Toward a Cyber Security Adoption Framework for Primary and Secondary Education Providers

Short paper

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

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

Abstract

The necessity for strong cyber security controls in primary and secondary education is growing as schools are increasingly targeted by cyber-attacks. This paper discusses how the adoption of technology in primary and secondary schools bring associated security threats, and how security standards and frameworks used in other industries may be applicable. The objective of this research is to create an adoption framework which incorporates current security industry standards and frameworks into the primary and secondary education environment. The proposed adoption framework aims to improve schools' security posture while maintaining minimal impact on the teaching and learning of students.

Keywords cyber security, primary and secondary education, cyber security frameworks, NIST

1 Introduction

Cyber security plays a significant role in today's society reaching a global spend of 145 billion US dollars in 2018 (Network 2019). Central to many governments plans to improve cyber security is the need to close the skills and workforce gap and improve cyber literacy. The adoption of technology in primary and secondary education is in continual growth as educators prepare students for life and career after education and rapidly adopt new and emerging technologies to aid in the delivery of teaching and learning, administrative tasks and community engagement. The role of cyber security within primary and secondary education is to enhance the overall security posture of the industry while simultaneously not impeding the delivery of pedagogy, teaching and learning, administrative tasks and community engagement.

Security best practices and frameworks are effective at reducing the risk associated with increased connectivity and rapid technology adoption, however, the motivation behind the adoption of these industry-supported security strategies extend from government policies and regulatory requirements to mitigation against the compromise of confidentiality, integrity and availability of data (Bendovschi 2015) and the loss of business continuity, reputation or financials (Davies 2019). Adopting well-known security standards and frameworks in primary and secondary education will allow for the use of existing mitigation strategies, practices and controls as recommended by the security community and government agencies. However, to use these standards successfully, they require tailored adoption strategies, implementation plans and customisation to meet the needs and address the challenges of primary and secondary education.

2 Cyber Security in Education

Primary and secondary institutes are prime targets for cyber-attacks. They are also a unique environment where most of the users are children, followed by teaching staff and administrative staff. This introduces unique challenges when implementing cyber security frameworks which introduce controls and complexities, as they require user adoption, interaction, understanding and awareness, the human factors. To add to the complexity the industry is known for their openness and collaborative nature as seen through the adoption of the flipped classroom model and blended learning and its use of online tools and resources (Sergis et al. 2018) as-well-as adoption of remote learning (Cavanaugh and Roe 2019) and distance learning. Furthermore, adoption of online tools has been exacerbated through the closure of schools during the Covid-19 pandemic (Hamilton et al. 2020), increasing the exposure of staff and students to cyber security risks as activities are conducted online.

IBM (2019) highlights the financial cost of data breaches in education averaging US 4.77 million dollars per breach. They also report the meantime to identify and the time to contain a data breach at 212 and 71 days respectively. Verizon (2018) reports the highest patterns and actions in education security incidents derive from denial of service and hacking attacks. While McAfee ranks education as the 6th highest industry targeted based on the number of breaches reported in 2019 (Beek et al. 2019). The cyber security threat to education is real and warrants mitigation strategies and investment into preventative measures to ensure schools remain safe, secure and operational. In 2018 two students accessed a Michigan school district IT system after finding credentials written on a sticky note (Mears 2018). A Melbourne secondary college posted students personal information including medical conditions and learning behaviour difficulties on the college's intranet site (SBS News 2018). While 2019 saw a Perth school become victim to a cyber-attack which may have resulted in the exposure of parents financial information and electronic copies of signatures (Geraldton Guardian 2019).

This research in progress identifies the following questions to be addressed through further research:

1. What, if any, security standards or frameworks are used in primary and secondary education?
2. What current industry security standards or frameworks can be used in primary and secondary education?
3. How would a school or education system adopt these security standards or frameworks?
4. Are existing standards and frameworks the most appropriate means to secure primary and secondary educational institutions?

Initial data collected involved interviews with industry experts and leaders in education with early results suggesting funding and resourcing; staff workloads; impact to teaching and learning, and; general awareness and understanding as key areas of concern when adopting cyber security controls in

primary and secondary education. This reinforces the need for a cyber security adoption framework that removes complexities associated with framework implementations while maintaining enough security controls to ensure risk is reduced, leveraging existing cyber security frameworks and controls.

