Beyond the Perimeter: Safeguarding Schools Through Third-Party Cyber Risk Management

AISNSW CYBER SECURITY SYMPOSIUM 2025

Empowering Schools for Cyber Resilience

Friday 21 February, 2025

Google Sydney

#AISNSWICT

10:20am - 10:50am

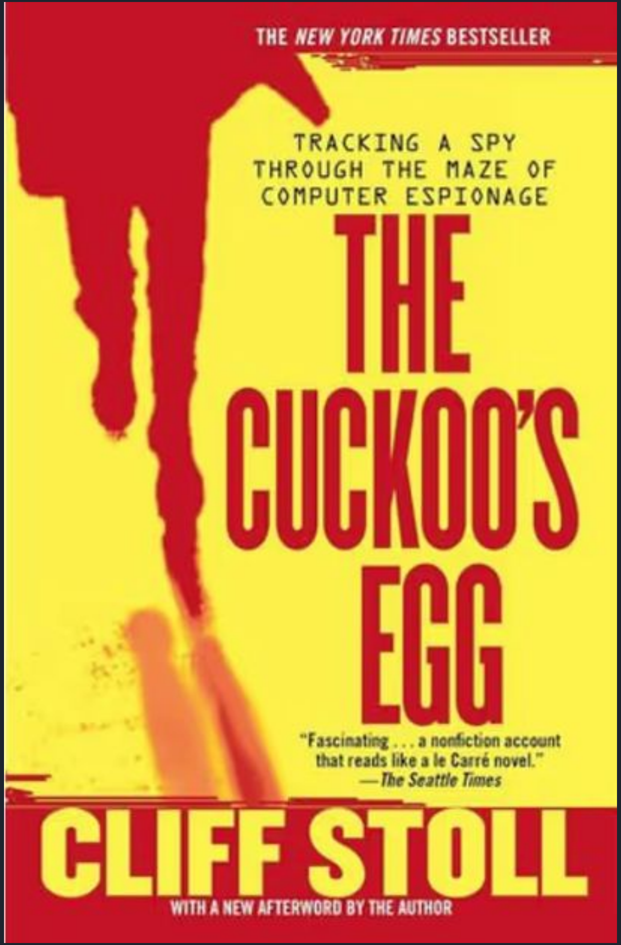
Andrew Hottes, Chief Digital Information Officer, Cranbrook School

Beyond the Perimeter: Safeguarding Schools Through Third-Party Cyber Risk Management

Leadership and Culture:

Building a Cyber-Aware School Community

The Cuckoo's Egg (1990) highlights the importance of cybersecurity and persistence, written by **Clifford Stoll**, a systems administrator at Lawrence Berkeley National Laboratory


THE NEW YORK TIMES BESTSELLER
TRACKING A SPY THROUGH THE MAZE OF COMPUTER ESPIONAGE
THE CUCKOO'S EGG
"Fascinating . . . a nonfiction account that reads like a le Carré novel."
—The Seattle Times
CLIFF STOLL
WITH A NEW AFTERWORD BY THE AUTHOR

A discovery of a small accounting error (75c!) that led to the uncovering of an international espionage operation in the late 1980s.

3rd party Access through Berkley – Who would have thought?

Did you know 98% of organisations have a relationship with a third party that has been breached?
Security.io

Types of Information Compromised:

1. **Classified Military Documents**
    1. The hackers gained access to systems related to military operations and sensitive military projects.
    2. This included information about **satellite tracking**, missile guidance, and military strategy.
2. **User Credentials and System Access**
    1. The hackers captured login credentials for multiple accounts across university, military, and government systems.
    2. This allowed them to **escalate privileges** and move laterally within networks.
3. **Software Source Code**
    1. They stole source code from research institutions and defence contractors.
    2. This could have been used to study vulnerabilities in U.S. systems.
4. **Research Data**
    1. Sensitive academic and scientific research data were compromised, particularly in physics, computer science, and artificial intelligence research.
5. **Government Network Maps**
    1. The hackers collected information on network topology, gaining a blueprint of connected systems.
    2. This allowed them to target other networks more effectively.
6. **Password Files**
    1. They regularly dumped password files from compromised systems and attempted to crack them offline.
    2. These files provided ongoing access to multiple systems.

Key Cyber Regulations

These are mandatory legal requirements designed to protect personal data, ensure security and enforce breach reporting. Non-compliance can lead to penalties.

