12-7-2022

Education Cybersecurity Assessment Tool: A cybersecurity self-assessment tool for the Australian K-12 sector

Mason Torres
Curtin University, mason.torres@postgrad.curtin.edu.au

Antony Mullins
Curtin University, antony.mullins@cbs.curtin.edu.au

Nik Thompson
Curtin University, nik.thompson@curtin.edu.au

Education Cybersecurity Assessment Tool: A cybersecurity self-assessment tool for the Australian K-12 sector

Full research paper

Mason Torres
School of Management
Curtin University
Perth, Australia
Email: mason.torres@postgrad.curtin.edu.au

Antony Mullins
School of Management
Curtin University
Perth, Australia
Email: antony.mullins@cbs.curtin.edu.au

Nik Thompson
School of Management
Curtin University
Perth, Australia
Email: nik.thompson@curtin.edu.au

Abstract

The K-12 education sector is a unique sector that continues to be the target of cyber security threats. A common misconception is that large organisations are the main target of hackers; however, the combined attack surface of K-12 schools can be greater than large organisations and small, medium enterprises (SMEs), given the number of students. Schools are tasked with protecting against cyber threats; however, existing frameworks are often complex and inappropriate for the education sector. This paper presents a novel cybersecurity self-assessment tool for Australian K-12 schools to assess their compliance with the National Institute of Standards and Technology – Cybersecurity Framework (NIST CSF)

Keywords cybersecurity assessment tool, primary and secondary education, K-12 education, cybersecurity frameworks, NIST CSF

1 Introduction

The state of cybersecurity in schools is a constantly growing area of interest for both attackers and those responsible for protecting data, IT assets, and services. A report on the Top Trends Impacting K-12 Education in 2022 outlines the costly lack of attention and resources cybersecurity has received, promoting an increased interest from cybercriminals (Williams et al. 2022). Lack of resourcing and attention shows schools are easy targets to penetrate, often being slow to react and not in possession of the required expertise to address cybersecurity threats. The report shows an increase in ransomware attacks and outlines technical action plans to address the associated risks. However, it should be noted that these actions are all technical and do not address human factors and implications. It is also noted that the other trends within the K-12 education sector, such as Digital Learning Environments, Learning Insights/Analytics, and Adaptive Learning, all utilise student data and require advancement in the trust and security of that data.

Richardson et al. (2020) note the increase in cyber-attacks, data breaches, and ransomware in schools is due to human-enabled errors comprising; flawed decision-making through lack of training and threat perception, poor organisational security culture, spear phishing, social engineering, malware, noncompliance, poor policies, and technology-introduced vulnerabilities (Nobles 2018; Richardson et al. 2020). Further, "the human factor is the underlying reason why many attacks on school computers and systems are successful … the uneducated computer user is the weakest link targeted by cybercriminals using social engineering" (Richardson et al. 2020, p. 27). Additionally, the authors state that security vulnerability is attributed to employees' lack of awareness (Richardson et al. 2020; Safa et al. 2015) and increased use of internet services. Attackers perceive schools as easy targets who cannot keep up with novel or zero-day attacks and provide a gateway to more significant opportunities through the number of potential targets. Clearly, K-12 schools require direction, frameworks, and self-assessment tools, to help mitigate cyber threats, primarily due to the unique attack scope of K-12 schools, which includes teachers, staff, and student users ranging from 3 years to 18 years old.

2 Security Education Training and Awareness in K-12

Training programs have been developed to address the issue of cybersecurity awareness and culture within schools; these programs provide methods for engaging with students and identifying challenges with their implementations. Howard (2021) developed a training program aimed at reducing problematic cyber practices for middle school students; they discuss the importance of cybersecurity and its need to be embedded in the school's culture and curriculum, emphasising the need to go beyond awareness alone. Howard (2021) further recognises that cybersecurity should not be a 'one-time' lesson but rather a continued activity that engages and encourages students to take an active role in protecting their personally identifiable information (PII). To address the 'one-time' lesson issue, Howard (2021) recommends implementing a quarterly lesson approach, with each lesson focusing on a specific area, such as; PII training, phishing, social media privacy and digital footprints. Furthermore, each lesson should provide a range of discussion topics, videos, handouts, and a quiz or discussion at the end of the lesson to assist teachers in delivering cybersecurity content without overly complex lesson plans or scripts that are often intended to be delivered to adults. Yan et al. (2021) developed a questionnaire targeted at K-12 students and teachers, aiming to understand the intuitive and rational judgement of cybersecurity risks of participants who attended a GenCyber summer camp in the USA. The GenCyber camp aims to increase interest in cybersecurity careers, develop cybersecurity knowledge, and improve cybersecurity teaching. The intuitive questions were quick-fire and designed to be answered quickly with little effort or conscious deliberation and could be attributed to past experiences and emotions. In contrast, the rational questions required careful consideration and thought, representing deliberate, effortful, and rule-based thought. The study found that students failed to demonstrate any improvement in intuitive or rational judgement scores before and after the camp. Teachers, however, did demonstrate improved rational and intuitive judgement after the camp; indicating that the training was more effective due to their increased awareness and security experience.

