Student Data Privacy Consortium

December 2021 webinar
Safer Technologies 4 Schools (ST4S)
st4s.edu.au

Anthony Yaremenko, NSIP Program Manager
Acknowledgement of Country

I wish to acknowledge the Kulin Nation, Traditional Custodians of the land on which ESA’s offices are located, and pay my respects to Elders past, present and emerging.

I also acknowledge the Traditional Owners of the lands across Australia, their Elders, Ancestors, cultures and heritage.
NSIP

- Safer Technologies for Schools (ST4S) is coordinated by the NSIP team at ESA
- NSIP long-term members of A4L / SDPC
- NSIP board: CIOs from all States and Territories, Catholic, Independents and Federal Government
- NSIP - business unit of Education Services Australia (www.esa.edu.au)
- ESA - national not-for-profit company owned by the state, territory and Australian Government education ministers
- ESA - established by education ministers in 2010 to advance key nationally agreed education initiatives, programs and projects
Over 4,000 different applications in use at schools
Education Supply Chain

District

School A

School B

State & Federal Reporting

Software application 1

Software application 2

Software application 3

Personal information

Academic results

Health and wellbeing

Financial data

Sensitive data
Education Supply Chain

Can we trust Software application 1?

With what level of data?
Just email addresses?
What about health data?
What about financial data?
Who is liable / responsible if/when things go wrong?
People also ask

Which is an example of a supply chain attack?

A supply chain attack is a cyber-attack that seeks to damage an organization by targeting less-secure elements in the supply chain. ... The Target security breach, Eastern European ATM malware, as well as the Stuxnet computer worm are examples of supply chain attacks.


Supply chain attack - Wikipedia
“Ransomware is really taking hold of Education vertical incidents, and has been responsible for 80% of the Malware-related incidents, up from 48% last year”

“...Educational Services have the longest number of days in a year—28—where they had credential dumps run against them. The global median here is eight days. The overall number of credentials attempted is also one of the highest of all industries we analyzed for this year’s report...”

**Ransomware payments**

Hackers target NSW school online accounts in phishing campaign

Scam email tries to exploit Microsoft platform used by schools in bid coinciding with prime minister’s warning of wider cyber-attack

Catholic school in Australia falls victim to Cyber Attack

December 20, 2019  By IZOlogic  In Financial Malware, Phishing, Compromised Data

Private school’s lessons crashed by Zoom ‘bongers’

Two teens managed to access the Zoom

Hacker group threatens Newcomb Secondary College in Victoria

A high school has been hit by a cyber attack, with the criminals threatening to release information if the school doesn’t ‘co-operate’ within a week.

Anton Nilsson

NCA NewsWire  APRIL 28, 2021 5:41PM
What is ST4S?

An Australian framework for online education services to assess:

• Security
• Privacy
• Online Safety
• Interoperability

Provides a nationally consistent baseline for assessments across Australia
Key Outcomes for Vendors & Sector

• To increase awareness and raise the profile of security & privacy controls
• Clear guidance on what is expected of vendors and for classrooms regarding safer usage
• National baseline requirements that allow vendors to self-assess
• Feedback and support to vendors on areas requiring improvement
• Reduced administrative burden for vendors & education sector

• All contributing to improved student and school safety
• **Working Group:** Security and privacy experts from across the country. Meet monthly. Suggest framework updates.

• **Assessment framework:** Set of control questions with response options.
  
  *Eg What are the minimum encryption algorithms applied to protect all data in transit over networks, including encryption of data that is communicated between the user, web applications and system components (e.g. database systems)?*

• **Assessment tiers:** Not all products are equal. Data & functionality require higher/lower levels of controls. Tier 1/2/3.
  
  *Eg encrypting basic class details vs encrypting mental health records or financial information*

• **Non-compliant responses:** Important controls are required to be met and if not generate a ‘non-compliant’ (fail) result
Assessment Framework

Security
• Where is the live solution hosted?
• Is multifactor authentication used?
• How often are audit logs reviewed?

Privacy
• How can users request a copy of their data?
• Does the privacy policy comply with the Federal privacy laws?
• Are photos and contact details associated with a user?

