Main factors and good practices for managing BYOD and IoT risks in a K-12 environment

Oluwaseun Akeju*, Sergey Butakov and Shaun Aghili

Concordia University of Edmonton,
7128 Ada Boulevard, Edmonton AB, Canada
Email: oakeju@student.concordia.ab.ca
Email: sergey.butakov@concordia.ab.ca
Email: shaun.aghili@concordia.ab.ca
*Corresponding author

Abstract: The presented research looks into information security and privacy risk related to using mobile and embedded devices for learning in the K-12 environment. *Bring Your Own Device* (BYOD) program and *Internet of Things* (IoT) for learning are the two focus areas discussed in this paper. The NIST privacy risk management framework (NIST-8062) template was used to illustrate the privacy impact factors K-12 ecosystem participants should consider while developing BYOD/IoT programs. The key factors involved in the decisions include reputation costs, direct business costs and non-compliance costs. Key security issues and risks such as network access, server and end-user device malware, application risks, and privacy risks were identified. The analysis of the risks suggested to recommend some good practices derived from various documents suggested by ISACA, IIA, SANS, and NIST. The proposed good practices were subsequently incorporated into BYOD guide for the K-12 system in two Canadian provinces (Alberta and Manitoba) in an attempt to increase its effectiveness in terms of addressing relevant risks. Although the good practices compiled in this research are proposed to be incorporated into the Alberta and Manitoba's BYOD guide for K-12 schools, the same process is applicable to any similar K-12 environment.

Keywords: bring your own device; BYOD; internet of things; IoT; information security; risk assessment; information privacy; K-12; good practices.

Reference to this paper should be made as follows: Akeju, O., Butakov, S. and Aghili, S. (2018) 'Main factors and good practices for managing BYOD and IoT risks in a K-12 environment', *Int. J. Internet of Things and Cyber-Assurance*, Vol. 1, No. 1, pp.22–39.

Biographical notes: Oluwaseun Akeju received his Master of Information Systems Assurance Management from Information Systems Security and Assurance Management Department, Concordia University of Edmonton. He is an aspiring professional in the area of IS Assurance and Security. His research interests include BYOD, IS Assurance, IS Auditing, and IT governance on the enterprise scale.

Sergey Butakov received his PhD, CISA; and is an Associate Professor and the Chair of the Information Systems Security and Assurance Management Department, Concordia University of Edmonton. He holds a PhD in Computer Science from Altai State University, Russia. He authored and co-authored more than 40 publications. In the last 15 years, he served as the principal researcher

in various industry and university funded research projects. He is interested in information systems security, text search, plagiarism detection, software development, and artificial intelligence.

Shaun Aghili is an Associate Professor of Management in Information Systems Security and Assurance Management Department, Concordia University of Edmonton. His academic research and professional interests revolve around internal audit, fraud prevention, and information systems assurance. He is the author/co-author of over 40 research papers and consumer-oriented articles, and has been awarded a certificate of merit for "Outstanding Character and Excellence in Contributing to the Literature for the Advancement of Management Accounting and Financial Management" by the Institute of Management Accountants (IMA). On a global scale, he is among an elite group of the Institute of Internal Auditors (IIA) academic members holding five internal auditing certifications conferred by the IIA.

1 Introduction

Technology in the K-12 system has moved from the traditional way of providing computers for learning. K-12 schools have adopted new forms of technologies such as mobile devices and embedded devices for learning and administration (K 12 Blueprint). Wireless technology provides the mobility in delivering content and helps to facilitate learning inside and outside of school. Students do not need to be tethered to wired desktops or computer labs anymore. Mobile devices and embedded Internet of Things (IoT) devices in a Bring Your Own Device (BYOD) model and in traditional company-owned model have helped in mass consumerisation of technology in K-12 schools (Selinger et al., 2013). Obviously, the two great technologies came with some challenges. The next two paragraphs expand more on the developments and challenges of BYOD and IoT in the K-12 environment.

BYOD in K-12 is the model where students or staff members bring personally-owned mobile devices to school for the purpose of learning and teaching (Alberta Education, 2012). These devices can serve as an alternative to computers provided by the schools. BYOD also refers to the ways employees access their organisations' applications and resources with their personally-owned devices over a network (Sansurooh and Williams, 2014). Mobile devices are playing the central role in BYOD and IoT: smartphones, laptops, tablet computers, Portable Digital Assistants (PDAs), portable storage devices, activity trackers, GPS locators, etc. (ISACA, 2012). It is expected that by 2018, the number of mobile computing devices will go over 10 billion, or, in other words, 1.5 devices for every single person in the world (Ernst & Young, 2013). Given the current mobile penetration pattern, students and teachers may exceed this number of 1.5 devices to 3–4 devices per person. Students can use mobile devices to conduct research, store assignments in the cloud, participate in class activities, provide information of their whereabouts to their parents, etc. (Bruder, 2014). In North America, a survey of student ownership of mobile devices showed that eight of ten K-12 students owned a smartphone device in 2015. Eighty-percent of elementary students were found to be using a tablet regularly in 2015 compared with 66% in 2014; and, 70% of middle school students used a tablet frequently in 2015, as compared to 42 in 2014 (Poll, 2015).

