Cybersecurity for information professionals: The personal dimension

Matt Moore and Kelly Tall*

Cybersecurity issues are becoming more pervasive and prevalent in our lives as technology infiltrates more of our experience. This article explores the challenges that we face as individuals from a broad range of risks. It also presents a case study on eSmart Libraries as an initiative that enables information professionals to deal more effectively with these issues.

INTRODUCTION

One of the key themes of the articles we have written for this publication is that "software is eating the world".[1] To put it another way, many everyday activities and objections are being transformed by internet-based technologies. This is not necessarily a sinister plot. This is happening because most of us benefit in the process. If we want to buy, sell, rent, hire, talk, shout or share, this internet-enabled world helps us do that more easily. However, this process is not all hugs, puppies and emojis. These technologies transform our relationships with each other in ways that are not wholly healthy and may expose us to shame and ridicule. They also may compromise our property and physical safety. How will we deal with this collectively and individually?

"Cybersecurity" is a growing area of attention for government, companies and individuals. 2014 offered many examples including the hacking of nude photos of Jennifer Lawrence and the release of large quantities of sensitive information from the Sony Corporation by individuals who may be associated with North Korea.

This article will:

- explore the personal implications of cybersecurity. What risks do we face as individuals?
- look at the range of technical threats cybersecurity tries to protect against. How do these threats manifest themselves and what does that mean for prevention?
- discuss cybersecurity initiatives that impact information professionals such as the eSmart libraries program.

An upcoming article will examine the organisational issues around cybersecurity.

THE PERSONAL IMPLICATIONS OF CYBERSECURITY

Crime is an ever-present threat in our society;[2] however, it may not be as prevalent as some perceive it to be – crime rates in Australia have been trending down since the 1990s.[3] Crime is fundamentally a human activity so as our society becomes more virtualised through the internet, it is inevitable that we will see more criminal activity expressed through this new medium. Technology has the opportunity to reduce some kinds of crime (such as property theft) but as crime is best understood as

* Matt Moore has spent 15 years working in knowledge and information management, learning and development and internal communications with organisations such as IBM, Oracle and the Australian Securities and Investment Commission. He lectures at the University of Technology Sydney and is a former chair of the New South Wales Knowledge Management Forum. Kelly Tall is an experienced market researcher with a passion for data visualisation. She has worked with many well-known global and Australian brands.

Many thanks to Jacqui Kinder (AMF) and Sue McKerracher (ALIA) for their assistance with the eSmart Libraries case study. All websites viewed April 2015.

[1] Andreessen M, "Why Software is Eating the World", *The Wall Street Journal* (20 August 2011), http://www.wsj.com/articles/SB10001424053111903480904576512250915629460.

[2] Australian Bureau of Statistics, *Crime Victimisation Survey* (2015), http://www.abs.gov.au/AUSSTATS/abs@.nsf/Lookup/4530.0Main+Features12013-14?OpenDocument.

[3] Davis B and Dossetor K, *(Mis)perceptions of Crime in Australia* (2010), http://www.aic.gov.au/publications/current%20series/tandi/381-400/tandi396.html.

"behaviour that is collectively disapproved of", as much as technology expands the reach and impact of our behaviour, so it potentially contributes towards crime. It expands our potential to be bad as well as good.

To get a sense of the variety of security issues that the general public faces, we turn to the Pew Research Center. In 2013, they surveyed[4] Americans about online security issues they had faced. The responses they received indicated that:

- 21% of internet users have had an email or social networking account compromised or taken over without their permission
- 12% have been stalked or harassed online
- 11% have had important personal information stolen such as their social security number, credit card, or bank account information
- 6% have had their reputation damaged because of something that happened online
- 6% have been the victim of an online scam and lost money
- 4% have had something happen online that led them into physical danger.

Of equal interest was the list of those they might want to protect their personal information:

- 33% of internet users said they had tried to hide their activities from hackers or criminals
- 28% said they had tried to hide their activities from advertisers
- 19% said they had tried to hide their activities from people in their past
- 19% said they had tried to hide their activities from certain friends
- 17% said they had tried to hide their activities from people who might criticise, harass, or target them
- 14% said they had tried to hide their activities from family members or a romantic partner
- 11% said they had tried to hide their activities from an employer, supervisor, or coworkers
- 6% said they had tried to hide their activities from companies or people who run the websites they visit
- 6% said they had tried to hide their activities from companies or people that might want payment for the files they downloaded such as songs, movies, or games
- 5% said they had tried to hide their activities from the government
- 4% said they had tried to hide their activities from law enforcement.