Nguyen and Bhatia (2020) focused on higher education and devised an awareness and training model to help mitigate social engineering risks and increase the preparedness across three human domains (students, faculty, and employees). The awareness model targets each human domain and provides physical (pamphlets, posters, newspapers, and flyers), and electronic (public monitors, digital publications, message boards, and email) distribution of materials tailored to the human domain and their respective responsibilities. The awareness model constitutes a passive learning method, given that no formal engagement is required. In contrast, the training model is comprised of active learning where the users physically participate in a cybersecurity program directed by a professional, further suggesting

that the training should also be bound by refresher courses delivered tri-annually and via electronic methods to promote continued learning. The awareness and training model reflects a growing concern in higher education on social engineering attacks' impact, as the expansion of technical cybersecurity solutions has forced attackers to target the human aspect of computing.

3 Cybersecurity Frameworks and Tools

Cybersecurity frameworks go a long way to help mitigate cybersecurity threats, and governments and regulatory bodies often develop complex frameworks. Hussain et al. (2020) discuss challenges and emerging threats through a review of 33 research articles; categorising cybersecurity into two components: governance and risk management, and culture and awareness. Governance and risk management often utilise a framework to provide the backbone for assuring cybersecurity, thus highlighting how important it is to be aware of frameworks and how to best utilise them. Whereas culture and awareness play an important role as issues arise from a lack of cultural understanding among users, particularly those with varying system access levels. Hussain et al. (2020) identify that those who are aware of their impact on cybersecurity often ignore rules and are, therefore, ignorant of the significance of cybersecurity. Their limited study identifies governance as the most significant impact on cybersecurity, while culture and awareness were the least significant; furthermore, their study identifies the challenges and issues for cybersecurity and supports the notion that scepticism and lack of awareness need to be addressed. The authors suggest that the application of technical controls is insufficient to address the perception of cybersecurity challenges and how to solve them. Instead, governance should be well-defined and address each cybersecurity function: identify, protect, detect, respond and recover, as depicted in the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF) (National Institute of Standards and Technology 2018).

Through a systematic review of 16,416 academic works related to cybersecurity standards, Syafrizal et al. (2020) identified 250 cybersecurity frameworks and standards currently in use; this was refined to reveal 33 unique and well-understood cybersecurity standards and frameworks that are general and can be used across different businesses, organisations, companies, and governments. However, most frameworks and standards are specific to local regions or industries. Furthermore, industry standards are typically associated with a higher degree of stringency and complexity when needed to meet regulatory compliance. They include standards like HIPAA, PCI-DSS and ISA/IEC 62443, related to medical/personal information, the payment card industry, and industrial automation/control systems, respectively. The NIST CSF, however, "enables organisations - regardless of size, degree of cybersecurity risk, or cybersecurity sophistication – to apply the principles and best practices of risk management to improving security and resilience" (National Institute of Standards and Technology 2018).

A Western Australian study into the use of NIST CSF within a local government organisation was conducted with a domain focused assessment tool targeted at three levels of participants; executive, management and technical (Ibrahim et al. 2018). The rationale of the targeted audience was to ascertain an organisation-wide understanding of cybersecurity risk across technical and non-technical components of security. Questions within the assessment tool were derived from the NIST CSF and supplemented with additional questions to help identify a baseline. After the assessment, the business was graded Compliant, Partially Compliant, or Non-Compliant. The author's findings allowed for identifying gaps within the organisation's security posture and how the gaps relate to specific people, processes, and technology. Furthermore, the authors discuss the use of other industry cybersecurity frameworks applicable to various business sectors and organisation sizes, arguing their challenging nature regarding self-assessment. NIST CSF, in this regard, provides a "High-level abstraction of related frameworks" (Ibrahim et al. 2018, p. 5178) and includes references to other related frameworks should the organisation wish to implement them.

