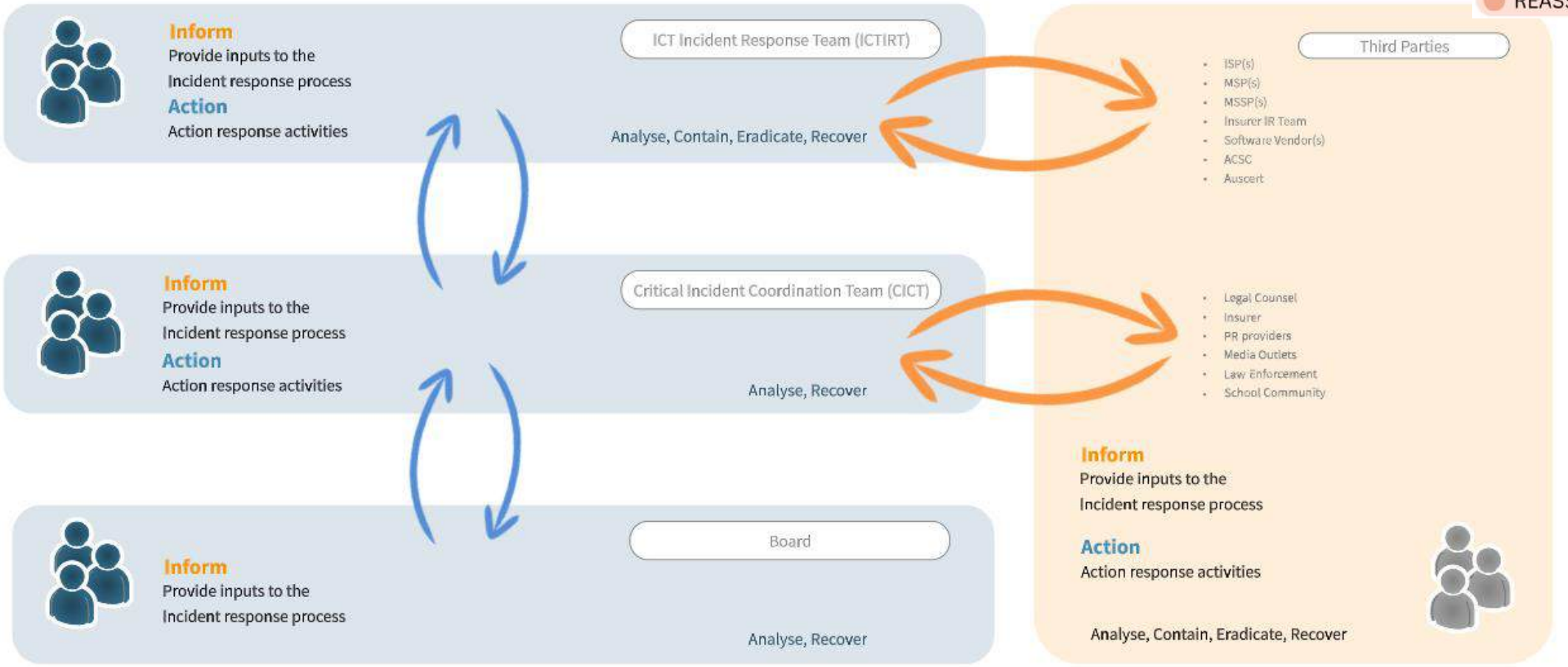
Although not actioning response activities, Board will assist the CICT in guiding response activities particular during containment and recovery phases.

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



Covenant Christian School
All knowledge through Christ

new era. TECHNOLOGY

Communication with School Community in the event of an outage

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 Christian School
All knowledge through Christ