IoT is used to describe embedded devices with internet access, which enables the devices to interact with each other, services, and people on a global scale (Mukhopadhyay and Suryadevara, 2012). IoT for schools means smart classrooms with advanced value. Smart devices throughout the school will be able to send data and receive instructions over the WI-FI network (Nillson, 2015). The value will be delivered through streamlined instruction and collection of data. The IoT brings benefit to K-12 schools: Students in science classes can use RFID to tag sample specimens and take notes without leaving the classroom. With the use of IoT, teachers are able to reduce the time in finding, connecting and implementing new resources (Augur, 2015). IoT is dependent on the development of wireless sensor networks and radio frequency identification devices (RFID). Researchers reviewed popular IoT device niches in schools, which include interactive whiteboards, webcams, thermostats, HVAC systems, and hubs for controlling multiple devices (Symantec, 2016). IoT will grow to 26 billion units installed by 2020, indicating a 30 times increase from 0.9 billion units in 2009. Cisco predicts that IoT in education has a net present value of $175 billion (Selinger et al., 2013).

The growing trend of both BYOD and IoT devices connecting to school networks causes information security and privacy risk concerns, however. Of the top ten sectors that experienced data breaches in 2014, the education sector sat in third position after the healthcare and retail sectors (Symantec, 2015). There is a 49% increase in security threats and 25% in data privacy risks according to IT Risk/Reward barometer on IoT (ISACA, 2012). IoT is related to BYOD in a number of ways, in that both introduce a vast array of access points to the network. IoT and BYOD can also be used as a medium for transmitting sensitive data. This research paper focuses on key security and privacy related issues when using personally-owned mobile devices and embedded devices for teaching, learning, and administration. The research also identifies some privacy impact factors and good practices that schools can consider when adopting a mobile device or an embedded device for learning.

The overall organisation of this research is as follows: the *background* section presents information about the growing trend of BYOD and IoT for learning. It also describes the security challenges that are present within the area. The background section analyses papers that discuss the risks, security challenges, and mitigation strategies for mobile and embedded devices in the K-12 system. After the analysis of the relevant articles, the common risks, security factors, and notable mitigation strategies common to all papers reviewed are outlined. The *scope, limitations, and methodology* section focuses on the boundaries and constraints of the research. The *discussion and analysis* section explains the results of the methodology used in the research and the solutions proposed to the research questions. The *conclusion* summarises the significance and the overall aim of this research. The paper includes two appendices: Appendix A is a NIST illustrative template used to assess and prioritise privacy risk. Appendix A also includes glossary of terms used in NIST privacy risk template. Appendix B contains a compiled good practices and some selected good practices mapped to BYOD guides for schools for Canadian provinces of Alberta and Manitoba.

2 Background

The impact of BYOD and IoT on education is threefold: First, the use of devices in schools boosts learning. Second, the trend of device usage is reducing the over-reliance on school computers, because many students and staff are already bringing their own mobile devices to school (Microsoft, 2013). Third, the impact of IoT in education is through the use of sensors. The sensors allow users to link physical objects to their local area network and cloud-based service (Selinger et al., 2013).

While BYOD and IoT add several benefits to learning, it also comes with several challenges. Studies identify the following risks and security concerns that could threaten K-12 schools' information:

- The safety of students' information faces a security threat as devices are allowed to access the schools' wireless network without being vetted (Smith et al., 2014).
- Devices can be stolen or lost leading to data loss. Data loss can also occur due to leakage through third party applications, device vulnerabilities, and unsecured and rogue Wi-Fi access points (Cloud Security Allaince, 2012).
- Unauthorised migration of malicious code/malware from personal devices to schools' networks (Miller et al., 2012).
- Major cloud based applications such as Google Apps, Office 365, and variety of online learning mobile applications designed for virtual learning may transform the devices into a gateway for malicious outsiders to enter the enterprise network (ISACA, 2012).
- Schools may have limited or no control over where user devices have been or what applications the user has downloaded as the history of the device is unknown (Sangani, 2013).
- Misuse and abuse of technology resources may occur. Students have been reported to bypass the security restrictions intentionally (e.g., password protection, IT practices and policies) for the convenience of using their own devices thereby compromising the safety of the schools' resources (Watters, 2013).
- Cloud operators and mobile app providers could track students online, collect their data and use it for financial gain. Such collection, especially without consent possesses significant risk to privacy (Krueger and Moore, 2015). In the light of the recent discoveries of unprotected security cameras, baby monitors, online alarm systems, home automation systems, etc. (Hill, 2013), the fact that IoT enables the creation, storage, and sharing of enormous amounts of data about a person's habits, behaviours, and preferences adds even more privacy concerns.

The above risks can be categorised as network access control risks, end user devices risks, cloud/data storage risks, information privacy risks, malware risks, application risks, IoT vulnerability management, and violation of policies and procedures. Given the sheer volume and the variety of threats in cyberspace, no single security strategy can adequately safeguard schools' networks (McDonough, 2010). A good first step to mitigating the risks and security is to illustrate some risk impact factors that must be considered as well as potential consequences if such consideration is omitted. The second step is prioritising these risk factors and then outlining a set of good practices that is based on related industry standards. Good practice avoids the need to perform intensive analysis, gather security-related information, and construct scenarios (Timbs, 2013).