Functionality & Education controls (10 +/- 20)
• What functionality is available (surveys, online meetings, remote access, screen share, chat, forums, commenting, file download/upload)
• In relation to <x> functionality, tell us about your controls (eg chat logs etc)

Interoperability
• What APIs are available to exchange data?
• What standards (incl. SIF, IMS) are supported?

All available in the ST4S Vendor Guide on www.st4s.edu.au
How does it work?

1. Vendors answer a set of control questions and are asked to upload evidence to support their response (e.g., privacy policy, security policy, incident response plan, etc).

2. Assessment team work with vendor to resolve any queries. Assessment team develop an understanding of the product, vendor develops an understanding of the assessment.

3. Draft report is developed and iterated.

4. Final report is signed-off and distributed to our CIOs and ST4S Working Group.
Sample product/service (Sample vendor)

Assessment outcome: Medium risk

The overall risk level is the highest risk level remaining after all available treatments have been applied.

### Service summary

<table>
<thead>
<tr>
<th>Version:</th>
<th>Paid – Latest</th>
<th>Review date:</th>
<th>18/05/2020</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tags:</td>
<td>Library management; Administrative support services; Booking systems.</td>
<td>Assessment Tier:</td>
<td>Tier 2</td>
</tr>
<tr>
<td>URL:</td>
<td><a href="http://www.sampleproduct.com.au">http://www.sampleproduct.com.au</a></td>
<td>Audience:</td>
<td>Staff and Students</td>
</tr>
</tbody>
</table>

**Purpose of use:** Sample product is a library management system. Modules include cataloguing, circulation, search, overdue notices, borrowers, reports and stocktake.

### Information assets and hosting

<table>
<thead>
<tr>
<th>Data hosting:</th>
<th>Onshore (in Australia)</th>
<th>Data classification:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service components (live solution, backup):</td>
<td>Onshore (in Australia)</td>
<td>✗ Non-personally identifiable information</td>
</tr>
<tr>
<td>Service provider staff location (support staff):</td>
<td>Onshore (in Australia)</td>
<td>✗ Personally identifiable information</td>
</tr>
<tr>
<td>Account holder data:</td>
<td>Onshore (in Australia)</td>
<td>□ Sensitive information</td>
</tr>
</tbody>
</table>

**Legal jurisdiction:** Victoria, Australia

**Parent/carer consent:**
- □ Student personal information is disclosed to register an account
- ✗ Student personal information is collected, used or disclosed through use of the service
- ✗ Student images, video, work and/or results are uploaded and published to the service
### Actionable risks and risk treatments

After conducting a comprehensive review, the following risks and associated treatments have been identified. The risk treatments listed are designed to reduce risk exposure. Users must adhere to all stated risk treatments when using this service. The risk level is that which remains after the listed treatments have been applied.

<table>
<thead>
<tr>
<th>#</th>
<th>Account management</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><em>Account management standards assess the Terms of Service for the service provider and user, including the data disclosed during account registration, consent requirements, and the policies and processes that apply to account termination, administrator control of accounts and generation of user profiles.</em></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Risk</th>
<th>Risk treatment</th>
</tr>
</thead>
<tbody>
<tr>
<td>PR3</td>
<td>- Complete only mandatory fields.</td>
</tr>
<tr>
<td>PR5</td>
<td>- Use anonymous and/or organisational details to replace personal information wherever possible.</td>
</tr>
<tr>
<td></td>
<td>- Do not use organisational passwords.</td>
</tr>
<tr>
<td></td>
<td>- Gain consent as per the Parent/carer consent section of this report.</td>
</tr>
<tr>
<td></td>
<td>- This service does not require users to enter complete and accurate information when registering accounts. Users should create accounts using anonymous and/or organisational details wherever possible.</td>
</tr>
<tr>
<td></td>
<td>Low</td>
</tr>
</tbody>
</table>

| PR8       | - When registering accounts, ensure users only enter the information specified in the Account Management section of this report. |
|           | Medium                                                                          |

