

Webinar: Is your school struggling with data security?



9 Nov 2022

Agenda

- **Introductions and Welcome**
- **Setting the Scene**
 - *What is data security for schools? What does it encompass?*
- **A School's Perspective**
 - *How are schools reacting to the recent cyber security breaches?*
- **Essential Steps to Secure School Data**
 - *What are the essential steps a school should take to start securing their data security?*
- **Q&A**
 - Please add your question to the chat function in MS teams. If you would like to submit your questions anonymously, please email emma@edsmart.com
- **4.30pm Thanks and Finish**

***Please note:** This webinar is being recorded, and a link will be distributed to attendees



Introductions & Welcome



David Eedle

CEO and Co-Founder, EdSmart

Co-founded EdSmart in 2014, previously worked with San Francisco-based SaaS firms, and launched and sold multiple online businesses in Australia. EdSmart supports 750,000 parents/caregivers, 560,000 students and 75,000 school staff in 8 countries.



James Lacey

Head of GRC, CTRL Group

Manages the Governance Risk and Compliance Team including designing and implementing data centric cyber risk assessments and preparing organisations to be compliant with ISO 27001, GDPR, APRA CPS 234, NIST and other data protection standards.



Thomas Blackwood

Head of ICT, Fahan School

Worked across cyber security and corporate IT roles before starting at Fahan School in 2018. Motivated to lead Fahan School on the journey of bringing the business and school to the cutting edge of technology and innovation while managing cyber risks.



Setting the Scene

James Lacey (CTRL Group)

- What are the unique considerations schools need to take into account concerning data security?
- Why are schools particularly vulnerable and how can they overcome this?
- Are there any real-world examples we can put forward as learnings?

A School's Perspective

Thomas Blackwood (Fahan School)

- How is Fahan reacting to the recent cyber security breaches?




FIGURE 2

Cybersecurity spending across sectors

■ Percentage of revenue

■ Percentage of IT spending

■ Per FTE

		2019	2020
	Retail/corporate banking	0.3% 10.1% US\$2,074	0.6% 9.4% US\$2,688
	Consumer/financial services (nonbanking)	0.3% 9.7% US\$2,817	0.4% 10.5% US\$2,348
	Insurance	0.3% 9.3% US\$2,245	0.4% 11.9% US\$1,984
	Service provider	0.6% 8.9% US\$1,956	0.6% 7.2% US\$3,226
	Financial utility	0.8% 15.2% US\$3,630	0.8% 8.2% US\$4,375
	Aggregated total	0.3% 10.1% US\$2,337	0.5% 10.9% US\$2,691

Note: FTE=Full-time employee or equivalent.

Sources: FS-ISAC/Deloitte Cyber & Strategic Risk Services CISO survey reports, 2019 and 2020; Deloitte Center for Financial Services analysis.

Cyber isn't an issue for us..

I am worried.. But not sure what to do

I have robust policies/defenses

And.. A strong second line compliance function

I don't understand how we were breached..

There is no absolute security – we need to manage risk

We can't do this alone – we are part of the community

Immature	Developing	Investing	Advanced	Leading
Limited Awareness	Discussion of what Cyber means	Investing to improve	Boards demand better risk discussion	Lead as part of the community
Reliance on basic Security tech	Reaching out for support/advice	Still adopting point technical solutions	Move towards structured security programs	Build a cyber ecosystem with clients/suppliers
No controls or Compliance process	Policies in place and basic security processes	Strengthening policies and compliance	Build out security operations	Intelligence-led approach linked to business
Seen as a technology issue	Often driven by regulatory concerns	Initial security architecture	Ramp up testing	Cyber resilience
		Education and awareness campaigns begin	Early-stage supply chain security initiatives	Risk quantification and mitigation strategy
				Technology enabled and data driven

A School's Perspective

Thomas Blackwood (Fahan School)

- What measures have you taken to secure vulnerable data at Fahan?



A School's Perspective

Thomas Blackwood (Fahan School)

- As a school yourself, what do you think a school could do in the event of a data breach?