3.1 Cybersecurity Assessment Tools

The target audience for frameworks and standards can be categorised into audience-specific and across-the-board (Azmi et al. 2018). Typically, large organisations are suited to implement and evaluate against frameworks, given the recognition of the importance of cyber security and their ability to act on it. However, smaller organisations may not possess the same ability, Emer et al. (2021) developed a cybersecurity assessment model for small and medium-sized enterprises targeting industry 4.0 technologies. Industry 4.0 technologies comprise of cyber-physical systems (CPS), the internet of things (IoT), automation, human-machine interaction (HMI) etc. (Rauch et al. 2020). The Emer et al. (2021) assessment tool is structured around five steps: 1. Listing and grouping cybersecurity concepts, 2. Definition of concepts' maturity levels, 3. Setting of concepts' current and target status of implementation. 4. Setting of concepts' importance, and 5. Derivation of strategies for implementation

measures. The author's approach is consistent with developing a new framework, while advantageous for specific industries, it requires significant effort and often overlaps existing well-established frameworks. Similarly, Carías et al. (2021) developed a web-based assessment tool utilising a preliminary framework grouping together common domains and actions from an analysis of 41 documents related to cyber resilience. However, simply using standards and frameworks like NIST CSF, MITRE Cyber Resiliency Metrics, ISO 27001, and the Department of Energy Cybersecurity Capability Maturity Model is often not sufficient, as they cannot target specific audiences (industry), and fail to identify the current state, improvements and ability to prioritise actions.

The application of cybersecurity assessment tools is often limited in the education sector. Garcia and Bongo (2022) studied students' and teachers' levels of cybersecurity awareness across their knowledge and practices. A questionnaire was developed to assess participants building on the NIST CSF as a foundation. NIST CSF was used as it integrates industry standards and best practices in a common language and provides an organisation with a risk assessment across threats, vulnerabilities and impacts while also providing measures for reducing risk and making improvements. Their findings show that 36% of students and 17% of teachers scored below the passing score regarding knowledge. At the same time, their practices relating to authentication, activities on social media, and system and browser updates were occasionally practised by students and often practised by teachers. Garcia and Bongo (2022), recommend increasing cybersecurity training and awareness for students and teachers to avoid becoming cybercrime victims; however, the study only focussed on a subset of the controls and recommendations depicted in NIST CSF. Therefore, an opportunity exists to expand this prior work, as a questionnaire alone does not integrate into an overall NIST CSF assessment.

4 Cybersecurity in Education

Identifying the inadequacy of information security management practices in K-12 environments, despite their ongoing acquisition and ownership of information, was the focus of Nyachwaya (2013). Their findings indicate a positive relationship between preventative and deterrent measures and information system security effectiveness; also, identifying greater senior management support employed better preventative measures; while those who spent more on IT budget used better preventative and deterrent measures. Additionally, only 41% of respondents recognised IT managers as leaders/decision makers; clearly undervaluing the IT manager role. While 70% of respondents identified four types of system users - faculty, administrators, non-teaching staff and students. Finally, 80% of the respondents understood the importance of schools using IT systems to aid in "finance, academic record operations, student assessment and grading, student attendance, library services, food services, special education pupil services, human resource services, and facilities management." (Nyachwaya 2013).

There is growing interest and research in security within primary and secondary education. Brown (2016) highlights the effectiveness of security elements within other industries while identifying the gap within the K-12 education sector, recognising the importance of technical and non-technical controls and their effectiveness concerning confidentiality, integrity, and availability. Brown's (2016) research examined how IT departments perceive the factors that go into a security framework, thus enabling an improvement on their deficiencies. The findings of the study identified adherence to compliance, annual IT budget for staff training, and time spent on systems security maintenance as the only indicators affecting security in K-12. Additionally, Brown (2016) recognised that costs associated with security hardware, software and maintenance do not significantly impact breaches on security; furthermore, they noted the lack of confidence that IT staff have in their security assets when attempting to prevent attacks.

Paakki (2019) explores the use of Information Assurance Technologists within K-12 organisations utilising the strategies and learning from other industries and organisations to aid in the implementation in the K-12 environment. The findings of the study indicated that 100% of respondents understood the need to comply with laws and regulations; 90% indicated a culture of security as a requirement to deliver adequate security; 90% utilise the security frameworks NIST CSF with varying use of other frameworks like CIS, HiTrust and ISO 27001 due to compliance with laws and regulation. Furthermore, 50% of respondents use managed security service providers to augment their security teams; While 80% report a positive use of auditors to drive the security roadmap and improve security posture and culture. The themes identified include laws and regulations, utilising internal and external auditors, and the need for a strategy that promotes security culture, frameworks, and augmenting information security teams.

Cybersecurity standards and frameworks are well documented and published, albeit occasionally behind a paywall, such as ISO27001. These standards and frameworks often require specialised skills, knowledge and resources to apply to the nuances of a given business (Carías et al. 2021). Cyber resilience in the small and medium-sized enterprises (SME) was the focus of Carías et al. (2021), reviewing 41 documents to establish their impact on cyber resilience operationalisation. The 41 documents were compared on their ability to "determine their current cyber resilience state, define improvement actions and prioritise them" (Carías et al. 2021, p. 9). The authors further note that for a tool to be ideal for SMEs, it requires the following four characteristics, which can also be incorporated into the k-12 assessment tool.