new era. TECHNOLOGY

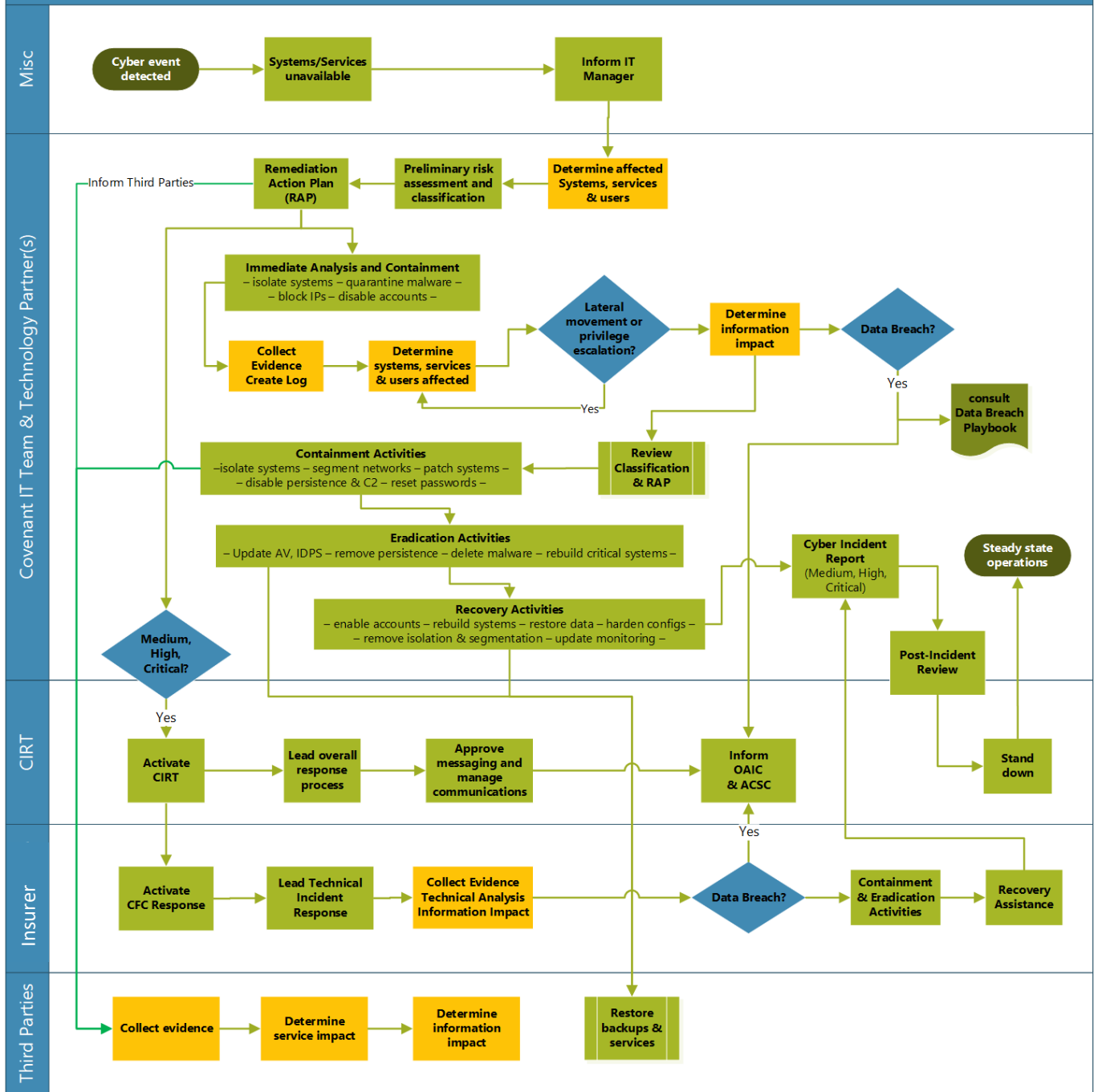
Covenant Incident Response Plan

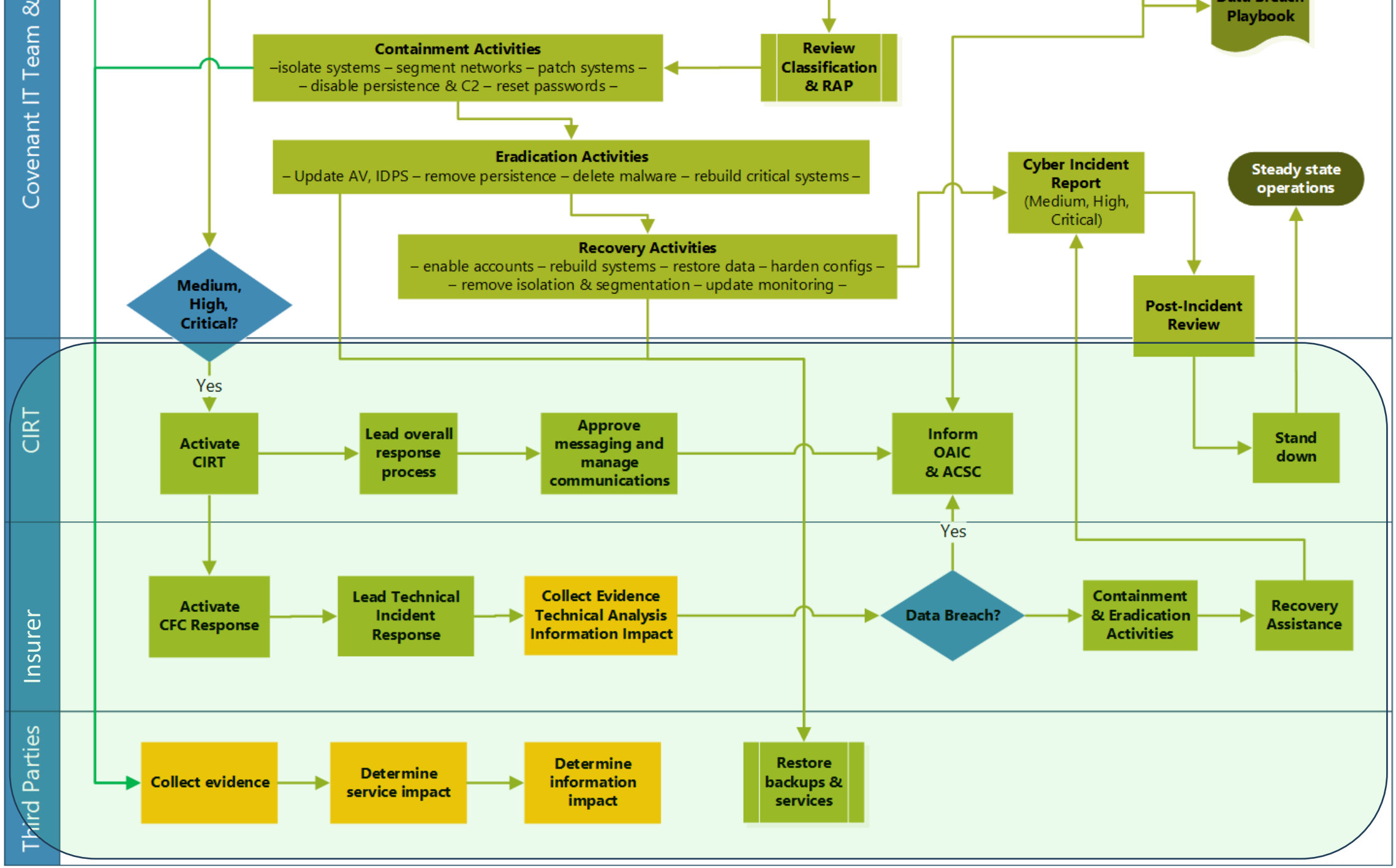
Extract: Playbooks

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




Covenant IT Team &
CIRT
Insurer
Third Parties
Containment Activities
–isolate systems – segment networks – patch systems –
– disable persistence & C2 – reset passwords –
Review Classification & RAP
Eradication Activities
– Update AV, IDPS – remove persistence – delete malware – rebuild critical systems –
Recovery Activities
– enable accounts – rebuild systems – restore data – harden configs –
– remove isolation & segmentation – update monitoring –
Cyber Incident Report
(Medium, High, Critical)
Steady state operations
Post-Incident Review
Medium, High, Critical?
Yes
Activate CIRT
Lead overall response process
Approve messaging and manage communications
Inform OAIC & ACSC
Stand down
Yes
Activate CFC Response
Lead Technical Incident Response
Collect Evidence Technical Analysis Information Impact
Data Breach?
Containment & Eradication Activities
Recovery Assistance
Collect evidence
Determine service impact
Determine information impact
Restore backups & services

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

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

Mitch Green

Thanks so much for joining us –

please scan the QR code to give us your details if you haven't already!