The industry good practices used in this research paper are based on the following IT security related documents: NIST special publication 800-53A R4 (NIST, 2014), SANS

Institute: Critical Security Controls (SANS, 2016), International Professional Practices Framework (IPPF) for auditing privacy risk (Institute of Internal Auditors, 2012) and ISACA Cyber Security Nexus (ISACA, 2012).

The considerations used to scope the framework selection for this research paper was based on industry-specific considerations, policy/regulatory considerations, and operational-related considerations. The considerations, combined with good practices were tailored specifically to the usage of mobile and embedded devices within the K-12 environment. The framework scoping helps to ensure only good practices that can provide the appropriate level of protection for the mobile and embedded devices in the K-12 environment of operation were chosen. Other security frameworks for managing information security risks that could have been included in this research are ISO/IEC 27002:2013 and ITIL version 3.0. ISO 27002 is focused specifically on information security and is therefore limited in scope compared to NIST 800-52. While ITIL version 3.0 primary contribution is towards IT process service management. These limitations suggest to limit the use of standards to the NIST document.

NIST SP 800-53 R4 (NIST, 2014) specifies cyber and physical security controls for organisational planning, policy, procedures, and training. The purposes of NIST SP 800-53 is

1 to provide guidelines for effective security assessment and privacy assessment plans

2 to provide a comprehensive set of procedures for assessing the effectiveness of security controls and privacy controls employed in organisations' information systems (NIST, 2014).

The guideline was developed to help promote a better understanding of the risks to organisational operations, assets, individuals, and organisations. For example, in managing access control the document recommends IT administrator to create a role-based account for users and assign privilege to ensure that online activities are visible and to manage user identity. The recommendations from (NIST, 2014) that are being extensively used are listed in Table 4 of Appendix C.

The SANS CSC document (SANS, 2016) shares insights on potential attacks and attackers, identifies root causes, and translates them into classes of defensive action. The activities recommended in CSC are not just good practices, but a highly focused set of actions that make them implementable, usable, and compliant with all industry or government security requirements (SANS, 2016). The document also proactively aligns with ongoing work in security standards and good practices such as security content automation program, NIST 800-53 SP and ISO/ISC 27002:2013. For example, to prevent the risk that education content delivered through web applications like Google apps for education are used to arbitrarily access system files, SANS recommends protection of web applications by deploying firewalls. The same is true for the NIST document, Table 4 in Appendix B extensively uses recommendations provided by SANS (2016).

The IPPF document (Institute of Internal Auditors, 2012) is a conceptual framework that assesses the adequacy of management's identification of risks related to its privacy objectives and establishes controls to mitigate those risks to an acceptable level (Institute of Internal Auditors, 2012). The document sets directions to establish privacy audit that provides the following: facilitates compliance with laws and regulations, identifies potential inconsistencies between policies and practices, provides information for a data protection system review, and provides assurance over reputation risks. See Table 4 in Appendix B for more IPPF recommendations on privacy risks mitigation.

ISACA CSX for security in mobile devices (ISACA, 2012) establishes a uniform management framework and provides guidance on planning, and implementing and maintaining comprehensive security for a mobile device in the context of enterprises. CSX for security also provides guidance on how to embed security for mobile devices in a corporate governance, risk management, and compliance strategy. ISACA CSX recommends organisations to establish data classification for information resident on, or flowing through, mobile devices and cloud services. The main objective of data classification is to prevent disclosure of classified information to unauthorised individuals (ISACA, 2012).

Since BYOD and IoT programs in the K-12 environment can add to the potential risks of information misuse in terms of user privacy, this research additionally considers recommendations provided in NIST Privacy Risk Management Framework (NIST, 2015). The document offers a consistent, repeatable process for evaluating privacy risk. It also evaluates the systems that are involved in the processing of information in a new program such as BYOD or IoT (NIST, 2015). Although the PRMF document does not examine specific controls or their applicability to specific privacy risks, the documents mentioned above can be used to enable an appropriate control environment.

3 Methodology and discussion of results

This research has studied the usage of mobile and embedded devices in K-12 schools in an attempt to identify issues related to the use of personally-owned mobile handheld devices for teaching, learning, and administration. The research identifies and discusses BYOD and IoT security-related issues and considerations from the student, faculty, and staff perspectives. Some mobile device and embedded device good practices relevant to the K-12 environment were identified and incorporated into BYOD guides for K-12 systems in the Canadian provinces of Alberta and Manitoba. The following research questions were put forward in this project:

1 What privacy impact factors should be considered when K-12 schools adopt mobile and embedded devices?

2 What additional good practices ought to be included in the current Alberta and Manitoba's BYOD guide for schools?

The subsequent sections and appendices discuss these questions and outline main recommendations for BYOD/IoT programs for K-12 environment.

The first research question focuses on privacy impact factors that ought to be considered when K-12 schools adopt mobile device or embedded device programs. To this end, we advocate the use of NIST Privacy Risk Management Framework (NIST, 2015), as a tool to help prioritise various privacy and security issues. Prioritising various privacy and security issues will also help schools in knowing factors to put into consideration when addressing privacy and security issues. The primary objective of PRMF is to enable K-12 schools to determine the source of privacy risks in the information system. First, NIST PRMF examines the systems likely to be involved in processing students' information. Second, it determines and prioritises factors that can impact K-12 BYOD/IoT programs. Lastly, the document determines the risks per data action based on likelihood and impact factors.