- Audience: Defined as SME.
- Self-Assessment: Ability for the SME to assess their current state.
- Maturity model: A progressive or hybrid model that represents the simple progression of characteristics, indicators, attributes, or patterns.
- Prioritise: Prioritisable actions to enable effective operationalisation.

A novel education-specific K-12 Cybersecurity Protection Framework (K-12 CPF) has been developed to aid in bridging the cybersecurity gap between a school's business mission, objectives, technical issues and risks (Kamaludeen et al. 2020). The authors use NIST CSF as a foundation and incorporate components from ISO 27001/27002, CIS and COBIT 5 to provide schools with cybersecurity, cyber safety, and privacy standards. However, the K-12 CPF fails to consider the student's and teaching staff's perspectives regarding training and self-assessment, and also lacks a tool to facilitate the processes defined in the framework. Furthermore, Qusa and Tarazi (2021), proposed a framework to raise cyber awareness amongst high school students using gamification; however, the framework recognises the importance of the human factor but does not integrate with existing, proven cybersecurity frameworks.

In lieu of guidance for K-12 education, the Australian Federal Department of Education (DoE) provides guidance for implementing cybersecurity strategies in universities. They identify the Commonwealth Information Security Manual (ISM), National Institute of Standards and Technology Cybersecurity Framework (NIST CSF), and ISO 27001 as suitable security control frameworks. They recommend that universities implement a well-developed cybersecurity strategy to align or incorporate one of these frameworks (Department of Education 2022), given cyber security is "a whole-of-organisation 'human' issue, with a strong emphasis on a positive security culture" (Department of Education 2022). DoE recognises that cyber awareness and security culture should consider; different groups of users; differing levels of university structures; cybersecurity challenges and solutions through the lens of users, not just technology, including user-centric design principles when developing and implementing safeguards; collective and individual responsibility; and measurement of shifts in user behaviour and other metrics to demonstrate progress. They also provide methods to encourage cybersecurity, one of which is through "short courses for technical and cultural education for internal use across the sector. This includes potential gamification of aspects of cybersecurity" (Department of Education 2022).

A study by IBM shows that 95% of cybersecurity incidents are human-enabled, citing "human error" as a disheartening and contributing factor (IBM 2014; Nobles 2018; Richardson et al. 2020). Human error factors include lack of awareness, negligence, carelessness, inability, and non-involvement of employees, which are the most significant security vulnerability (Richardson et al. 2020; Safa et al. 2015). Gyunka and Christiana (2017) further label humans as the most vulnerable link in cybersecurity. Clearly, training cyber users to combat cyber threats is paramount. Caballero (2017) provides a Security Education, Training and Awareness program (SETA) for designing, developing, and delivering program components to their explicitly targeted user base. These methods within SETA are targeted at organisations, and their employees through a top-down approach with management provided support. The design phase identifies the topic areas, e.g., password security, mobile device security, business communications and related content, which may take the form of computer-based training, phishing awareness emails, video campaigns, newsletters etc. Following this, the implementation and delivery phases identify the scope, audience, motivation, and administrators of the program while also delivering the content in a manner that is easy to use, scalable, and accountable. The potential impact of human error drives the need for self-assessment tools instead of solely relying on complex frameworks and training programs.

5 Education Cybersecurity Assessment Tool

There is a growing trend toward online assessment tools aimed at helping small to medium-sized enterprises and even schools adopt cybersecurity best practices, training, and awareness. Table 1 lists various assessments and resources available for K-12 schools that focus on adopting technical tools to mitigate risk; however, many are vendor-centric, do not approach the human factor of cybersecurity, or solely focus on student online safety. It should be noted that tools that reference the NIST CSF controls do not provide methods for implementation in school environments; there are no directions for how the control should be implemented and any impact it may have on students and staff. Similarly, the NIST CSF assessment tool developed by NIST has been deprecated and is no longer maintained; in the case of Apple Mac OS, it no longer runs on modern operating system versions.

Website	Country	Supplier	Aligned Framework
https://360safe.org.uk/	UK		
https://www.k12six.org/essential-cybersecurity-protections	USA		
https://k12cybersecure.com/resources/k-12-cybersecurity-self-assessment/	USA		NIST CSF
https://cyber.org/standards			
https://www.vmware.com/au/solutions/industry/education/k12/education-cybersecurity.html		Vendor	
https://www.cosn.org/edtech-topics/cybersecurity/	USA	Vendor	
https://www.fortinet.com/solutions/industries/education/k12		Vendor	
https://managedmethods.com/		Vendor	NIST CSF
https://www.nist.gov/cyberframework/nist-cybersecurity-framework-csf-reference-tool		Government	NIST CSF