Australian Privacy Act (Including the Notifiable Data Breach Scheme) – Regulates how personal information is collected, used, and protected in Australia [1]

GDPR (General Data Protection Regulation) – EU regulation on data protection and privacy

HIPAA (Health Insurance Portability and Accountability Act) – U.S. regulation for protecting healthcare data

California Consumer Privacy Act (CCPA) – U.S. law focusing on consumer rights over personal data

DORA (Digital Operational Resilience Act) – EU regulation for operational resilience in the financial sector **new**

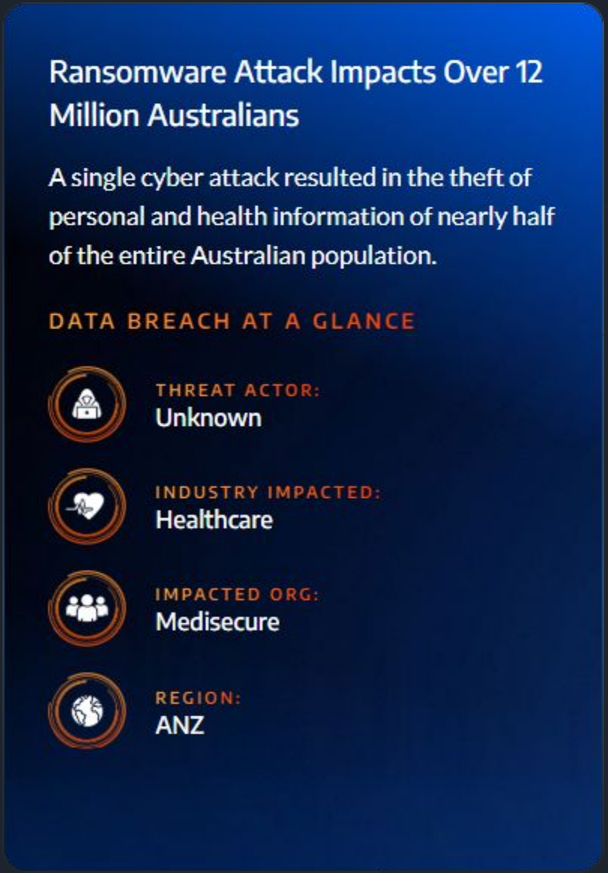
NIS2 Directive – EU directive to strengthen cybersecurity in critical infrastructure sectors

Did you know the Privacy Legislation Amendment (Enforcement and Other Measures) Act 2022, penalties for more severe breaches can be much higher:

$50 million AUD, or three times the value of the benefit obtained through the misuse of data, or 10% of the organisation's annual domestic turnover (whichever is greater).

[1] Individuals and Small Entities: Fines up to $50,000 AUD for serious or repeated breaches.
Organisations and Larger Entities for serious or repeated breaches, fines can reach up to $2.5 million AUD.

The breach did not originate from a direct attack on healthcare providers, but rather on a **third-party service handling sensitive health records**.



Ransomware Attack Impacts Over 12 Million Australians

A single cyber attack resulted in the theft of personal and health information of nearly half of the entire Australian population.

DATA BREACH AT A GLANCE

THREAT ACTOR:
Unknown

INDUSTRY IMPACTED:
Healthcare

IMPACTED ORG:
Medisecure

REGION:
ANZ

Made off off with **6.5 terabytes of data** before encrypting systems, exfiltrated the **personal and health information of 12.9 million Australians**

MediSecure appointed liquidators and went into administration. “This made it not practicable to specifically identify all individuals and their information impacted by the incident without incurring substantial cost that MediSecure was not in a financial position to meet,” administrators said.

2024 Data Breaches in Review - Arctic Wolf

Average Cost of a Data Breach

$4,880,000

The global average cost of a data breach in 2024, **marking a 10% increase from the previous year** and the highest average to date.
ibm.com

Time taken to Identify and Contain Breaches

In 2024, organisations took an average of

194 days to Identify

64 days to Contain

Breaches involving stolen or compromised credentials had the longest resolution time, averaging 88 days to contain.

varonis.com

3rd Party Data Breach Trends

3,000,000,000+

Globally Exposed Records in 2024

National Public Data Breach (2024)

Incident: National Public Data (NPD), a background check company, experienced a significant data breach in early 2024. The breach allegedly exposed up to **2.9 billion records** containing highly sensitive personal data of individuals in the U.S., U.K., and Canada. The compromised information included full names, addresses, dates of birth, phone numbers, and Social Security numbers. The breach reportedly occurred in December 2023 and continued undetected for several months until April 2024, when the hackers began selling the stolen data online. NPD acknowledged the breach in August 2024 and has since been cooperating with law enforcement agencies. strongdm.com

Third-Party Nature: As a data broker, **NPD collects and processes personal information** from various public and private sources. Organisations relying on NPD for background checks and other services were indirectly affected by this breach, as their employees' or **clients' data handled by NPD were compromised**. This incident underscores the risks associated with third-party service providers that manage sensitive information on behalf of other organisations.

And in our own backyard…….

University of Sydney Data Breach (August 2023):
Incident: A third-party service provider associated with the University of Sydney suffered a data breach, leading to unauthorised access to personal information of a limited number of recently applied and enrolled international students.