As per NIST PRMF recommendations, three tables have been developed for privacy assessment. The tables are located in Appendix A. Table 1 is the likelihood table, which analyses systems likely to be involved in the processing of information in a mobile/embedded learning environment. The likelihood table is divided into five sections: data action (DA), personal information (PI), problematic data action (PDA), individual potential problem (IPP) and scale of likelihood (SOC). The data action (DA) section contains the possible systems that can be involved in processing personal information in a K-12 environment, e.g., end users device, mobile applications, etc. The example used in Table 1 shows that DA1 has the highest number of likelihood followed by DA2 and DA3 respectively. The business impact factor table – Table 2 in Appendix A – determines and prioritises the factors that can impact a K-12 BYOD/IoT programs. In the example used in Table 2, DA1 has the highest business impact factor based on potential problems to individuals and DA3 has the lowest value. Which means DA1 has to be considered first and DA3 should be least important when making decisions on factors to consider when adopting a BYOD program. The third table is the data action risk prioritisation table – Table 3. The data action risk prioritisation table estimates risk per data action using the results of the likelihood table and the business impact table. The example used in Table 3 shows that the topmost priority should be given to DA1 followed by DA2 when making the decision to mitigate risks on data action. DA1 needed urgent attention because it had the highest value based on likelihood and impact.

The NIST PRMF template helps schools to identify and prioritise privacy risks on data actions. Prioritisation enables schools to allocate and appropriate resources to address privacy risks. Having prioritised and decided the factors, schools can then select and implement a suitable control from the proposed good practice table—Table 4 in Appendix B – to mitigate the risks. It should be noted that assigned values in all NIST PRMF tables are for illustration purposes to introduce the reader to the assessment process. The actual number will depend on the environment where the BYOD/IoT program is being developed.

For the second research question, this paper provides non-industry specific BYOD practices derived from the literature review process in the background section. The proposed good practices table – Table 4 in Appendix B – presents the reader with fifty-one (51) information security and privacy good practices based on a review of four standards and position papers from different information security and auditing organisations.

The process used to fill out the proposed good practices table (Table 4 in Appendix B) was derived from the NIST Risk impact assessment table in Appendix A. The proposed good practices are meant to mitigate the risks derived from the NIST risk impact assessment table. It should be noted that values assigned to tables in Appendix A are for illustration purposes only. Actual values should be based on the particular K-12 school adopting the BYOD/IoT program. The category and sub category columns in Table 4 are based on the risks categorised in the background section of this research.

The compiled good practices are categorised into three main sections: policy and procedures, technical controls, and privacy risk controls. Each of these main sections are, in turn, broken down into a more specific sub categories namely, account monitoring, usage and control, wireless and device access control, data security, end user device security, malware protection and application security. A reference is provided for each good practice presented. For effective governance and management of BYOD/IoT programs in K-12 schools, the proposed policies and procedures should be communicated to the appropriate department. The technical and privacy controls should be aligned with the schools information security management program(s).

The next step to address the second research question was to incorporate all applicable good practices derived in the first phase into the 2012 edition of the Alberta K-12 BYOD document and Manitoba BYOD guide for schools. The purpose of this step was to help mitigate some identified risks outlined in Appendices A through C. Table 5 in Appendix B shows the good practices proposed in this research being mapped to section three, six, and seven in the Alberta BYOD guide. Table 6 in Appendix B shows the good practices being mapped to section two, three, and four in the Manitoba BYOD guide. The short codes used in the 'applicable good practices category' can be cross-referenced with the proposed good practices table: Table 4 in Appendix B. The good practices incorporated into the guide helps to address issues related to ethical usage of mobile devices, information security, and privacy risks.

4 Conclusions

This research highlighted the privacy impact factors to consider in K-12 BYOD/IoT programs. The factors to consider are the business impact factors, which includes reputation costs, direct business costs due to data breaches, and cost of non-compliance with governance, policies, and procedures. These business impact factors, also called considerable factors, were derived from the NIST Privacy risk framework template. The considerable factors were prioritised to enable K-12 schools to allocate appropriate resources to the factors that need considerable attention. This research also compiled and categorised 51 specific BYOD/IoT good practices from four information security and auditing standards. The complied good practices address areas such as access to the school network, school network security, data security, IoT device vulnerability, end user's device security, and mobile application security, privacy of data, policies, and governance. For illustration purposes, this research paper incorporated the proposed good practices into the appropriate section of the Alberta BYOD guide for schools and the Manitoba BYOD guide for schools.

The good practices proposed in this paper provide a safe approach to address the major security and privacy areas for mobile and embedded devices usage in the K-12 environment. The integration of the good practices and risk privacy template into BYOD guide for K-12 will help school administrators to identify the risks users and their devices pose to the network environment. The good practices will also help to assess the risks users and devices pose to systems before granting access to users, while users are on the network and after leaving the network. It is expected that this research will be able to contribute to K-12 schools BYOD/IoT program in terms of good practices in mitigating the security risks and privacy issues. The methodology outlined in this research could also be used to assist K-12 schools in other provinces to update their respective BYOD guides in regular intervals. For the future research the good practices and factors highlighted in this research can be embedded as controls in mobile/embedded device management solutions software for K-12 schools. Other standards and categories of good practices can also be added depending on each school's needs or legislation environment.