A School's Perspective

'Essential 8'

<https://www.cyber.gov.au/acsc/view-all-content/publications/essential-eight-maturity-model>



Appendix D: Comparison of maturity levels

Strategy	Maturity Level One	Maturity Level Two	Maturity Level Three
Application control	The execution of executables, software libraries, scripts, installers, compiled HTML, HTML applications and control panel applets is prevented on workstations from within standard user profiles and temporary folders used by the operating system, web browsers and email clients.	<p>Application control is implemented on workstations and internet-facing servers to restrict the execution of executables, software libraries, scripts, installers, compiled HTML, HTML applications and control panel applets to an organisation-approved set.</p> <p>Allowed and blocked executions on workstations and internet-facing servers are logged.</p>	<p>Application control is implemented on workstations and servers to restrict the execution of executables, software libraries, scripts, installers, compiled HTML, HTML applications, control panel applets and drivers to an organisation-approved set.</p> <p>Microsoft's 'recommended block rules' are implemented.</p> <p>Microsoft's 'recommended driver block rules' are implemented.</p> <p>Application control rulesets are validated on an annual or more frequent basis.</p> <p>Allowed and blocked executions on workstations and servers are centrally logged and protected from unauthorised modification and deletion, monitored for signs of compromise, and actioned when cyber security events are detected.</p>

Fahan School Essential 8 Progress 2022

Implemented		Fahan School Essential 8 Progress 2022				
Not implemented but plan for implementation exists						
No plan for implementation						
Strategy	Level 1	Notes	Level 2	Notes	Level 3	Notes
MFA	Multi-factor authentication is used by an organisation's users if they authenticate to their organisation's internet-facing services.	The Tree MFA will be enabled by Jan 2022	Multi-factor authentication is used by an organisation's users if they authenticate to their organisation's internet-facing services.	The Tree MFA will be enabled by Jan 2022	Multi-factor authentication is used by an organisation's users if they authenticate to their organisation's internet-facing services.	The Tree MFA will be enabled by Jan 2022
	Multi-factor authentication is used by an organisation's users if they authenticate to third-party internet-facing services that process, store or communicate their organisation's sensitive data.	Enabled for MS Office 365	Multi-factor authentication is used by an organisation's users if they authenticate to third-party internet-facing services that process, store or communicate their organisation's sensitive data.	Enabled for MS Office 365	Multi-factor authentication is used by an organisation's users if they authenticate to third-party internet-facing services that process, store or communicate their organisation's sensitive data.	Enabled for MS Office 365
	3rd party applications like Edsmart, AccessIT, Box of Books ect would require MFA. Possible through use of Azure Login Services (in use with other applications today).		Multi-factor authentication (where available) is used by an organisation's users if they authenticate to third-party internet-facing services that process, store or communicate their organisation's non-sensitive data.	3rd party applications like Edsmart, AccessIT, Box of Books ect would require MFA. Possible through use of Azure Login Services (in use with other applications today).	Multi-factor authentication (where available) is used by an organisation's users if they authenticate to third-party internet-facing services that process, store or communicate their organisation's non-sensitive data.	3rd party applications like Edsmart, AccessIT, Box of Books ect would require MFA. Possible through use of Azure Login Services (in use with other applications today).
	Multi-factor authentication (where available) is used by an organisation's users if they authenticate to third-party internet-facing services that process, store or communicate their organisation's non-sensitive data.		Multi-factor authentication (where available) is used by an organisation's users if they authenticate to third-party internet-facing services that process, store or communicate their organisation's non-sensitive data.		Multi-factor authentication (where available) is used by an organisation's users if they authenticate to third-party internet-facing services that process, store or communicate their organisation's non-sensitive data.	
	users can choose to opt out) if they authenticate to an organisation's internet-facing services.	MFA for the parents and students. Will require planning to initiate.	users can choose to opt out) if they authenticate to an organisation's internet-facing services.	MFA for the parents and students. Will require planning to initiate.	users can choose to opt out) if they authenticate to an organisation's internet-facing services.	MFA for the parents and students. Will require planning to initiate.
			Multi-factor authentication is used to authenticate privileged users of systems.	Administrator accounts require MFA for all systems with sensitive data	Multi-factor authentication is used to authenticate privileged users of systems.	Administrator accounts require MFA for all systems with sensitive data
			Multi-factor authentication uses either: something users have and something users know, or something users have that is unlocked by something users know or are.	Yes Password and Phone	Multi-factor authentication is verifier impersonation resistant and uses either: something users have and something users know, or something users have that is unlocked by something users know or are.	Yes Password and Phone
			Successful and unsuccessful multi-factor authentications are logged.	Yes with Azure Security logs	Successful and unsuccessful multi-factor authentications are centrally logged and protected from unauthorised modification and deletion, monitored for signs of compromise, and actioned when cyber security events are detected.	MFA is not required to login to the school Database System 'Synergetic'
Regular Backups	Backups of important data, software and configuration settings are performed and retained in a coordinated and resilient manner in accordance with business continuity requirements.	We have hourly backups kept for 48 hours. Daily backups kept for 30 days. Archive system keeping quarterly backups for 10 years.	Backups of important data, software and configuration settings are performed and retained in a coordinated and resilient manner in accordance with business continuity requirements.	We have hourly backups kept for 48 hours. Daily backups kept for 30 days. Archive system keeping quarterly backups for 10 years.	Backups of important data, software and configuration settings are performed and retained in a coordinated and resilient manner in accordance with business continuity requirements.	We have hourly backups kept for 48 hours. Daily backups kept for 30 days. Archive system keeping quarterly backups for 10 years.
	Restoration of systems, software and important data from backups is tested in a coordinated manner as part of disaster recovery exercises.	Random backups tested every Friday with all backups tested once per quarter.	Restoration of systems, software and important data from backups is tested in a coordinated manner as part of disaster recovery exercises.	Random backups tested every Friday with all backups tested once per quarter.	Restoration of systems, software and important data from backups is tested in a coordinated manner as part of disaster recovery exercises.	Random backups tested every Friday with all backups tested once per quarter.
	Unprivileged accounts can only access their own backups.	Unprivileged accounts cannot access backups.	Unprivileged accounts, and privileged accounts (excluding backup administrators), can only access their own backups.	Creation of a backup administrator account to only access backups planned for early 2023.	Unprivileged accounts, and privileged accounts (excluding backup administrators), cannot access backups.	Creation of a backup administrator account to only access backups planned for early 2023.
	Unprivileged accounts are prevented from modifying or deleting backups.	As above	Unprivileged accounts, and privileged accounts (excluding backup administrators), are prevented from modifying or deleting backups.	As above	Unprivileged accounts, and privileged accounts (excluding backup break glass accounts), are prevented from modifying or deleting backups.	No plan for this implementation.