Consequence: The compromised data included personal details of international applicants. The university promptly secured its systems, initiated an investigation, and notified affected individuals. itnews.com.au

Tasmanian Department of Education Data Breach (April 2023):
Incident: A third-party file transfer service used by the Tasmanian Department of Education was compromised, resulting in the exposure of sensitive information, including schoolchildren's data.

Consequence: Approximately 16,000 documents were leaked on the dark web, prompting the department to enhance its cybersecurity measures and provide support to those affected. theguardian.com

Large-Scale Education Data Leak (2019):
Incident: An online mathematics resource with a significant Australian user base experienced a data leak, exposing information belonging to individuals with email addresses ending in vic.edu.au and wa.edu.au.

Consequence: The breach raised concerns about the security practices of third-party educational tools and led institutions to reassess their data-sharing agreements and cybersecurity protocols. itnews.com.au

University of Melbourne Third-Party Data Breach
Incident: A third-party software provider to the University of Melbourne, FORTRA GoAnywhere MFT, experienced a cyberattack. The university intercepted an email from a threat actor claiming to have stolen university data from the compromised system.

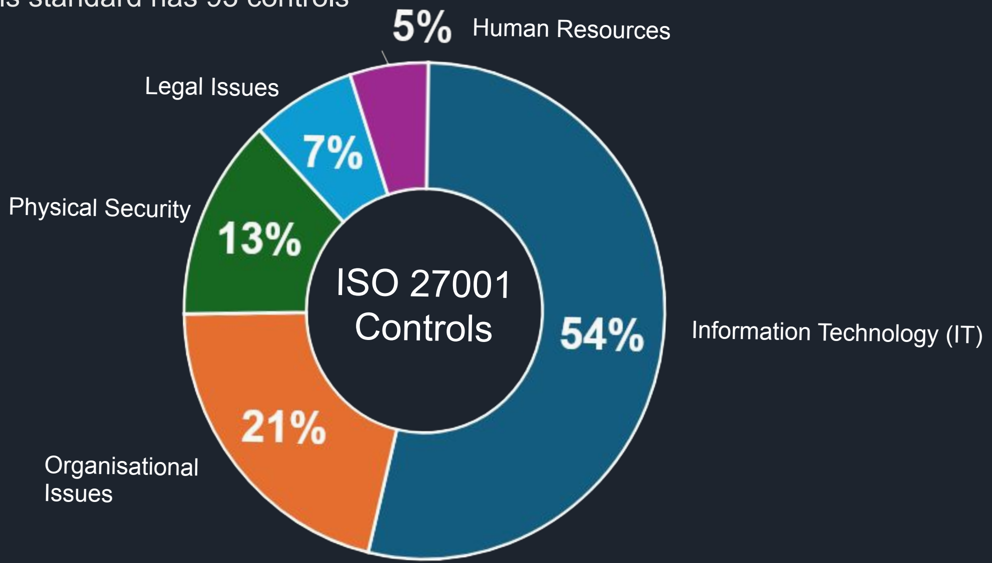
Positive Outcome

Consequence: The investigation revealed that the stolen data primarily consisted of cost codes used for university accounts, which do not contain personal or sensitive information. Consequently, the breach did not impact the university's operations or compromise personal data. staff.unimelb.edu.au

ISO 27001 and the Essential Eight?

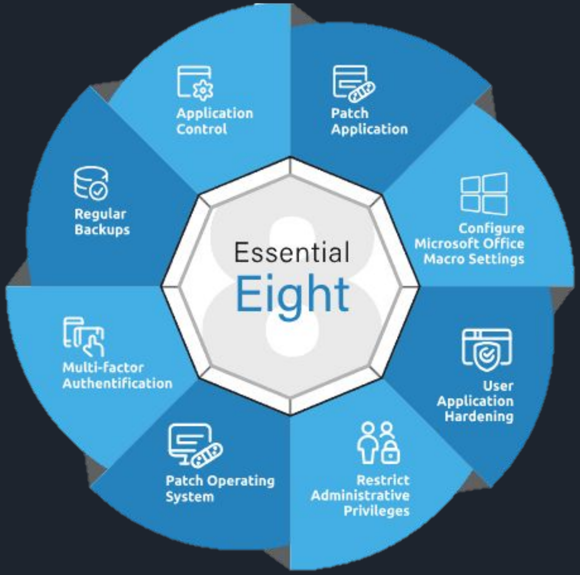
ISO 27001 is an international cybersecurity standard developed by the **International Organization for Standardization (ISO)** to help organisations manage and secure sensitive information. It focuses on a **risk-based approach to information security**, ensuring confidentiality, integrity, and availability of data through a structured **Information Security Management System (ISMS)**.