3 Technology Trends in Education

Information Technology in primary and secondary education is an ever-changing landscape and an example of an industry with high adoption of new and emerging technologies. Key observations from Gartner's strategic technologies trends in primary and secondary education include the use of technologies that are delivered through a third party or online service providers, including cloud services, which introduces risk through the distribution of personally identifiable or private information through the connectedness required to integrate to these services. This is further supported through the 2016 trend of exostructure as it refers to "acquiring the critical capability of interoperability as a deliberate strategy to leverage the increasing numbers of partnerships, tools and services in the education ecosystem" (Williams 2015). The use of technology that supports these strategies and trends introduces organisational risk and security risk that warrants consideration, understanding and mitigation strategies to handle the risk and associated security vulnerabilities. Further to the adoption of new and emerging technologies, the education sector are heavy embracers of traditional IT services as there is a drive to integrate technology into the classroom to prepare students "with the skills needed to prepare for college and a career" (Delgado et al. 2015). Delgado et al highlight the use of technology in the classroom through initiatives including bring your own device (BYOD), blended learning, flipped learning and flipped classrooms, and online learning. Additionally, six barriers of technology integration are identified; resources, knowledge/skills gap, institution and attitudes/beliefs, assessment and subject culture (Delgado et al. 2015; Hew and Brush 2007).

4 The State of Cyber Security in Education

Richardson et al. (2020) discuss the factors that make the education industry a prime target for cybercriminals. They outline the variety of valuable data as it pertains to students, parents, alumni, faculty and staff that can be retained for decades; the lack of centralised structure for cyber security through storage of data in multiple disparate locations; organisational vulnerabilities through the lack of a top-down organisational structure where responsibilities for implementing and operating security tasks are spread across reporting structures; and the prevalent use of less well-protected personal devices to access corporate data. In a report published by The K-12 Cybersecurity Resource Center (Levin 2020) the top known attacks against primary and secondary education reported in the US for 2019 included data breaches and unauthorised disclosure, ransomware and malware, phishing, denial of service and website/social defacement. Additionally, citing 80 per cent of schools in the UK have experienced at least one cyber incident in 2019.

Additionally, accountability and awareness of data accessed by teachers and administrative staff expose a lapse in security education for education employees. The 2018 Education Cybersecurity Report (SecurityScorecard 2018) discusses tracking student data from assessments, attendance and educator feedback etc into online tools, analytics engines and centralised databases. As teachers consume this data, they need to be cognisant of the security implications linked to the data. The 2018 Education Cybersecurity Report shows education at the bottom of performers on the list of industries for total cyber security safety.

Current literature and research for cyber security in primary and secondary education is closely aligned to curriculum design. Conversely to the integration of cyber security into the curriculum, the literature on the adoption of cyber security best practices specific to primary and secondary education providers is scarce. The current literature in the education sector focusses specifically on tertiary education, however primary and secondary education per capita equates to a significantly larger staff and student cohort. The Australian Curriculum Assessment and Reporting Authority (2018) report shows 3.89 million students were enrolled in 2018 across Australian primary and secondary schools. With a total of 288,583 teaching staff and 126,941 non-teaching staff. While higher education had 1,562,520 students enrolled (Department of Education 2018a) and 121,718 staff (Department of Education 2018b). The difference in the number of students and staff between primary and secondary and tertiary education highlights an increased attack surface through the sheer number of entry points, while also highlighting a disproportion in the literature which focuses on tertiary providers. Nussbaum and Lewis (2017) discuss the social aspect, which affects all users, as a large part of the problems faced by cyber security professionals, where the security professional spends their time dealing with people as much as with the technology. Additionally, they expose the idea of

specialisation, decentralisation and economies of scale, as they relate to cyber security, that is associated with larger organisations. For perspective, primary and secondary education received a total of 61.5 billion Australian dollars from recurrent government funding (Australian Curriculum Assessment and Reporting Authority 2018). While universities may arguably possess more critical or sensitive information based on their research and operations, schools still possess significant personal, financial and sensitive information, remaining a large target for cybercriminals.

An independent report commissioned by CISCO focussing on universities, TAFEs and school systems describes the changes in landscape as the world introduces IoT devices, machine learning technologies and Dev Ops design processes (Davies 2019). These changes introduce an increased attack surface and additional risk through the 50 billion IoT devices being connected, the availability of machine learning to quickly scale and develop threats, and the speed at which new solutions are developed. Similarly, Gul et al. (2017) outline the high adoption of IoT in education as schools implement smart classrooms and bolster their teaching through the "highly exciting and stimulating" topic of IoT as it attracts and engages students. Drawing attention to the need for security and privacy controls as IoT devices are an "internet-based network of connected devices".