This is a heterogeneous group of people. It is not just good guys and bad guys. Indeed, many of those who are viewed as "threats" would not necessarily see themselves as such.

As can be seen above, individuals face a range of threats from personal harassment to identity theft and financial loss. The compromising of personal communication services is relatively common. While this does not always lead to a material loss, it is nevertheless unpleasant – in much the same way as having a stranger rifle through your belongings feels. The relative insecurity of users' personal communications tools has important implications for organisations. Many people use personal email and file-sharing accounts to get around corporate limitations on document-sharing and collaboration. These limitations are driven by security considerations but may have unintended consequences – ie their inconvenience drives employees to use less secure collaboration mechanisms.

Even more concerning is that 12% of respondents had been stalked or harassed online. Online harassment may take the form of one individual paying unwanted attention to another, abusive comments on social networking sites and discussions forums or the sharing of private information such as photographs. Cyberbullying can impact anyone but is a particular concern for children and teens. In 2011, 72% of Australian teenagers surveyed said that they had been the object of unwanted or unpleasant contact by strangers via their social networking profile.[5]

[4] Raine L et al, *Anonymity, Privacy, and Security Online* (2013), http://pewinternet.org/Reports/2013/Anonymity-online.aspx.

[5] de Zwart M et al, *Teenagers, Legal Risks and Social Networking Sites* (2011), http://newmediaresearch.educ.monash.edu.au/lnmrg/article/teenagers-legal-risks-and-social-networking-sites.

Online harassment need not be a matter of only one or two harassers. The internet is a mass medium. In 2014, "Gamergate" brought this into sharp relief.[6] What began as the apparent fallout from a messy love affair between two people quickly escalated into social media mob attacks on individuals – especially women in the technology industry. These included everything from doxxing (where you publish private information about an individual such as their real name or their physical address) to threats of rape and murder. Campaigns of harassment against individuals, their acquaintances or those with whom they have a commercial relationship (employers, sponsors, customers) were coordinated on social media platforms and discussion boards.

Online harassment can have a lasting impact on someone even if it does not escalate to a physical threat. This can be in terms of their mental health but also their career. Looking at prospective employees' social media profiles has become the norm in many organisations. Hence the fourth item on the list – reputational damage. This can be especially severe if it is the result of an internet mob – as the negative material about you can be spread across multiple online platforms and multiple user accounts.[7] This has given rise to businesses such as reputation.com[8] that offer to repair an individual's online reputation. The techniques they deploy include swamping negative content and search results with neutral or positive information and identifying personal information inadvertently exposed through social media services.

This focus on reputation is reminiscent of a bygone world. The characters of Jane Austen are similarly concerned with their reputations – at the edge of the landed gentry in their rural worlds, they cannot hide in the anonymity of the modern city. The "global village" of McLuhan is not as reassuring as the metaphor might seem at first. Anyone who has lived in a village knows the intense observation of others' behaviour that goes on. This online village offers a similar level of observation – or surveillance, sousveillance, and coveillance – as Pew put it:[9]

- Surveillance is observation by those in power. Since 9/11, states have been claiming the need for greater powers to track the activities of their citizens for national security purposes. The response to the NASA-Snowden revelations and the mandatory metadata retention scheme indicates that not all citizens are comfortable with these claims.
- Sousveillance suggests the inverse. This may mean citizens reporting on governments. Sites like openaustralia.org or theyworkforyou.com attempt to make public information.
- Coveillance, or as UK comedian Stewart Lee puts it:

> If I was to have a mental breakdown and forget anything that had ever happened to me, it wouldn't matter because I could just go on Twitter and put my name into the search engine and I would gradually be able to piece together everything that had happened to me because every 90 minutes one of you feels obliged to go online and do a live update of where I am and what I'm doing … I hate Twitter. It's like a state surveillance agency run by gullible volunteers. A Stasi for the Angry Birds generation.[10]

This sense of exposure is neither constant nor absolute but it arises in real life and we become conscious of it. Many people google those they have first dates and business meetings with. We are "on show", whether we like it or not.