This standard has 93 controls

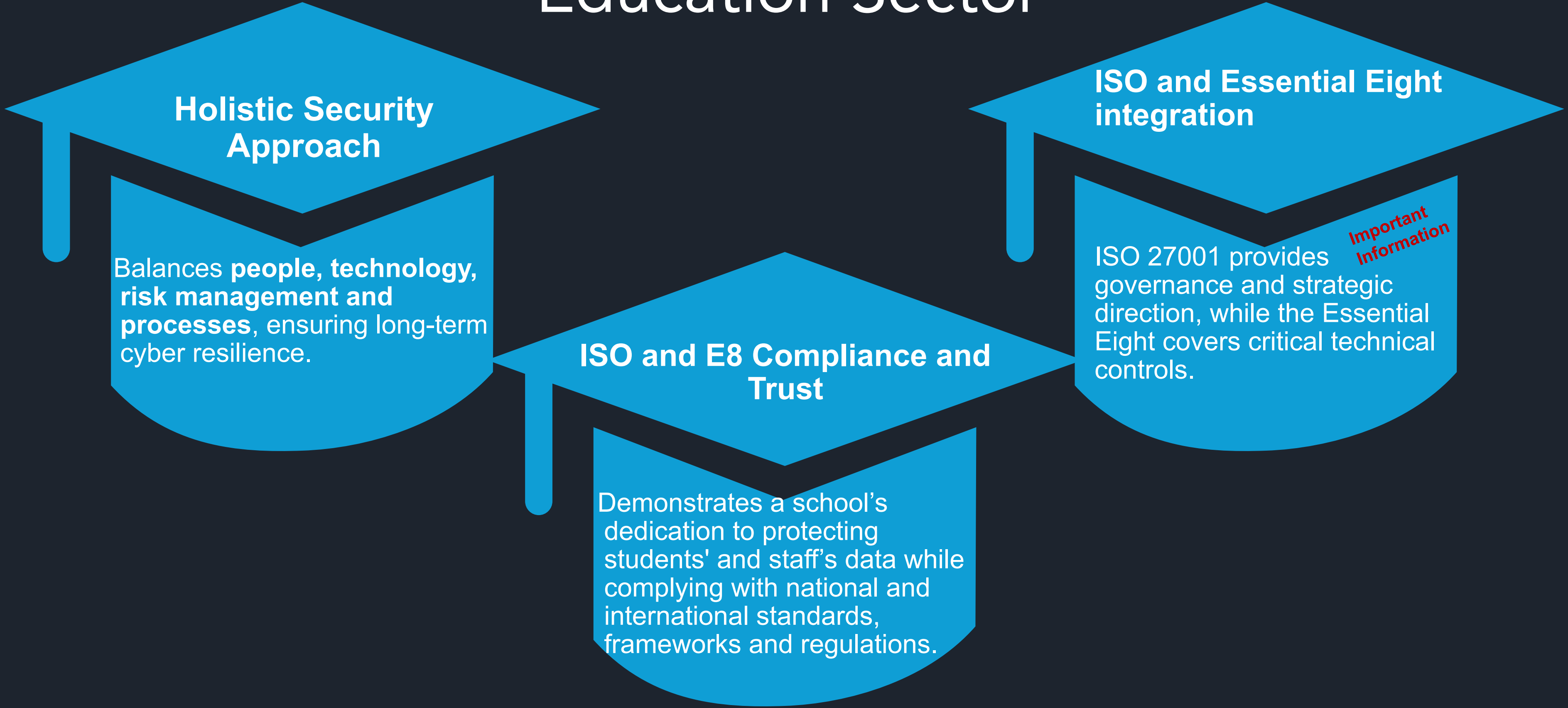


The **Essential Eight** is a **baseline cybersecurity framework** developed by the **Australian Cyber Security Centre (ACSC)** to help organisations protect against cyber threats. It focuses on **practical, achievable security measures** to **mitigate common attack vectors** such as ransomware, phishing, and data breaches.

The framework has 3 Maturity levels


Essential Eight
Application Control
Patch Application
Configure Microsoft Office Macro Settings
User Application Hardening
Restrict Administrative Privileges
Patch Operating System
Multi-Factor Authentification
Regular Backups

ISO 27001 and the Essential Eight within the Education Sector



Holistic Security Approach

Balances **people, technology, risk management and processes**, ensuring long-term cyber resilience.