<table>
<thead>
<tr>
<th>#</th>
<th>Usage conditions</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><em>Usage conditions vary based on the functionality available within the service. These conditions aim to reduce the risks associated with student safety, reputational damage, loss of intellectual property rights, and unauthorised or over-disclosure of personal, sensitive or organisational information.</em></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Risk</th>
<th>Risk treatment</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Risk level</td>
</tr>
<tr>
<td></td>
<td>Low</td>
</tr>
</tbody>
</table>
Journey so far... 2019-2021
Statistics

- 187 assessment criteria
- 23,000+ security and privacy controls evaluated
- 4 major framework updates
- 149 detailed reports delivered
- 28 members of ST4S Working Group
- 6 hours average time to complete
- 582 days longest assessment
- 251 Outcomes

ST4S
Wide Range of Vendors
Findings

Encryption on the wire - TLS/SSL (S1, S3)
- TLS version & SSL Cipher Suites
- BaaS – Google Firebase, AWS Amplify, move to ‘serverless’
- Cipher suites configured on the server
- As SSL/TLS is configured ‘server side’ BaaS basically hides away server settings
- Challenging for vendors to adjust SSL ciphers and sometimes the TLS versions
- Looking at working with security teams and possible revisions to assessment criteria (ie set of known and supported BaaS’s)

Data Segregation – S4
- Evolving space: physical tin, logical segregation, cloud
- Focus more on vendor APIs and communication with database
- Are well developed frameworks in use (Nest.JS, Laravel, LoopBack etc) or using serverless eg AWS API Gateway, Authy etc.
- Expect this space to develop
Findings

Increase in Artificial Intelligence and Insights
• Increase in apps offering data insights/analytics (Billy didn’t do so well in maths and is below the 5% of his cohort)
• Data handling and data ethics

Increase in Health and Wellbeing Apps/Services
• Increase in health and wellbeing type apps coming through (especially with covid).
• ‘Duty of care’ issues emerging eg if a student is repeatedly hitting the ‘sad face’ and not the ‘happy face’ for 3 months on a health check-in mobile app, does that establish an actionable concern? What should the school do? What should the product do in terms of alerts etc?
Learnings

Non-participating vendors
• Vendors who were invited to participate but did not respond
• Vendors who did not want to participate
• Developed non-participating reports
• Created trouble 😞

Large vendor companies
• Separate sales, security, privacy, legal, sales/marketing silos
• Teams distributed across the globe
• Applications that require underlying platform
• Responses shift based on last area to review
• Process may halt at 99% completion
• Complex +++

Small-Medium vendor companies
• Keen to please
• Time & resource sensitive
• May over-commit
Readiness Check Launched

www.st4s.edu.au/readiness-check

- Now the first step for all vendors
- Critical subset of full assessment criteria (~40 criteria)
- Provides instant feedback to vendor
- Vendors can complete over multiple sessions and take multiple attempts
- Submit when ready
- Working Group then prioritise for full assessment
### ST4S Readiness Check Results

**Ready Status**: Not Ready for ST4S Assessment

**Tier**: Tier 1

#### Detailed Results:

<table>
<thead>
<tr>
<th>Item</th>
<th>Question</th>
<th>Response</th>
<th>Minimum Required</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>S1</td>
<td>What are the minimum encryption algorithms applied to protect all data in transit over networks, including encryption of data that is communicated between the user, web applications and system components (e.g. database systems)?</td>
<td>Encryption: DES, RC4; Hashing: Message Digests (MD to MD5), RIPEMD-128 or above, SHA-1, SHA-256, SHA-384, SHA-512; Digital Signatures: DSA (1024) or RSA (1024); Key Exchange: DH (1024) or RSA (1024); Protocol TLS 1.1 or below</td>
<td>The minimum requirement for a Ready outcome is: Encryption: AES 128 or above only (AES 256 recommended), Hashing: SHA-256 or above only (SHA-384 recommended), Digital Signatures: DSA (2048) or ECDSA (256) or RSA (2048); Key Exchange: DH (2048+), ECDH (P-256) and/or RSA (2048); Protocol: TLS 1.2 or above only (TLS 1.3 recommended) (T1)</td>
<td>Not Ready</td>
</tr>
<tr>
<td>S3</td>
<td>If customer data is uploaded to the service using a mechanism such as encrypted USB, SFTP, Secure API, etc., what are the minimum encryption methodologies applied?</td>
<td>Encryption: AES 128 GCM/CCM, CHACHA20 POLY1305 or above only (AES 256 GCM/CCM recommended); Hashing: SHA-256 or above only (SHA-384 recommended); Digital Signatures: DSA (2048) or ECDSA (256) or RSA (2048); Key Exchange: DH (2048+), ECDH (P-256) and/or RSA (2048); Protocol: TLS 1.2 or above only (TLS 1.3 recommended) (T1)</td>
<td></td>
<td>Ready</td>
</tr>
</tbody>
</table>
But......