Table 1. K-12 cybersecurity assessments and resources

To address the above concerns and for schools to successfully mitigate cyber threats, they need the ability to align to well-known and regarded industry frameworks efficiently. Currently, no assessment tool adequately assesses schools' compliance against a cybersecurity framework, nor do any tools aid in the implementation of the frameworks' controls with respect to the school environments and their unique challenges. To achieve this, we focus on NIST CSF as it is generalisable and provides a solid underlying structure, categorising its controls into technical and non-technical components. We developed an online assessment tool that allows IT and security staff to assess their organisation's compliance with the NIST CSF. As IT staff progress through an online assessment assessing their compliance against the technical controls, they can elect to assign constituents to specific controls; this triggers a user-based assessment for the specific constituent and the targeted control. The user-based assessment is a specialised online tool that addresses the human factor and aims to improve training and awareness, while also being measurable from a management perspective. The content in the user-based assessment is tailored to the comprehension of the target audience.

For example, when assessing NIST CSF control '*PR.DS-5: Protections against data leaks are implemented*' we may involve two constituent groups: year eight students and business staff. Through the online user assessment tool, the year eight students will be introduced to the importance of retaining and storing data in a manner appropriate to their comprehension. In contrast, business staff will be introduced to the importance of keeping PII and business-critical data safely stored on corporate-managed devices. A short questionnaire follows to test the users' knowledge; allowing IT staff to assess their school's compliance at a technical level while end users become more educated and aware of their involvement with cybersecurity.

Not all controls will necessarily have assessments for students as their scope, involvement and direct impact may be very limited. The online assessment tool, across all its components, will help improve schools' overall cybersecurity posture through the following:

1. **Training and awareness**. Each constituent (students, teachers, business staff, leaders, and privileged users) will have tailored learning activities with a knowledge check that is recorded against a school's organisation assessment and its related control.
2. **Implementation of NIST CSF controls in K-12.** Implementation guidance will be provided for NIST CSF controls relating to implementation challenges within school environments – across technical and non-technical components.
3. **Compliance with the framework.** Progress of NIST CSF assessment is tracked in near real-time, reported, and allows for continued progress over time.

The assessment tool is an online browser-based application written using the modern React library, allowing for access anywhere with an internet connection and modern browser, eliminating the need for users to install specialised software. The backend service that provides the functionality to complete the online assessment allows for analysis of assessments across individual schools and at a system level providing insights and comparisons across demographics. The report component of the online assessment visualises compliance against the framework's technical and non-technical controls. It allows schools to track progress over time while also allowing them to prioritise their cybersecurity efforts based on their current assessment. Aggregated results from other school assessments provide insights into the overall prioritisation of controls within the education sector. Technical controls that may have a detrimental impact on end users can be documented using this aggregated data, and guidance can then be developed on how to best implement the control in primary and secondary education environments. Figure 1 shows the components of the assessment tool and how the organisation assessment relates to the individual user-based assessment.