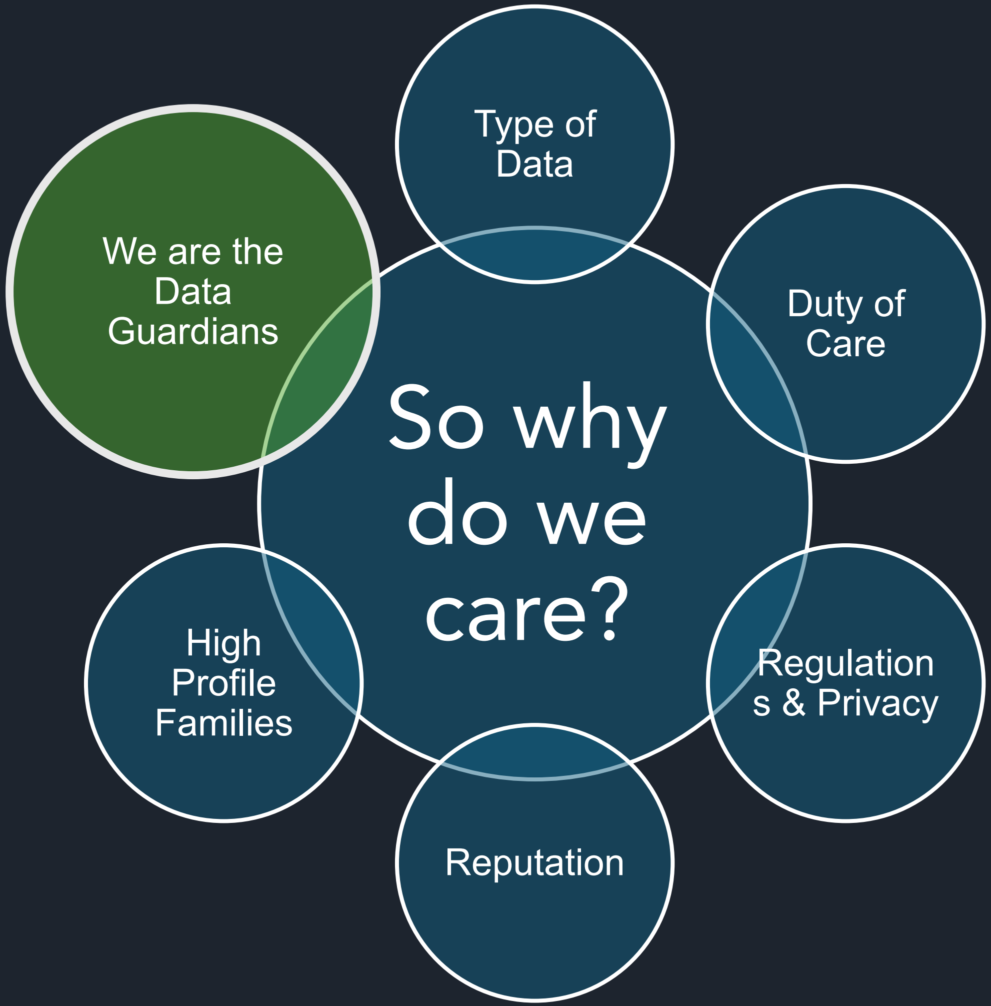
ISO and E8 Compliance and Trust

Demonstrates a school's dedication to protecting students' and staff's data while complying with national and international standards, frameworks and regulations.

ISO and Essential Eight integration

Important Information

ISO 27001 provides governance and strategic direction, while the Essential Eight covers critical technical controls.



So why do we care?