Javidi and Sheybani (2019) discuss introducing cyber security concepts to students at a young age. Noting students are taught how to use technology at a young age but are not taught the threats associated with technology. They continue to discuss the need for teachers to integrate cyber security concepts in the classroom. These factors of incorporating cyber security concepts into everyday teaching can be used to promote and increase the overall cyber security posture of schools while also having the added benefit of introducing students to positive security behaviours which will assist them in their future careers. Without an adoption framework schools are less informed on how to implement security controls like multi-factor authentication, assessment of threat intelligence or access permissions and authorisations as defined by the National Institute of Standards and Technology (2018) Cybersecurity Framework.

5 Role of Frameworks

Security frameworks provide guidelines, procedures and processes aimed at reducing the risk associated through cyber security threats against an organisation, outlining how organisation manage their systems, services and information. Humayun et al. (2020) analysed various definitions of cyber security concluding that "Cyber security can be considered as a mechanism of protecting individuals' and organisations' assets from unauthorized access" closely linked to protection and privacy and the confidentiality, integrity and availability policies and rules. They also conducted a systematic literature review on key cyber security vulnerabilities and their risk mitigation approaches. Creating a mapping "overview of existing cyber security vulnerabilities and their detection and mitigation approaches". Identifying denial of service, malware and phishing as the top three vulnerabilities discussed in current literature. Businesses and individuals were the most targeted victims with businesses being targeted more than individuals. While threat mitigation was predominately achieved through intrusion detection systems and firewalls followed by traffic analysis and anti-phishing tools.

The information technology and cyber security community along with government agencies have developed numerous standards, guidelines and frameworks for managing risk to organisations from internal and external cyber threats. Sabillon et al. (2016) compiled a list of national cyber security strategies, global intergovernmental organisations and cyber security frameworks. The most prominent frameworks identified include NIST CSF, NIST SP 800-53 and ISO 27032:2012. Each frameworks' purpose is to reduce and mitigate risk associated with cyber activities from adversaries and malicious actors. Many frameworks are targeted at specific industries while others like NIST CSF are widely applicable as "it can be used by organizations in any sector of the economy or society" (National Institute of Standards and Technology 2018).

Each framework details a set of controls or activities that are required to be compliant with the framework. The NIST CSF comprises of three components, the framework core, implementation tiers, and framework profiles. The framework core supplies a set of activities to accomplish cyber security outcomes. Starting with the high-level functions, then delving into more detail with categories, subcategories and informative references. The functions comprise of identify, protect, detect, respond and recover (National Institute of Standards and Technology 2018). Similarly, NIST SP 800-53 has its own controls that "(i) protect the confidentiality, integrity, and availability of information that is processed, stored, and transmitted by those systems/organizations; and (ii) satisfy a set of defined security requirements" (National Institute of Standards and Technology 2013). NIST CSF can be used for "identifying, assessing, and managing cybersecurity risk" within an organisation (National Institute

of Standards and Technology 2018). It complements existing business risk management and cyber security processes and provides management with the ability to make informed decisions. It is technology-neutral and makes use of pre-existing standards, guidelines and practices. These frameworks specifically identify the controls required to achieve the desired outcome. They do not, however, state how industries should approach the adoption of these controls.

5.1 Adoption of Frameworks

A recent evaluation of cyber security in a Western Australia government organisation discussed the benefits of deriving metrics from alignment to the frameworks core functions, identify, protect, detect, respond and recover, to enable the organisation to be prepared for actual risk (Ibrahim et al. 2018). Metrics were acquired through an assessment tool targeted at the executive, management and technical participants identifying risks and areas of growth and improvement. When benchmarked against NIST CSF, the agency scored only 25% compliance in detection of cyber security incidents, and 36% compliance in identity management. Adoption of an established framework, such as NIST CSF would support formalised cybersecurity governance and address many of the risks that were identified.

Hussain et al. (2020) outline governance and risk management and culture and awareness as components of cyber security. Governance being achieved using frameworks and the oversight of risks within an organisation. Further emphasising the need for a holistic cyber security strategy that is implemented across the entire organisation. While culture and awareness encompass the importance of users understanding of cyber security, specifically when users have access to many systems with varying levels of access to data.

As frameworks can be applied in diverse environments, technical prescriptions are generally not included (Scofield 2016). Therefore, the lack of research and evidence into how such frameworks may be applied to the primary and secondary education environment is a gap which needs to be addressed.