References

Alberta Education (2012) *Bring your Own Device: A Guide for Schools*, Alberta Education, Edmonton.

Augur, H. (2015) *Iot in Education: The Internet of School Things*, 7 December, Dataconomy [online] http://dataconomy.com/iot-in-education-the-internet-of-school-things/ (accessed 17 August 2016).

Bruder, P. (2014) 'GADGETS GO TO SCHOOL: the benefits and risks of BYOD (Bring Your Own Device)', *Education Digest*, November, Vol. 80, No. 3, p.15.

Cloud Security Allaince (2012) *Security Guidance for Critical Areas of Mobile Computing*, November, V1.0, Retrieved from Cloud Security Allaince, USA [online] https://downloads.cloudsecurityalliance.org/initiatives/mobile/Mobile_Guidance_v1.pdf (10 November 2015).

Ernst & Young (2013) *Bring your Own Device: Bring your Own Device: Security and Risk Considerations for your Mobile Device Program*, Ernst & Young [online] http://www.ey.com/Publication/vwLUAssets/EY_-_Bring_your_own_device:_mobile_security_and_risk/$FILE/Bring_your_own_device.pdf (accessed 22 September 2015).

Hill, K. (2013) *Baby Monitor Hack' Could Happen To 40,000 Other Foscam Users*, 27 August, Forbes [online] http://www.forbes.com/sites/kashmirhill/2013/08/27/baby-monitor-hack-could-happen-to-40000-other-foscam-users/ (accessed 11 August 2016).

Institute of Internal Auditors (2012) *International Professional Practices Framework (IPPF) for Auditing Privacy Risks*. Institute of Internal Auditors, Altamonte Springs, FL.

ISACA (2012) *Securing Mobile Devices*, ISACA.

K 12 Blueprint. (n.d.) *Mobility Emerges as the Next Wave*, K 12 Blueprint [online] https://www.k12blueprint.com/sites/default/files/Mobility_Next_Wave_K-12_Innovation.pdf (accessed 15 October 2015).

Krueger, K. and Moore, B. (2015) 'New technology 'clouds' student data privacy', *Phi Delta Kappan*, February, Vol. 96, No. 5 [online] http://pdk.sagepub.com/content/96/5/19.full.pdf+html (accessed 17 October 2015).

McDonough, A. (2010) *More Is More*, 1 October, THE Journal [online] https://thejournal.com/Articles/2008/10/01/More-Is-More.aspx (accessed 15 October 2015).

Microsoft (2013) *BYOD in Education: A Practical Guide that Will Get You Thinking*, Presentation, Redmond, WA.

Miller, K.W., Voas, J. and Hurlb, G.F. (2012) 'BYOD: security and privacy considerations', *IT Professional*, Vol. 14, No. 5, pp.53–55.

Mukhopadhyay, S.C. and Suryadevara, N.K. (2012) *Internet of Things: Challenges and Opportunities*, Internet of Things: Challenges and Opportunities, Springer, Basel, Switzerland, Copyright 2014.

Nillson, B. (2015) *Is Your School An Internet of Things Smart School?*, 20 November, Extreme Networks, San Jose, CA [online] http://www.extremenetworks.com/is-your-school-an-internet-of-things-smart-school/ (accessed 23 August 2016).

NIST (2014) *NIST Special Publication 800-53A Revision 4: Assessing Security and Privacy Controls in Federal Information Systems and Organizations*, National Institute of Standards and Technology, Gaithersburg, MD.

NIST (2015) *NIST 8062: Privacy Risk Management for Federal Information Systems*, National Institute of Standards and Technology, Gaithersburg, MD.

Poll, H. (2015) *Pearson Student Mobile Device Survey 2015. National Report: Students in Grades 4-12*, June, Pearson [online] http://www.pearsoned.com/wp-content/uploads/2015-Pearson-Student-Mobile-Device-Survey-Grades-4-12.pdf (accessed 28 September 2015).

Sangani, K. (2013) 'BYOD to the classroom', *Engineering & Technology*, Vol. 8, No. 3, pp.42–45, doi:10.1049/et.2013.0304.

SANS (2016) *The CIS Critical Security Controls for Effective Cyber Defense*, SANS Institute [online] https://www.sans.org/critical-security-controls (accessed 15 October 2015).

Sansurooh, K. and Williams, P. (2014) 'BYOD in eHealth: Herding cats and stable doors, or a catastrophe waiting to happen?', *Australian eHealth Informatics and Security Conference*, pp.28–34, SRI Security Research Institute, Edith Cowan University, Perth, doi: 10.4225/75/5798284331b46.

Selinger, M., Sepulveda, A. and Buchan, J. (2013) *Education and the Internet of Everything: How Ubiquitous Connectedness Can Help Transform Pedagogy*, Cisco [online] http://www.cisco.com/c/dam/en_us/solutions/industries/docs/education/education_internet.pdf (accessed 2 September 2016).