We are the Data Guardians

Type of Data

Duty of Care

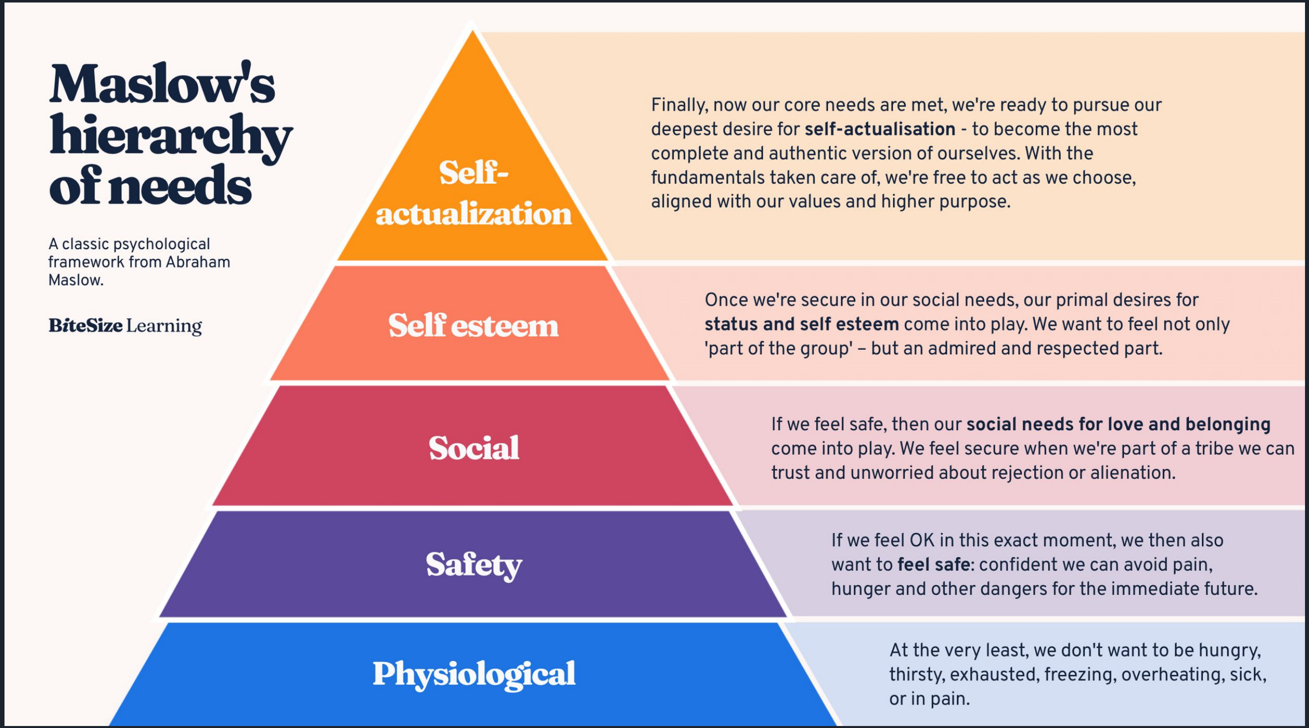
Regulation s & Privacy

Reputation

High Profile Families

Maslow’s Hierarchy of Needs

www.bitesizelearning.co.uk



Maslow's hierarchy of needs

A classic psychological framework from Abraham Maslow.

BiteSize Learning

Self-actualization

Finally, now our core needs are met, we're ready to pursue our deepest desire for **self-actualisation** - to become the most complete and authentic version of ourselves. With the fundamentals taken care of, we're free to act as we choose, aligned with our values and higher purpose.

Self esteem

Once we're secure in our social needs, our primal desires for **status and self esteem** come into play. We want to feel not only 'part of the group' – but an admired and respected part.

Social

If we feel safe, then our **social needs for love and belonging** come into play. We feel secure when we're part of a tribe we can trust and unworried about rejection or alienation.