A School's Perspective

Useful FREE Resources

- MXToolbox for blacklist monitoring
- GoPhish for free phishing exercises
- Haveibeenpwned for domain alerts for data breaches
- Joe Sandbox for payload detonation
- Qualys Community Edition for Vulnerability Scanning



A School's Perspective

Answers for Senior Leaders

1. Do we have effective Cyber Policies and a Security Program that aligns with our business and IT Strategy?
2. Have we identified our crown jewels: critical assets, infrastructure, and processes to support our business?
3. How are we protecting our critical assets and information?
4. Are we aware of the compliance and regulatory requirements related to our sector?
5. What are the biggest threats to our business?
6. In case of a cyber breach or ransomware, do we know how quickly our organisation can recover? Have we tested it?
7. Do we have a Cyber Assurance program? What is it covering?



A School's Perspective

Day zero of a data breach

- Don't panic
- Try to contain the incident
- Don't act alone
- Be ready for a lengthy journey
- Learn from the experience



Essential Steps to Secure School Data

James Lacey (CTRL Group)

- What are the essential steps a school should take to start securing their data security and how can they maintain their maturity moving forward?
- Building on Thomas' response, what could a school do in a data breach?
- What are the most important things schools should remember regarding their data security?



Q&A

- We will endeavour to get through as many questions as possible.
- Please add your question to the chat function in MS teams.
 - If you would like to submit your questions anonymously, please email emma@edsmart.com

Thank you

Thank you to all the attendees for your valuable time.

Thank you to James and Thomas for giving us their time, expertise and insights today

Please note: All attendees will shortly receive a data security resource pack to help with their cyber security, along with a recording of the webinar