The third and fifth of Pew's security issues dealt with theft. Even with the improvement in spam filtering over the last few years, attempts at online fraud are common. In Australia, 97% of respondents to the consumer fraud taskforce survey had received a scam of some kind (eg fake lottery wins, phishing, bogus computer support) with email as the most significant delivery channel. Around

[6] Hathaway J, "What is Gamergate, and Why? An Explainer for Non-Geeks", *Gawker* (2014), http://gawker.com/what-is-gamergate-and-why-an-explainer-for-non-geeks-1642909080.

[7] Ronson J, "'Overnight, Everything I Loved was Gone': The Internet Shaming of Lindsey Stone", *The Guardian* (21 February 2015), http://www.theguardian.com/technology/2015/feb/21/internet-shaming-lindsey-stone-jon-ronson.

[8] http://www.reputation.com.

[9] Raine L, *Networked Privacy in the Age of Surveillance, Sousveillance, Coveillance* (2015), http://www.pewinternet.org/2015/01/23/networked-privacy-in-the-age-of-surveillance-sousveillance-coveillance.

[10] Lee S, "Stewart Lee vs The Internet", *BBC* (2014), https://www.youtube.com/watch?v=7XpvH-j9BHg.

10% of survey respondents reported a financial loss.[11] Targeting individuals can be very profitable for criminals. While personal information is often targeted to get access to bank or credit card details, it can also be used to apply for loans, passports, benefits, jobs, mobile phone contracts and vehicle registrations. The Pew data indicates that Identity theft may be a bigger problem than simple online robbery.

TYPES OF CYBERSECURITY VULNERABILITIES

As the 2013 Pew Survey indicates, people can be exposed to different kinds of risks from others – and those "others" are not a homogeneous group. Some of these "others" are technically unsophisticated and with limited resources whereas some have great technology and resources at their disposal.

Users can be exposed to unsophisticated threats online simply because they have an online presence. You can block unwanted email, phone numbers and social media messages. The privacy settings on most social networks are changed on a notoriously frequent basis so users may not be aware of who can see their details and their information. A persistent pest may get a new phone number or email or social media account and therefore can only be stopped by action from law enforcement or the service provider. While there are laws that cover online harassment, their application can vary. Service providers such as Twitter have recently acknowledged that their response to online harassment has been inadequate and they have promised to improve it.

Users may also be threatened by sophisticated, criminal entities. Typically, the techniques that are used include:

- Phishing. You will receive an email that appears to be from a bank, telco or online service provider, informing you of an issue that needs resolving, and providing you with a link to their site. In fact, the link is to a fake site and they want to steal your log-in information. The dumber (and yet still effective) version of phishing is the 419 scam – where you will be told that you have somehow come into a fortune and all you need to do is to send a small sum of money to get it transferred to you.
- Password protection. The passwords that protect many user accounts are either easy to guess ("Password1") or vulnerable to brute force techniques because the minimum possible number of characters for a password are used.
- Unsecured sites. If you are transferring sensitive information such as credit card details via a website then it should be encrypted. Typically this is indicated by an HTTPS in a URL. However, not all web sites have set this up.
- Physical theft of a device. As our devices are becoming more secure and trackable, the benefits of device theft are getting less. Nevertheless this is still a risk. Critical data on a device should be protected through secure passwords and other security features.

Finally users may seek to avoid entities that are acting legally but with interests that they perceive as being different to their own – governments, advertisers and corporates, employers. Users may seek to hide their activities through pseudonymous accounts, encryption, virtual private networks (VPNs) and anonymity networks such as Tor.

eSMART LIBRARIES

The eSmart initiative is a behaviour-change initiative designed to improve cybersafety and deal with cyberbullying and bullying. The project is led by the Alannah and Madeline Foundation (AMF). It began as eSmart Schools,[12] which has been adopted by more than 1,400 schools across Australia since 2010. Discussions with local authorities led to an additional focus on libraries and a reference group was formed including the Australian Library and Information Association (ALIA), the Public Libraries Advisory Committee (PLAC), Public Libraries Australia (PLA) and National and State Libraries Australasia (NSLA), the Telstra Foundation, local government and regional development. AMF and

[11] Jorna P, *Australasian Consumer Fraud Taskforce: Results of the 2013 Online Consumer Fraud Survey* (2015) http://aic.gov.au/publications/current%20series/tbp/41-60/tbp058.html.