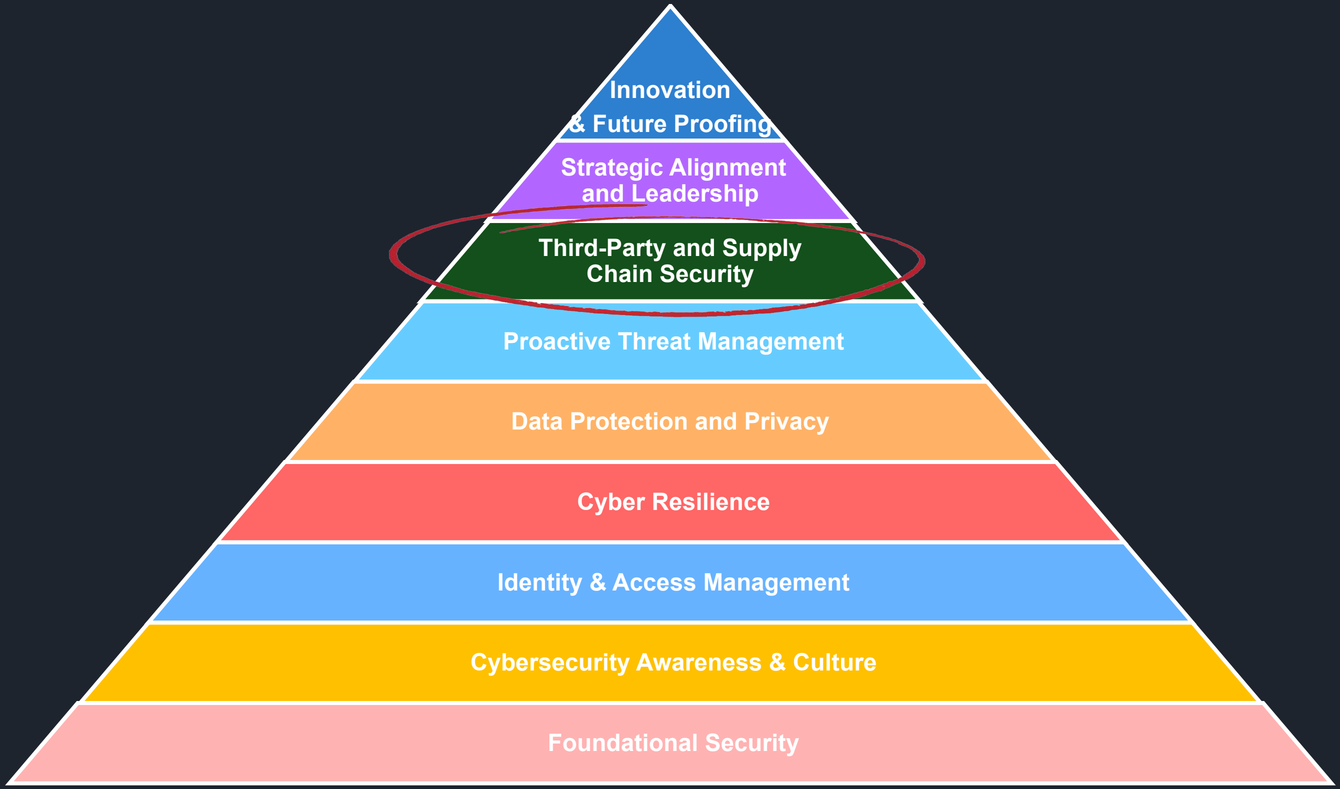
Safety

If we feel OK in this exact moment, we then also want to **feel safe**: confident we can avoid pain, hunger and other dangers for the immediate future.

Physiological

At the very least, we don't want to be hungry, thirsty, exhausted, freezing, overheating, sick, or in pain.

Andrew’s Hierarchy of Cyber Needs



Innovation & Future Proofing

Strategic Alignment and Leadership

Third-Party and Supply Chain Security

Proactive Threat Management

Data Protection and Privacy

Cyber Resilience

Identity & Access Management

Cybersecurity Awareness & Culture

Foundational Security

A Security Stack for Schools: ISO 27001 and Essential Eight Tools

Antivirus: Protects against malware and other malicious threats

SIEM (Security Information and Event Management): Collects and analyses security data from various sources.

MDR (Managed Detection and Response): Provides 24/7 monitoring and response to security incidents

24x7 SOC (Security Operations Center): Ensures continuous surveillance and management of security operations

Microsoft Secure Score: Measures and helps improve the security posture of the school's Microsoft environment

Vulnerability Scanning: Identifies and assesses vulnerabilities in the school's IT infrastructure

Penetration Testing: Simulates cyberattacks to test the effectiveness of security measures

Data Location Tools: Helps track and manage the location of sensitive data

Phishing Campaigns: Educates staff and students on recognising and responding to phishing attempts

Firewall Protection: Ensures network security by monitoring and controlling incoming and outgoing network traffic based on predetermined security rules.

Data Loss Prevention (DLP): Helps to detect and prevent potential data breaches by monitoring, detecting, and blocking sensitive data while in use, in motion, or at rest.

Identity and Access Management (IAM): Controls user access to critical information within an organisation, ensuring that the right users have access to the right resources.

Multi-Factor Authentication (MFA): Adds an extra layer of security by requiring two or more verification factors to gain access to a system.

Security Awareness Training: Educates staff and students about the latest cybersecurity threats and best practices for maintaining security.

Patch Management: Ensures that all systems and software are up to date with the latest security patches to protect against vulnerabilities.

Encrypted Communication Tools: Secures communications within the school, ensuring that messages and data exchanged between staff, students, and parents are encrypted.

Zero Trust Architecture: Implements a "never trust, always verify" approach to secure the network by assuming that threats could be both inside and outside the network

Backup and Recovery Solutions: Ensures that all data is regularly backed up and can be recovered quickly in the event of data loss or a cyber incident.

And remember…

Third-party vendors expand your attack surface

They handle sensitive student, staff, and financial data, making them a high-value target for cyber threats.

Due diligence is not a one-time task

Schools must move beyond basic vendor assessments and adopt continuous monitoring for ongoing risk management.

Require security compliance

Vendors should align with ISO 27001, Essential Eight, and Australian Privacy Laws to ensure adequate security measures.

Access management is critical

Limit third-party access to only what is necessary and enforce multi-factor authentication (MFA) and regular access reviews.

Review past vendor-related breaches (e.g., University of Melbourne, Medisecure) to understand the risks.

Cybersecurity is a leadership issue

School leaders (Principals, COOs, ICT teams) must own the vendor risk conversation and prioritise security in procurement decisions.

Proactive risk management is key

Schools must integrate continuous security monitoring, training, and contingency planning to mitigate third-party threats.

Third-party breaches can cost schools financially and reputationally

Conduct Vendor Security Assessments

Evaluate vendors on data collection, storage, security controls, and breach response plans before onboarding.