5.2 Barriers to Adoption

Hussain et al. (2020) identified challenges and emerging threats to critical infrastructure. Governance, risk management and awareness were the three identified challenges. Identifying poor governance as a precursor to poor risk management and in turn, poor culture and awareness, which is subsequently abused by emerging threats. Emerging threats comprised of cloud computing, internet of things (IoT) and smartphones. While schools may not be considered critical infrastructure, they can utilise lessons learned from industry organisations, specifically as they relate to the adoption of security frameworks. Hussain et al. state that cyber security governance is the implementation of a framework and the oversight of risk assessments such that risk can be mitigated. Expressing the importance to integrate cyber security into the "DNA" of every organisation.

Change within a school environment affects not only the students but the teaching staff, administrative staff and leadership. Razak et al. (2018) discuss the integration of information communication technology (ICT) into schools stating, "it is crucial for all school stakeholders to know their respective roles in working to successful ICT integration". This notion can be applied to security controls, defined by frameworks, as they can relate directly to the technologies used in schools. Similarly, Razak et al. articulate the meaning of cultural change as creating a culture of change where users seek, assess and incorporate new ideas and practices highlighting the lack of cultural understanding of cyber security as a significant cause of cyber security concern.

Dedeke (2017) outline three implementation risks that may result in higher cost, increased implementation time, loss of morale and delayed results when implementing a security framework; implementation creep – implementing cyber security across too many departments at once; framework creep – merging too many frameworks; control creep – implementing too many controls at once. Similarly, a survey of 319 IT security decision-makers identified four key organisational challenges when adopting security frameworks; lack of trained staff; inadequate budget; lack of prioritization, and; not enough management support. While technology challenges included lack of appropriate tools to automate controls; lack of appropriate tools to audit continuous effectiveness of controls; lack of integration among tools; and lack of reporting (Dimensional Research 2016).

6 Conclusion

Primary and secondary education encompass large cohorts of students and staff that are exposed to cyber security risks like any other industry. The cyber security challenges across all industries range from the approach of governance and risk management, the adoption of standards and frameworks into business processes, the culture and awareness of users, and the human factors associated with cyber security controls and policies. In the context of primary and secondary education, the user base primarily consists of young students who possess the tools to engage with technology but not necessarily the comprehension to follow cyber security controls. Similarly, educators and school administrators are affected by security controls in both their administrative duties and their pastoral care duties. This creates an additional complexity of how to balance the teaching and learning components and the business functions within schools.

Research into the adoption of security frameworks in primary and secondary education may significantly improve schools' security posture and rate of adoption. It will also make it possible to prioritise controls that have a low financial cost and low impact on user experience, to provide the most efficient and effective solutions. Furthermore, the adoption can begin the cultural change for individuals to understand their cyber security responsibilities. A potential limitation to this study may be the scope and breadth of security controls which may be feasible to implement in the primary and secondary education environment. This however provides an opportunity for further research to explore new directions in the implementation of cyber security controls.

This research in progress proposes an adoption framework for security in primary and secondary education that can help align existing industry controls in a context that is suitable for schools, improving overall security, awareness and education, providing a pathway to the broader implementation of security controls across schools, their users and services. To address this, the subsequent stages of this research will identify and contribute to literature the current use of frameworks in primary and secondary education, identify the appetite for the use of frameworks, create an assessment tool to align current security strategies implemented to existing frameworks, and identify framework controls that can be prioritised to increase security posture while limiting user impact.

7 References

Australian Curriculum Assessment and Reporting Authority. 2018. "National Report on Schooling in Australia," Australian Curriculum Assessment and Reporting Authority.

Beek, C., Dunton, T., Fokker, J., Grobman, S., Hux, T., Polzer, T., Lopez, M. R., Roccia, T., Saavedra-Morales, J., Samani, R., and Sherstobitof, R. 2019. "Mcafee Labs Threats Report."

Bendovschi, A. 2015. "Cyber-Attacks – Trends, Patterns and Security Countermeasures," Procedia Economics and Finance (28), pp. 24-31.

Cavanaugh, C., and Roe, M. 2019. "Developing Pedagogy and Course Design Skills in Novice Virtual School Teachers in Australia," Journal of Online Learning Research (5:1), pp. 5-22.

Davies, B. 2019. "How Universities, Tafes and School Systems Are Responding to the Escalating Cyber Security Threat," Vector Consulting, Vector Consulting.

Dedeke, A. 2017. "Cybersecurity Framework Adoption: Using Capability Levels for Implementation Tiers and Profiles," IEEE Security & Privacy (15:5), pp. 47-54.

Delgado, A. J., Wardlow, L., McKnight, K., and O'Malley, K. 2015. "Educational Technology: A Review of the Integration, Resources, and Effectiveness of Technology in K-12 Classrooms," Journal of Information Technology Education (14).