... we would all benefit from an international approach...
Apache Log4j2 library vulnerability (CVE-2021-44228) and Conti ransomware incidents

NCSA- 3 ALERT: A cyber threat that requires immediate monitoring, analysis and strategic coordination....

**ST4S Controls:**

T1 - Does your organisation have an implemented continuous monitoring plan ...
T2 - Does your organisation use a centrally managed approach to patch or update applications...
T3 - Are security vulnerabilities in operating systems, applications, drivers and hardware devices assessed as extreme risk patched or mitigated within 48 hours of being identified?
T7 - When a data breach occurs, are affected customers and/or organisations notified as soon as possible after a data breach is discovered and given all relevant details?
S1: What are the minimum encryption algorithms applied to protect all data in transit over networks, including encryption of data that is communicated between the user, web applications and system components (e.g. database systems)?

<table>
<thead>
<tr>
<th>ST4S Control</th>
<th>AU ISM</th>
<th>NIST 800-53 rev4</th>
<th>ISO 27002</th>
</tr>
</thead>
<tbody>
<tr>
<td>S1</td>
<td>1139</td>
<td>SC-8 Protect the confidentiality /integrity of transmitted information.</td>
<td>10.1.1 13.2.3 14.1.2 14.1.3</td>
</tr>
</tbody>
</table>
NIST Cybersecurity Framework

• Flexible framework that can be applied to any organization
• References NIST 800-53, COBIT, ISO 27001:2013
  • https://www.nist.gov/cyberframework

https://www.nist.gov/cyberframework
NIST Cybersecurity Framework

5 keys functions
- Identify
- Protect
- Detect
- Respond
- Recover
NIST Cybersecurity Framework

- Identify critical enterprise processes and assets
- Document information flows
- Maintain software and hardware inventory
- Establish cyber policies including roles and responsibilities
- Identify threats, vulnerabilities, and risks to assets

Develop an organizational understanding to manage cybersecurity risk to: systems, assets, data, and capabilities.
What should an education CSF look like?

• Work needed to determine scope of controls suitable for education context
• What is in scope?
• What is out of scope?
• Are there additional considerations?
  • Adults & children
  • Consent
  • Functionality: Information exposure Functionality: Communication
  • What is reasonable for education vendors?
CSF: Identify – Asset Management

ID.AM-1: Physical devices and systems within the organization are inventoried

Q6. Does the vendor have a documented and implemented IT Asset management process including:

• An ICT equipment and media register that is maintained and regularly audited;
• A directive that ICT equipment and media are secured when not in use;
• The secure disposal of ICT equipment and media (including sanitising/removal of any data or secure destruction/shredding)?
A Way Forward:

1. Agree we have a shared problem worth solving
2. Establish an international Project Team (A4L SDPC)
3. Identify a suitable, recognised control set
4. Work through the control set (relevancy, develop control questions and responses)
5. Develop a standardised assessment approach
6. Develop standardised assessment reporting
7. Develop a results sharing process
8. Maintain the framework
Thank You & Questions
DataHubs

The MA DataHub:
Real-time statewide data integration and privacy management for SEAs and Districts

Access 4 Learning Community
Powered by: SIF
I finally figured out a way to make our computer secure.