Safer Technologies
4 Schools

Addressing Security and Privacy
Anthony Yaremenko
Program Manager
National Schools Interoperability Program (NSIP)
Business unit of Education Services Australia (ESA)

Anthony.Yaremenko@nsip.edu.au
Acknowledgement

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.
Who are ESA-NSIP?

- **Education Services Australia** is a national not-for-profit company owned by the state, territory and Australian Government education ministers.

- ESA was established by education ministers in 2010 to advance key nationally agreed education initiatives, programs and projects.

- **National Schools Interoperability Program (NSIP)** established in 2010 targeting standards in digital learning infrastructure and interoperability, and are a business unit of ESA.

- The ESA NSIP program is operationally informed by the NSIP Steering Group made up of:
  - CIOs from each Government State & Territory
  - Catholic & Independent sector representation
  - DESE, ACARA & ESA

- NSIP manage the SIF-AU data model, NAPLAN Online data specifications, ST4S, HITS and other data tools and services.
What is ST4S?

An assessment of online services used in the Australian & New Zealand Education Sector against agreed criteria for:

• Security
• Privacy
• Functionality / Online Safety
• Interoperability
What is ST4S?

www.st4s.edu.au

A National Privacy and Security Initiative for Digital Products in K-12 Education

The Safer Technologies 4 Schools initiative is a standardised approach to evaluating digital products and services used by schools across Australia against a nationally consistent security and privacy control framework.

About the Guide

The ST4S vendor guide concepts the ST4S assessment framework and provides guidance and best practice regarding:

- The assessment process and results
- The questions included in the ST4S assessment questionnaire and the minimum acceptable responses
- To be released under any standards
- The criteria used to determine a compliant, non-compliant response, with criteria being repeatable, measurable, and marketable across the country
- The risk prioritisation of products and services based on assessment results
- How the assessment results will be shared with participating member organisations.
Security
How is data encrypted on the wire?
Are backups in place and are the backups actually tested?

Example
T6. Does your organisation have a formal, documented and implemented incident response plan which requires security, privacy and online safety incidents to be:

• Investigated;
• Remediated; and
• Recorded in a register with the following information at a minimum:
  o Date incident occurred;
  o Date incident discovered;
  o Description of the incident;
  o Actions taken in response to the incident; and
  o Name of person to whom the incident was reported?
Coverage

Functionality / Online safety
What functionality does the product offer?
Are there reasonable controls in place?

Example
PF6. In relation to the online meeting, video conference, audio conferencing and/or livestreaming functionality available within the service, select all that apply:

A. Access to sessions can be made available to the public
B. Access to sessions can be made private (e.g., access to sessions is invitation only)
C. Participant details can be displayed to all session participants
D. Participants can be displayed with de-identified/anonymous details or kept private
E. Sessions can be recorded and made available to the public
F. Sessions can be recorded and made private (e.g., participants only)
G. Audit logs are not kept for all recordings
H. Participants are not notified if they are participating in a recorded session (e.g., via on screen prompt)
Privacy
How can users request a copy of their data?
Does the privacy policy comply with Privacy Principles?
Are photos and contact details associated with a user?

Example
PR3B. What mandatory information is collected by the service when students generate their own accounts for this service?
Interoperability
What APIs are available to exchange data?
What standards are supported?

Example:
Have custom APIs been developed for integrating with the product? If so please describe these and provide technical documentation detailing the API (e.g., REST based, JSON payload, etc.)
1. Vendor completes Readiness Check

2. Vendor prioritised

3. Vendor completes full assessment

Open to all vendors 24/7

Working group meet monthly

Collaborative assessment
Evidence documents
Technical checks
Coherence
Safer Technologies 4 Schools Assessment

Sample product/service (Sample vendor)

Assessment outcome: Medium risk

A non-compliant assessment outcome means the service does not meet the minimum requirements for information security, privacy, and/or online safety.

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>
<tr>
<td>Purpose of use:</td>
<td>Sample product is a library management system. Modules include cataloguing, circulation, search, overdue notices, borrowers, reports and stocktake.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Information assets and hosting

<table>
<thead>
<tr>
<th>Data hosting:</th>
<th>Onshore (in Australia)</th>
<th>Data classification:</th>
<th>Non-personally identifiable information</th>
</tr>
</thead>
</table>
Progress

- Over 200 products/services assessed
- 99% of vendors want to do the right thing
- 30+% of vendors make changes to improve their offerings
- Google, Apple, Microsoft, Adobe +++other products/services
1. There are all sorts of vendors

Small, medium, large
Distributed, complex, simple
Learnings

Introduced **ST4S Readiness Check** [https://st4s.edu.au/readiness-check/](https://st4s.edu.au/readiness-check/)

- Critical subset of the full assessment criteria
- Provides information and standards to support vendors in improving their products and services
- Vendors can self-assess at any time

- Highlights significant gaps early in the process
- ‘Ready’ vendors are then prioritised by the ST4S Working Group for a full assessment
2. There are all sorts of products and services

Old, new
Different approaches to problems & controls
Changing functionality
Learnings

- Regular communication with vendors
- Changes to tool
- More help text
- Additional functionality questions

- Collaboration, collaboration, collaboration
3. Threats keep evolving
What to focus on? Can’t protect everything…

- Underlying security standards updated ~monthly
- Working group - share learnings and monthly meetings
- Get participants to sign NDAs
- Share more
- Detail impacts
- Detail controls that worked
- Detail controls that didn’t
4. Standardisation in this space is tricky
Learnings

- Variety of opinions (diverse group)
  - Deny everything
  - Allow everything
- Use reference standards – don’t make things up
- 80% is good enough. Land on a workable path forward.
5. Communication

*Internally and to market*
Learnings

Communications to market
  • Competing, overlapping requests: vendor confusion
  • Duplication of effort
  • Open-channels, advocate for vendors and education stakeholders

Communications to schools
  • ‘Safe to use’?
  • Accessing reports
6. A range of key issues repeat
Learnings

- TLS/SSL versions and support for out-of-date SSL and TLS 1.0 (multiple URLs)
- Vendor performing internal security testing as part of development practices
- Relocation or expansion of where data is processed/accessed from
- Downstream visibility of data sharing and controls

- Backups are critical, need to be tested and reliable.
- Patching. Manage and apply automagically if possible.
- Restrict admin privileges.
- Multi-factor authentication.
7. Effort vs Reward
Learnings

• Validating a vendor submission is hard
  • Did they understand the question?
  • Did they understand the response options?
  • Did the right person answer?
  • Does the answer contradict other answers or evidence?
• Validating a vendor’s product and the vendor organisation is even harder
• What is a vendor comfortable in sharing? What is their investment? For what benefit?
• Is this a detailed audit? What is the cost/effort to complete an assessment?
War stories

1. The industrious student
2. The super administrator
3. The misconfigured teacher
Next steps...

**Catalogue**
- Number of States/Territories, Catholic and Independent sectors have limited means of securely communicating with schools
- Establishing a searchable catalogue
- Search on product tags/types/outcomes
- Integrate with local directories (SSO)
Next steps...

**Product badging**
- Encourage vendors to participate
- Reward for effort and product improvements
- Strict terms around usage (outcome, time based components)
Thank-you for your time ☺

Anthony.Yaremenko@nsip.edu.au