Department of Education, S. a. E. 2018a. "2018 Full Year Higher Education Statistics," S.a.E. Department of Education (ed.). Department of Education, Skills and Employment.

Department of Education, S. a. E. 2018b. "Selected Higher Education Statistics—Staff 2018," 2018_staff_2_number_0.xlsm (ed.). Department of Education, Skills and Employment.

Dimensional Research. 2016. "Cybersecurity Frameworks and Foundational Security Controls Survey," Tenable Network Security.

Geraldton Guardian. 2019. "Parents' Financial Details Stolen in Cyber Attack on Geraldton Catholic School." Retrieved 29/07/2020, 2020, from https://thewest.com.au/news/geraldton-guardian/parents-financial-details-stolen-in-cyber-attack-on-geraldton-catholic-schools-ng-b881236197z

Gul, S., Asif, M., Ahmad, S., Yasir, M., Majid, M., Malik, M. S. A., and Arshad, S. 2017. "A Survey on Role of Internet of Things in Education," International Journal of Computer Science and Network Security (17:5), pp. 159-165.

Hamilton, L. S., Grant, D., Kaufman, J. H., Diliberti, M., Schwartz, H. L., Hunter, G. P., Setodji, C. M., and Young, C. J. 2020. "Covid-19 and the State of K–12 Schools: Results and Technical Documentation from the Spring 2020 American Educator Panels Covid-19 Surveys,").

Hew, K. F., and Brush, T. 2007. "Integrating Technology into K-12 Teaching and Learning: Current Knowledge Gaps and Recommendations for Future Research," Educational technology research and development (55:3), pp. 223-252.

Humayun, M., Niazi, M., Jhanjhi, N., Alshayeb, M., and Mahmood, S. 2020. "Cyber Security Threats and Vulnerabilities: A Systematic Mapping Study," Arabian Journal for Science and Engineering), pp. 1-19.

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. 2019. "Cost of a Data Breach Report," IBM.

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.

Javidi, G., and Sheybani, E. 2019. "Design and Development of a Modular K-12 Cybersecurity Curriculum," 2019 ASEE Annual Conference & Exposition.

Levin, D. A. 2020. "The State of K-12 Cybersecurity: 2019 Year in Review," The K-12 Cybersecurity Resource Center.

Mears, D. 2018. "Student Hacker Shows Holes in K-12 Cybersecurity." Retrieved 29/07/2020, 2020, from https://www.detroitnews.com/story/news/education/2018/10/03/rochester-hills-student-hacking/1369297002/

National Institute of Standards and Technology. 2013. "Nist Special Publication 800-53," in: Security and Privacy Controls for Federal Information Systems and Organizations.

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

Network, A. C. S. G. 2019. "Australia's Cyber Security Sector Competitiveness Plan 2019."

Nussbaum, B., and Lewis, C. 2017. "Sizing up People and Process: A Conceptual Lens for Thinking About Cybersecurity in Large and Small Enterprises," Journal of Cyber Policy (2:3), pp. 389-404.

Razak, N. A., Jalil, H. A., Krauss, S. E., and Ahmad, N. A. 2018. "Successful Implementation of Information and Communication Technology Integration in Malaysian Public Schools: An Activity Systems Analysis Approach," Studies in Educational Evaluation (58), pp. 17-29.

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.

Sabillon, R., Cavaller, V., and Cano, J. 2016. "National Cyber Security Strategies: Global Trends in Cyberspace," International Journal of Computer Science and Software Engineering (5:5), p. 67.

SBS News. 2018. "Probe into Melb High School Privacy Breach." Retrieved 29/07/20, 2020, from https://www.sbs.com.au/news/probe-into-melb-high-school-privacy-breach

Scofield, M. 2016. "Benefiting from the Nist Cybersecurity Framework," Information Management (50:2), p. 25.

SecurityScorecard. 2018. "2018 Education Cybersecurity Report," SecurityScorecard.

Sergis, S., Sampson, D. G., and Pelliccione, L. 2018. "Investigating the Impact of Flipped Classroom on Students' Learning Experiences: A Self-Determination Theory Approach," Computers in Human Behavior (78), pp. 368-378.

Verizon. 2018. "2018 Data Breach Investigations Report," Verizon.

Williams, K. C. 2015. "Top 10 Strategic Technologies Impacting Education in 2015," Gartner.

Acknowledgement

The authors gratefully acknowledge Sunitha Prabhu, Waikato Institute of Technology, for her feedback during the preparation of this manuscript.

Copyright