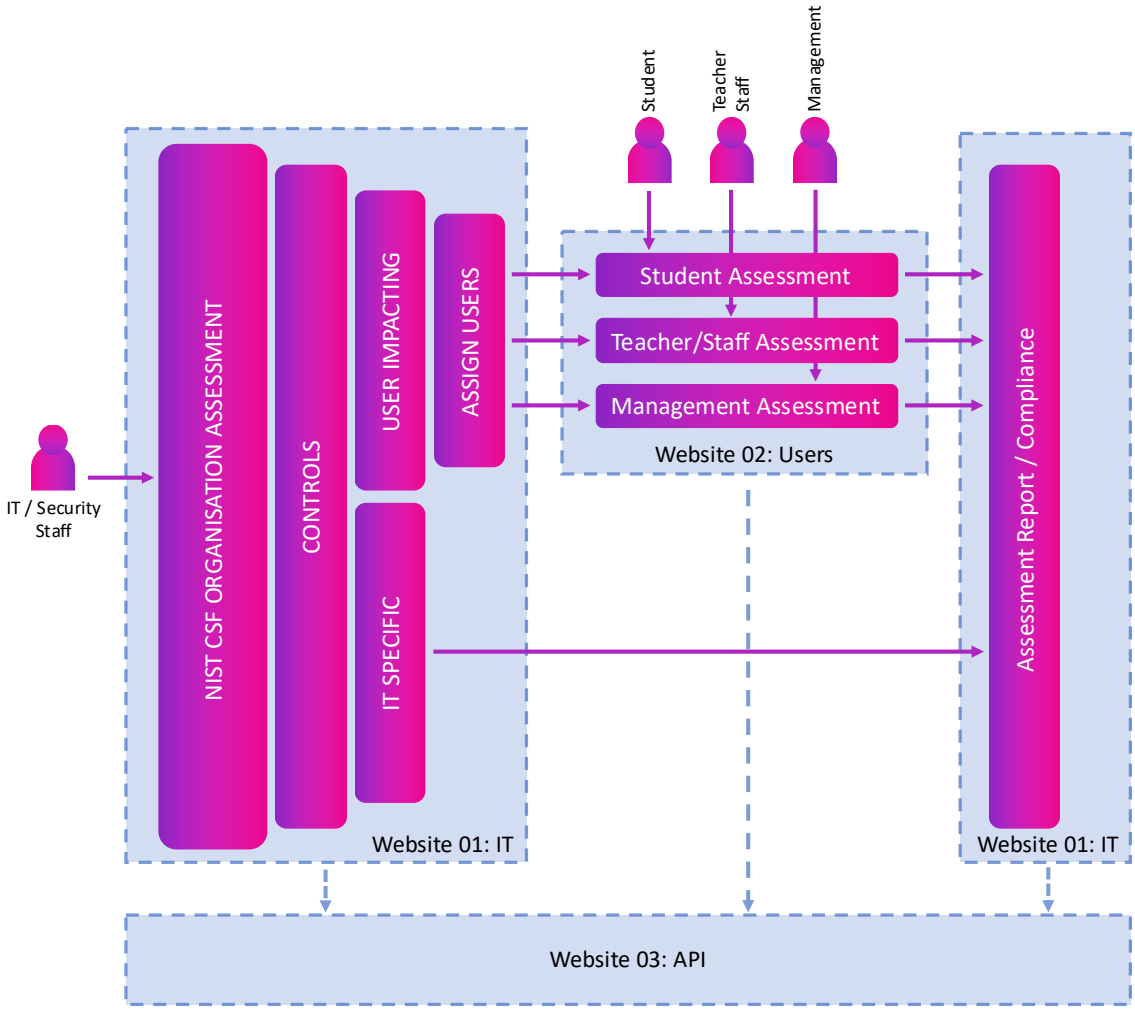

Figure 1 - Assessment tool components

The assessment tool comprises two front-end websites and a backend application programming interface (API). Website 01 is the core interface for administration activities, completing technical assessments, developing and assigning user assessments, and reviewing reports. The target audience for website 01 is IT and security staff responsible for cybersecurity within their school. Website 02 is dedicated to end-users and provides a streamlined interface for completing their learning activities and assessments. Lastly, website 03 provides the API, which allows external systems to interact with the business logic of the assessment tool. This includes organisation and user management, IT assessments, user assessments, and assessment reporting. The API is an OData RESTful API that supports the JSON format. Websites 01 and 02 are single-page applications written in the React JavaScript library, while the API is written in .NET 6.0. Websites 01, 02, and 03 utilise Microsoft Azure AD as its authentication provider and support OAuth authentication, ensuring users have access only to the components they are authorised to access. Figure 2 shows an example of the user interfaces for website 01.