Smith, M., Worell-Burrus, P. and Davis, K. (2014) 'Are we ready for BYOD?', *Journal of the Effective Schools Project*, XXI.

Symantec (2015) *Internet security Threat Report Appendices*, Symantec [online] https://www4.symantec.com/mktginfo/whitepaper/ISTR/21347931_GA-internet-security-threat-report-volume-20-2015-appendices.pdf (accessed 20 June 2015).

Symantec (2016) *2016 Internet Security Threat Report*, Symantec [online] https://www.symantec.com/security-center/threat-report (accessed 15 August 2016).

Timbs, N.H. (2013) *Physical Security Assessment of a Regional University Computer Network*, East Tennessee State University, Johnson City, TN.

Watters, A. (2013) *Students Are 'Hacking' Their School-Issued iPads: Good for Them*, 2 October, The Atlantic [online] http://www.theatlantic.com/technology/archive/2013/10/students-are-hacking-their-school-issued-ipads-good-for-them/280196/ (accessed 19 May 2015).

Appendix A

Privacy risk management framework using NIST 8062

Table 1 Likelihood table

Data action (DA)	*Personal information (PI)*	*Problematic data action (PDA)*	*Individual potential problem (IPP)*	**Scale of likelihood (SOC)*
Information collected from access to the network (DA1)	• Names • Postal code • Date of birth • Student number • Email address • Grade	• Appropriation • Distortion • Insecurity • Surveillance • Unwarranted restriction	Loss of trust Economic loss Exclusion	8 7 4
Information collected from end user device (DA2)	• Phone number • Email address • Age • Grade • Contact • Type of device	• Appropriation • Insecurity • Unanticipated revelation	Power imbalance Stigmatization Loss of trust	6 4 5
Information collected from mobile applications (DA3)	• Phone number • Email contact • Calendar data • Device location • Device unique ID	• Induced disclosure • Surveillance	Loss of liberty	6

Note: *Scale of Likelihood is measured from 1-10

Source: NIST 8062 [25], p.48

Table 2 Business impact factors

Data actions (DA)	*Individual potential problem (IPP)*	*Business impact factors*			*Total business impact**
		Non-compliance costs (on the scale of 1-10)	*Direct business costs (on the scale of 1-10)*	*Reputation costs (on the scale of 1-10)*	
DA 1	Loss of trust	9	9	9	27
	Economic loss	8	7	8	23
	Exclusion	7	6	7	20
DA 2	Power imbalance	4	2	2	8
	Stigmatisation	7	7	6	20
	Loss of trust	9	9	9	27
DA 3	Loss of liberty	6	7	5	18

Note: *Total Business Impact = Non-compliance Costs + Direct Business Costs + Reputational Costs

Source: NIST 8062 [25], p.49

Table 3 Risk per data action

Data actions (DA)	*Individual potential problem (IPP)*	*Scale of likelihood (SOC)*	*Business impact*	*Risk per potential problem*	**Risk per data action*
DA 1	Loss of trust	8	27	216	457
	Economic loss	7	23	161	
	Exclusion	4	20	80	
DA 2	Power imbalance	6	8	48	163
	Stigmatization	4	20	80	
	Loss of trust	5	27	35	
DA3	Loss of liberty	6	18	108	108

Note: *Risk per data action is the addition of all risk per potential problem

Source: NIST 8062[25], p.50

It should be noted that assigned values in all NIST PRMF tables are for illustration purposes. Actual numbers should be based in the risk assessment.

Glossary of terms in Tables 1 to 3:

- Appropriation – Appropriation occurs when personal information is used in ways that an individual would object to. Privacy harm that appropriation can lead to include loss of trust and economic loss.
- Insecurity – lapses in data security can result in loss of trust, as well as exposing individuals to economic loss
- Surveillance – Although tracking and monitoring can be very narrow in terms of surveillance. Tracking maybe conducted for operational purposes such as protection from cyber threats or to better services, but it becomes surveillance when it leads to harms such as loss of trust and loss of liberty
- Unwarranted Restrictions- This involves blocking tangible access to the user and limiting awareness of the personal information in the system. Such restrictions of access can result in harms such as exclusion
- Unanticipated Revelation – Non- context use of data exposes facets of an individual many ways. This can give rise to stigmatization and power imbalance.
- Induced Disclosure – induced disclosure include leveraging access or privilege to an essential services. It can lead to surveillance and loss of liberty.
- Loss of Trust – the breach of the medium handling this personal information will resulted in loss of trust from the user and it will leave individual reluctant to engage BYOD. The probability or likelihood that this will become problematic
- Economic Loss – losses on the part of government as there will be extra budget funding to savage the infringement and financial loss on the individual due to identity theft.
- Exclusion – unauthorized access to names of students can resulted in social exclusion to the individual

- Power imbalance – acquisition of information about types of device been used by student can resulted in supporting one device over another. It can also cause unwarranted web advert to be directed towards the individual.
- Stigmatization – information on type of device can resulted in discrimination social economic category of the individual.
- Loss of trust – unauthorized access to phone number and email address can reduced the level of confidence placed on the authority. Loss of liberty - information about device location can resulted in loss of liberty if accessed by unauthorized individual.