Vendor Security Assessments

Section 1: Data Collection and Handling

1. What types of personal data do you collect from our business transactions? (This might include things like names, phone numbers, addresses, payment details, or any other information that can identify someone personally.)
2. Please specify any personally identifiable information (PII) you collect, store, or process other than basic contact information for the School as described above.
3. For what purposes do you collect PII?
4. How do you collect and store this data? Describe your data storage systems.
5. Who has access to the PII you collect?
6. Do you share any PII with third parties? If yes, please list the third parties and describe the nature of the sharing.

Section 2: Data Security Measures

7. What security measures do you have in place to protect the data you hold?
8. Do you have a formally documented Information Security Policy? If yes, please provide details.
9. Are you compliant with any national or international data protection frameworks or standards (e.g., ISO 27001, Essential Eight, Privacy Act etc)?
10. Have you undergone any security audits or certifications? If yes, provide details.
11. Describe your incident response plan in the event of a data breach.
12. How do you ensure data security when data is transferred to or from your organisation?

Vendor Security Assessments

Section 3: Data Retention and Disposal

13. What is your data retention policy for PII?
14. How do you dispose of PII once it is no longer needed? Describe your data destruction processes.

Section 4: Additional Information

15. Do you provide training to your employees on data protection and security?
16. Are there any recent incidents of data breaches or security lapses within your organisation? If yes, how were they resolved?
17. Is there any additional information about your data handling and security practices that you would like to share with us?

Technology Risk = Business risk

A **Technology Risk Ambassador** could play a pivotal role in safeguarding a school's digital ecosystem by identifying, communicating, and mitigating risks beyond financial loss.

This person acts as a bridge between technical teams and school leadership, translating technology risks into clear, actionable insights. By focusing on areas such as reputation, operations, legal compliance, cybersecurity, human impact, and strategic planning, the Technology Risk Ambassador ensures that decision-makers have a holistic view of potential threats.

They help implement proactive risk management strategies, ensuring adherence to standards like ISO 27001 and the ACSC Essential Eight while fostering a culture of cyber resilience.

They can minimise disruptions to learning, maintain stakeholder trust, and **align the school's digital policies with emerging global trends—ultimately turning risk management into a strategic advantage**.

Practical Strategies

Building a Cybersecurity Culture

Takeaways for, School Principals, COO's and ICT Leaders

Cybersecurity is an Organisational Risk:

Cyber threats impact more than just IT departments; they have financial, operational, and reputational consequences for schools.

Vendor Due Diligence is Critical:

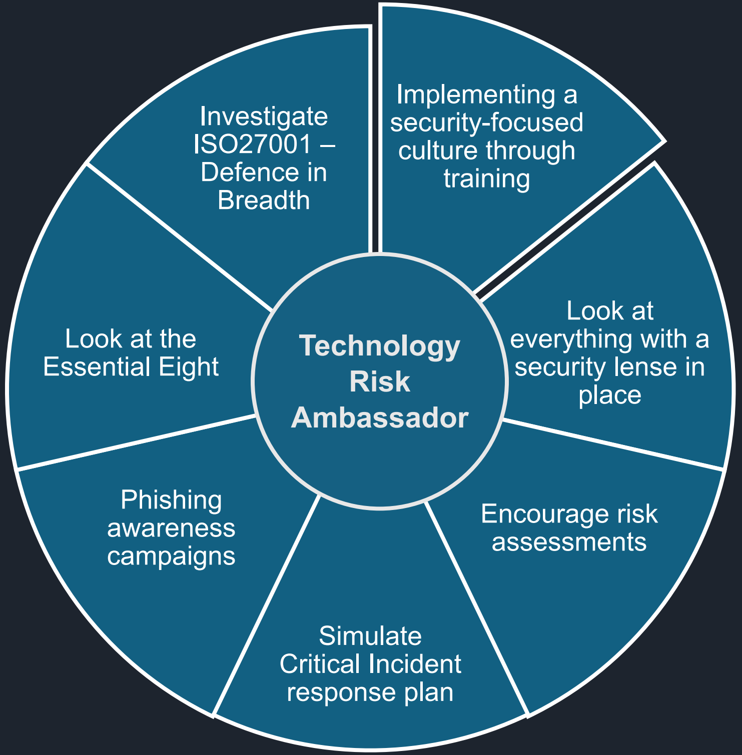
Schools must move beyond basic vendor assessments and adopt a continuous monitoring approach.

Proactive Risk Management is Essential:

Schools must build proactive security postures with regular security awareness training and contingency planning.

Technology Risk = Business risk

Practical Strategies



Technology Risk Ambassador
Implementing a security-focused culture through training
Look at everything with a security lense in place
Encourage risk assessments
Simulate Critical Incident response plan
Phishing awareness campaigns
Look at the Essential Eight
Investigate ISO27001 – Defence in Breadth

If a vendor is storing or processing your school's data,

Their security posture is

YOUR RISK!

Andrew Hottes, Chief Digital Information Officer

ahottes@cranbrook.nsw.edu.au