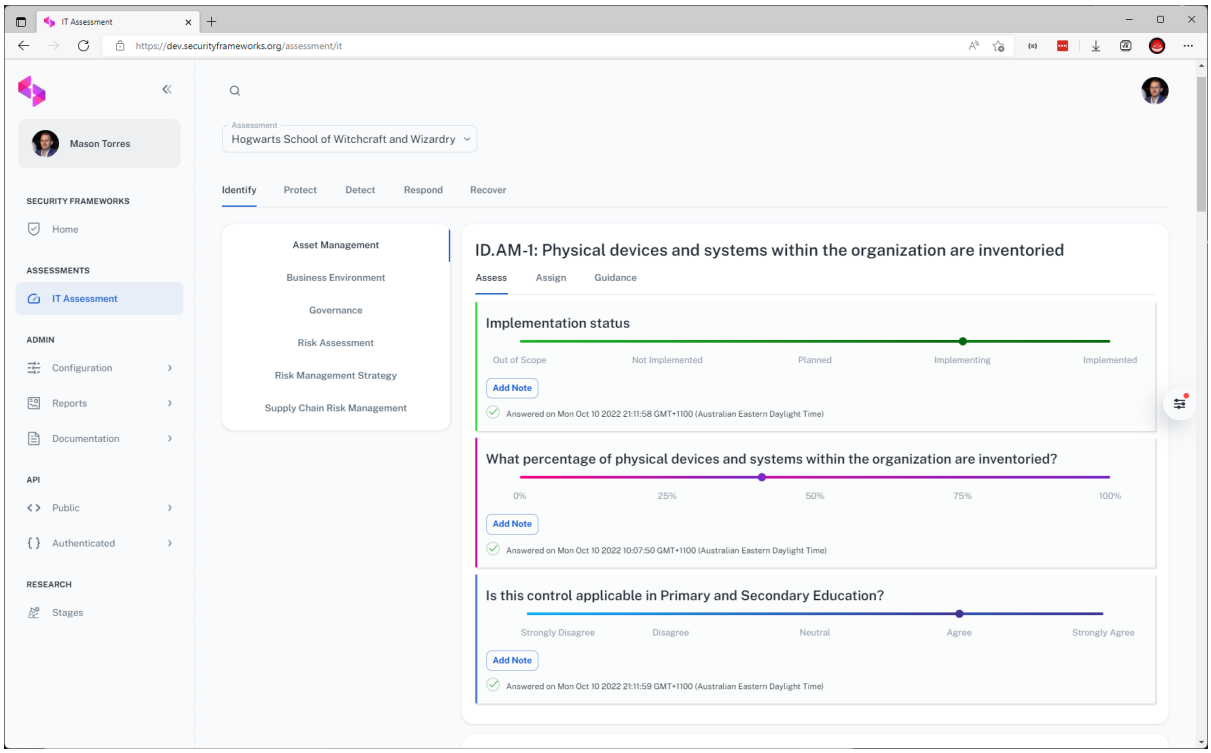

Figure 2 - Examples of the online assessment tool (website 01)

To reduce the assessment tool's exposure to personally identifiable information, the only user data stored is confined to a users' first name, last name, and email address. Participating schools and systems can opt-in to share their assessment aggregated results with other schools/systems. Aggregated data is currently limited to how applicable a specific control is to k-12. Furthermore, the database, backups, and logs are encrypted at rest and access to the assessment tool and API is communicated over an encrypted HTTPS channel.

Overall, the assessment tool provides a report of compliance against the NIST Cybersecurity Framework, providing training and awareness components for constituents within school environments, technical guidance for IT and security staff within school environments, and an ability to track quantifiably and prioritise cybersecurity efforts for school management. The assessment tool goes beyond existing frameworks and tools by incorporating human-specific components that align with the overall assessment compliance. Furthermore, the learning content is related to cybersecurity and goes beyond cyber safety, which is typically the focus within schools. The assessment tool also provides a standardised way to measure all schools within an education system, body, or jurisdiction; enabling the school systems to assess all schools within their purview. For Australia, this comprises public, catholic, and independent schools. Lastly, the aggregated data from individual school assessments can be utilised to assess all schools' compliance and priorities to understand further the challenges associated with implementing cybersecurity within school environments.

6 Beyond the Assessment

Enhancing learning analytics and insight capabilities, the assessment tool is designed to be open and allow schools to access and export their data through an API, thus, enabling schools to implement their own tracking and analytics of assessments over time and to maintain the ownership of their data. It also allows schools to ingest the data into their own reporting tools.

Through a semi-structured interview with a Chief Information Security Officer for an extensive network of schools, it was identified that tools or assessments need to be vetted by the Teaching and Learning department so as not to impede schools' implementation of the defined curriculum. Curriculum considerations may be an obstacle for this assessment tool as schools are directly aligned to deliver curriculum-based learning and do not often stray from the prescribed curriculum. To accept the assessment tool as a helpful aid for cybersecurity prevention and awareness, schools will need to adopt the assessment tool at a strategic level. However, to combat the obstacle, the assessment tool user-based assessments could be tailored to align with curriculum standards.

The online assessment tool is designed to evolve and adapt as guidance and recommendations to address school challenges become known. The aim is to incorporate a community effort to improve cybersecurity for all schools and address the human-centric gap in other tools. For example, aggregated data on school compliance against controls within NIST CSF can provide insight into the education sector's cybersecurity posture. Additionally, a school can be enabled to contribute content to the training and awareness components of the tool, further improving the training content for all. To assess this, further research will be conducted with schools that will pilot the assessment tool.

7 Conclusion

Primary and secondary education environments continue to be high-technology adopters responsible for significant amounts of personal and sensitive information. However, cybersecurity efforts to prevent unauthorised access and misuse of data and systems are often not supported by proportionate resources and expertise. Cybersecurity frameworks can be used to help determine and plan mitigation activities or controls to reduce the risk of cyber-attacks, but often these frameworks are aligned to specific industries and regulations. However, some generalisable frameworks exist and can be used within any industry. To assist primary and secondary education environments with the adoption of cybersecurity frameworks, an online assessment tool was developed using the NIST Cybersecurity Framework as a foundation, given that it can be generalised to any industry.

The online assessment tool is designed to address challenges specific to education environments; this is achieved through the designation of technical and non-technical controls depicted in NIST CSF. IT staff assess their compliance against the technical controls within the framework, analyse the results and determine which controls to implement next, adapting them to their environments. In addition to the technical controls, IT staff assign non-technical controls to various constituents, which assigns training and awareness material commensurate with the comprehension and role of the individual. The objective is to educate users on their impact and responsibility of cybersecurity practices in a quantifiable and engaging manner. Finally, the assessment tool reports allow school management and IT staff to track, identify gaps and prioritise the next set of cybersecurity controls to implement to improve their cybersecurity posture.