Appendix B

Compiled BYOD good practices mapped to BYOD guide for schools

Table 4 Proposed good practices

Category	*Sub category*	*Good practices*		*Reference*
Policy and procedures (CAT-1)		A	Create a mobile acceptable usage policy and mobile device security standard. It should define	ISACA (CSX)
			I Ethical usage	
			II Types of mobile devices allowed	
			III Approved applications	
			IV Usage of web services and application	
		B	Align mobile device use policy and security standard to legislation and regulation	ISACA (CSX)
		C	Align mobile device security standard with risk management policy	ISACA (CSX)
		D	Develop or review and update Access control policy. The policy should define personnel and roles, responsibility and procedures	NIST (AC-1)
		E	Develop and implement a software/firmware management policy controls for IoT devices	NIST (CM-2)
		F	Ensure there is a well written data and privacy policy. The policy should state procedure for collection, use, retention and disposal of personal information	IIA
		G	Review current policies, standards, and procedures related to privacy of personal information. It should address areas such as data classification and record management	IIA
		H	Develop and documents procedures to facilitate the implementation of training policy and associated awareness	NIST (AT-1)
Technical controls (CAT-2)	Account monitoring, usage and control (SUB CAT-1)	A	Create a role based account for users and assign privileges to administrator and user. Review account status and privileges periodically to reflect organisational missions/business needs	NIST (AC-2)
		B	Ensure all user account have a strong passwords that contain letters, numbers and special characters	SANS (CSC 16-8)
		C	Ensure that account usernames and passwords are encrypted and associated password hash files are stored securely	SANS (CSC 16-17)
		D	Ensure all account have expiration date and determine the length of revocation of users	SANS (CSC 16-2)
		E	Establish and follow a process for revoking or disabling user account	SANS (CSC 16-4)
		F	Monitor usage of account and create a report of user account regularly	SANS (CSC 16-5,7)
		G	Create a system notification or banner by the information system to user before granting access to the system	NIST (AC-8)
		H	The information display to users before granting access provides privacy and security notices with applicable laws, policies, regulation, standard and guidance. It should also indicate information system may be monitored, recorded and subject to audit	NIST (AC-8).

Table 4 Proposed good practices (continued)

Category	*Sub category*	*Good practices*		*Reference*
Technical controls (CAT-2)	Wireless and device access control (SUB CAT-2)	A	List the type of mobile devices by authorising officer to be use on the facilities	NIST (AC-19)
		B	Usage of non-permitted mobile device on the facilities requires approval from authorising official	NIST (AC-19)
		C	Ensure each wireless device connected to the network matches an authorised configuration	SANS (CSC 7-1)
		D	Ensure that all wireless traffic leverages at least Advance Encryption standard (AES) encryption and used with at least WI-FI protected Access 2 (WPA2)	SANS (CSC 7-6)
		E	Ensure that network use authentication protocols such as Extensible Authentication Protocol- Transport layer security (EAP/TLS), which provide credential protection and mutual authentication	SANS (CSC 7-6)
		F	appropriate logging and monitoring should be applied to enable recording and detection of actions that may affect, or are relevant to, information security	SANS CSC
Technical controls (CAT-2)	Data security (SUB CAT-3)	A	Establish data classification for information resident on or flowing through mobile devices. Include cloud services and storage	ISACA (CSX)
		B	Encrypt and encapsulate individually protect sensitive information before moving to cloud	ISACA (CSX)
	Data at rest (SUB CAT 3-1)	A	maintain the confidential, integrity of information at rest	NIST (SC -28)
		B	Perform assessment of data to identify sensitive information that requires application of encryption and integrity control	SANS CSC
		C	Conduct periodic scans of server machines that holds sensitive information (i.e., PII) to identifying if there is any leak in sensitive information	SANS (CSC 17-6)
	Data in transit (SUB CAT 3-2)	A	Enforce detailed audit logging for non-public data and special authentication for sensitive data	SANS (CSC 15-2)
		B	Review cloud provider security practices for data protection	SANS (CSC 17-4)
	End user device security (SUB CAT-4)	A	Define the types of digital or non-digital media permitted and restricts access to non-permitted types of digital or non-digital media	NIST (MP -2)
	End user device security (SUB CAT-4)	B	Define the nature of services accessible through the devices taking into account the existing IT architecture	ISACA
		C	For proving support to various device turn to cross platform centrally managed mobile device manager	ISACA
		D	Implement a central management console for device remote, i.e., data wipe out password /PIN change or strong user authentication	ISACA
		E	Integrate all enterprise issued devices into an asset management program	ISACA
		F	Educate end users about mobile security and provide useful tools for user self-protection	ISACA (CSX)

Table 4 Proposed good practices (continued)

Category	*Sub category*		*Good practices*	*Reference*
Technical control (CAT-2)	Malware protection (SUB CAT-5)	A	Employ anti-malware software that offers a remote, cloud based centralised infrastructure	SANS (CSC 5-2)
		B	Configure anti malware protection mechanism to block, quarantine and send alert to administrator in response to malicious code detection	NIST (SI-3)
		C	Use automation to ensure anti-virus signatures are up to date	SANS (CSC 5-1)
		D	Extend protective measure to mobile device, and ensure that they're functional and effective without users having to bring the device	ISACA (CSX)
		E	Implement procedure to address the receipt of false positive relating to malware. Reputable journals and reliable journal on information security and assurance can be helpful	NIST (SI-3)
	Application security (SUB CAT-6)	A	For all acquired application software, check the version you are using is still supported by the vendor. If not, update to the most current version and install all relevant patches and security recommendations	SANS (CSC 6-1)
		B	Protect web application by deploying Web Application firewalls. For application that are not web based, specific application firewall should be deployed	SANS (CSC 6-2)
		C	For acquired applications that rely on a database and critical to business process, use standard hardening configuration template and should also be tested	SANS (CSC 6-9)
	Application security (SUB CAT-6)	D	Examine security process of application software (history of vulnerabilities, customer notification) for overall risk management process	CSC 6-8
		E	Apply required controls on application handling and process personal information in house or in cloud	IIA
		F	Establish software lifecycle controls for Apps develop in-house or acquired	ISACA (CSX)
IoT vulnerability management (CAT-3)	IoT software/firmware security (SUB CAT-7)	A	Establish and ensure the use of standard secure software/firmware configurations on IoT devices	CSC (3-1)
		B	Evaluate software/firmware upgrade and critical patches in live environment before installing them on IoT devices	SANS (CSC 4-9)
		C	Implements cryptographic mechanisms to authenticate organisation-defined software components of IoT device prior to installation	NIST (SI-7(15))
		D	Run automated vulnerability scanning tools against all IoT devices on the network on a weekly or more frequent basis	CSC (4-1)
	IoT device integrity (SUB CAT-8)	A	Utilise file integrity checking tools to ensure that critical system files on embedded devices have not been altered	CSC (3-8)
		B	Manage IoT devices using two-factor authentication and encrypted sessions	CSC (10-4)
		C	Ensure remote administration of IoT devices, over secure channels. Protocol such as telnet can be used with a secondary encryption channel, such as SSL or IPSEC	CSC (3-7)

Table 4 Proposed good practices (continued)

Category	*Sub category*	*Good practices*		*Reference*
IoT vulnerability management (CAT-3)	IoT device interface security (SUB CAT-9)	A	Connect IoT devices to external networks or information systems only through managed interfaces consisting of boundary protection devices (e.g., proxies, firewall, encrypted tunnel, etc.)	NIST (SC-7c)
		B	Define components of IoT device to be authorised as internal connections to the information system. Documents, for each internal connection for IoT devices: the interface characteristics; the security requirement; the nature of information communicated	NIST (CA-3b)
	IoT device interface security (SUB CAT-9)	C	Implements subnetworks for publicly accessible IoT devices that are either: physically separated from internal organisational networks; and/or logically separated from internal organisational networks	NIST (SC-7b)
		D	Obtain end user permission to store, process and use personal information	ISACA (CSX)
Privacy risk control (CAT-4)		A	Liaise with legal department to understand law and regulations concerning privacy in the jurisdiction, e.g., School Act, FOIP, PIPEDA, PIPA	IIA
		B	Separate personal identity of user from technical identity of the media device	ISACA (CSX)
		C	Segregate between trusted device and untrusted device. It can be divided into separate network domain	ISACA (CSX)
		D	Liaise with IT specialists to understand information flows, system control, storage and use of personal information	IIA
		E	Ensures that the information system is configured so that data or information collected by mobile device/ embedded device is only reported to authorise individuals	NIST (SC-42(1))
		F	Implement a privacy risk management process that assesses privacy risk to individuals resulting from the collection, sharing, storing, transmitting, use, and disposal of personally identifiable information (PII)	NIST (AR-2)

Table 5 Good practices mapped to Alberta BYOD guide for schools

Relevant sections of Alberta BYOD guide	*Relevant sub sections of BYOD guide for schools*	*Applicable good practices category (see Table 4)*
Section 3: Policy consideration	Responsible/appropriate use of personally owned devices	CAT-1
	Network access/bandwidth for students	
Section 6: Digital content	Privacy of student and faculty	SUB CAT-3, SUB CAT 3-1, SUB CAT-5
Section 7: Access and infrastructure considerations for BYOD model	Networks, wireless technology and bandwidth	SUB CAT-1, SUB CAT-2, SUB CAT-5
	Suite applications	SUB CAT-6
	Cloud computing	SUB CAT-3, SUB CAT 3-1, SUB CAT 3-2

Table 6 Good practices mapped to Manitoba BYOD guide for schools

Relevant sections of Manitoba BYOD guide	*Relevant sub sections of BYOD guide for schools*	*Applicable good Practices Category (see Table 4)*
BYOD policy consideration, safe and appropriate use of technology	Appropriate usage policy	CAT-1
	Privacy of student and faculty	SUB CAT-1, CAT-4
BYOD Infrastructure and security issues	Access points	SUB CAT-2
	Network reliability	SUB CAT-4, SUB CAT-3, SUB CAT 3-1, SUB CAT 3-2
	Network security	SUB CAT-2, SUB CAT-4, SUB CAT-5, SUB CAT-7
	Cloud computing	SUB CAT 3-2, SUB CAT-3 SUB CAT-4