8 References

Azmi, R., Tibben, W., and Win, K. T. 2018. "Review of Cybersecurity Frameworks: Context and Shared Concepts," *Journal of Cyber Policy* (3:2), pp. 258-283.

Brown, B. R. 2016. "Measuring the Level of Security in the K-12 It Environment in Southern California." Capella University.

Caballero, A. 2017. "Security Education, Training, and Awareness," in *Computer and Information Security Handbook*. Elsevier, pp. 497-505.

Carías, J. F., Arrizabalaga, S., Labaka, L., and Hernantes, J. 2021. "Cyber Resilience Self-Assessment Tool (Cr-Sat) for Smes," *IEEE Access* (9), pp. 80741-80762.

Emer, A., Unterhofer, M., and Rauch, E. 2021. "A Cybersecurity Assessment Model for Small and Medium-Sized Enterprises," *IEEE Engineering Management Review* (49:2), pp. 98-109.

Garcia, A. B., and Bongo, S. M. C. 2022. "A Cyber Security Cognizance among College Teachers and Students in Embracing Online Education," *2022 8th International Conference on Information Management (ICIM)*: IEEE, pp. 116-119.

Gyunka, B. A., and Christiana, A. O. 2017. "Analysis of Human Factors in Cyber Security: A Case Study of Anonymous Attack on Hbgary," *Computing & Information Systems* (21:2).

Howard, C. D. 2021. "Development of a Pilot Training Program for Middle School Students to Reduce End-User Cyber Vulnerabilities." Walden University.

Hussain, A., Mohamed, A., and Razali, S. 2020. "A Review on Cybersecurity: Challenges & Emerging Threats," *Proceedings of the 3rd International Conference on Networking, Information Systems & Security*, pp. 1-7.

IBM. 2014. "Ibm Security Services 2014 Cyber Security Intelligence Index."

Ibrahim, A., Valli, C., McAteer, I., and Chaudhry, J. 2018. "A Security Review of Local Government Using Nist Csf: A Case Study," *The Journal of Supercomputing* (74:10), pp. 5171-5186.

Kamaludeen, M., Ismaeel, S., Asiri, S., Allen, T., and Scarfo, C. 2020. "A Framework for Cyber Protection (Fcp) in K-12 Education Sector," *3rd Smart Cities Symposium (SCS 2020)*: IET, pp. 239-244.

National Institute of Standards and Technology. 2018. "Framework for Improving Critical Infrastructure Cybersecurity." National Institute of Standards and Technology.

Nguyen, T., and Bhatia, S. 2020. "Higher Education Social Engineering Attack Scenario, Awareness & Training Model," *Journal of The Colloquium for Information Systems Security Education*, pp. 8-8.

Nobles, C. 2018. "Botching Human Factors in Cybersecurity in Business Organizations," *HOLISTICA–Journal of Business and Public Administration* (9:3), pp. 71-88.

Nyachwaya, S. 2013. "Information Security Management Practices of K-12 School Districts," *ProQuest LLC*).

Paakki, T. 2019. "An Exploration of the Strategies Information Assurance Technologists Need to Improve Information Security Practices in an School District." Colorado Technical University.

Qusa, H., and Tarazi, J. 2021. "Cyber-Hero: A Gamification Framework for Cyber Security Awareness for High Schools Students," *2021 IEEE 11th Annual Computing and Communication Workshop and Conference (CCWC)*: IEEE, pp. 0677-0682.

Rauch, E., Unterhofer, M., Rojas, R. A., Gualtieri, L., Woschank, M., and Matt, D. T. 2020. "A Maturity Level-Based Assessment Tool to Enhance the Implementation of Industry 4.0 in Small and Medium-Sized Enterprises," *Sustainability* (12:9), p. 3559.

Richardson, M. D., Lemoine, P. A., Stephens, W. E., and Waller, R. E. 2020. "Planning for Cyber Security in Schools: The Human Factor," *Educational Planning* (27:2), pp. 23-39.

Safa, N. S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N. A., and Herawan, T. 2015. "Information Security Conscious Care Behaviour Formation in Organizations," *Computers & Security* (53), pp. 65-78.

Williams, K. C., Mahmood, S., Sheehan, T., and Furtado, P. 2022. "Top Trends Impacting K-12 Education in 2022,").

Yan, Z., Xue, Y., and Lou, Y. 2021. "Risk and Protective Factors for Intuitive and Rational Judgment of Cybersecurity Risks in a Large Sample of K-12 Students and Teachers," *Computers in Human Behavior* (121), p. 106791.

Copyright