[12] http://www.amf.org.au/esmartschools.

the Telstra Foundation formed a partnership in 2012 to develop and implement eSmart Libraries[13] with the involvement of the reference group, backed by an investment of $8 million over six years.

Cybersecurity has been a concern of ALIA since the mid-1990s. Successive governments have thought that internet filtering would be the best way to protect Australians from harm on the internet – especially for vulnerable groups like children. However, the issue with filtering is that it is not effective. For example, while you might filter for a term like "breasts" related to pornography, there is plenty of socially important material on topics like "breast feeding" or "breast cancer" that would be blocked in the process. Rather than rely solely on filtering, ALIA's view of cybersecurity literacy is based on three core principles:

(1) Education. The education of the general public – especially parents, teachers, and children – is key to ensuring their safety.
(2) Policing. We would like to see increased funding for policing of highly objectionable content (eg child pornography).
(3) Filtering. Only with the first two principles in face should filtering be introduced – with a narrow focus rather than broad brush (eg blocking specific sites).

ALIA has supported eSmart in both school and public libraries as a key part of the education process.

The eSmart program had originally been designed for schools so the new program had to move from a focus on the school curriculum to library operations. The eSmart Libraries program offers librarians the following:

- A framework for ensuring cybersecurity within libraries that covers library management in five elements.
- An online system tool that allows libraries to record, track and report their progress over time.
- An online database of resources including videos, games and case studies that support the implementation of the framework.
- Support in the form of training on the eSmart system and helpdesk, telephone and email support.

The framework itself has the following elements:

(1) Library vision, strategy and leadership – an eSmart Library has the capacity to foster smart, safe and responsible use of digital technologies in the community. The library's management has provided a clear mandate for change, reflecting the vision and principles of the organisation and the needs of the library community. The program is steered by the eSmart Libraries Working Group and facilitated by an eSmart Coordinator.
(2) Library agreements and procedures – an eSmart Library has discussed practices and agreements, reviewed and aligned to reinforce cybersafety and wellbeing values so that day-to-day operations in the library exhibit a safe, smart and responsible environment.
(3) Effective staff knowledge and capabilities – an eSmart Library's staff have knowledge of digital technologies, training in cybersafety practices and are capable of responding to inappropriate cyber-behaviours consistently and effectively.
(4) Guidance and learning for users – an eSmart Library offers information, guidance and lessons on how users can utilise the benefits of technology, avoid online pitfalls and be able to embody positive, smart, safe and responsible behaviours online.
(5) Community connections – an eSmart Library enhances connections and reach out to the wider community to promote "eSmart" behaviours, helping to embed cybersafety and wellbeing principles.

The pilot for the program began in early 2013 with 22 library services consisting of 110 branches. Now in its third year, nearly 600 public library branches (out of around 1,500 total across the country) are involved in the program. All States have library systems involved in the program except for Tasmania. The local authorities already engaged include a mix of metropolitan, regional and remote communities. Different States have a different matrix of organisations involved; however, the public library associations within each State have been pivotal in terms of raising awareness about the

[13] http://www.amf.org.au/eSmartlibraries.

program and training library staff. The Public Libraries Victoria Network (PLVN) has been particularly enthusiastic in engaging its membership, featuring case studies from pilot libraries at its meetings. Victorian councils have also made it easy for libraries to use the eSmart systems tools. Therefore it is no surprise that the four library services to have moved through registering, planning and implementing to achieving eSmart status (and therefore needing to sustain their implementation) are all based in Victoria – Bayside, Hume, Wellington, and Campaspe.

In rolling out the program, lessons have been learned. In many libraries, time and resources are scarce so on-demand, self-paced learning tools like videos are appreciated by staff. There also can be the opportunity to use interns and work placement staff to plan and implement cybersecurity projects. In terms of the sequencing of activities, some library services have focused on the education of staff and patrons to gain a baseline level of understanding and engagement before reviewing strategy and operations. Additionally, this means that multiple staff on site can champion the initiative. The online system now allows multiple users from a site to access the materials, although only one person can upload assessments and evidence. Finally, the program can be constrained by the environment in which it operates. Some local authorities have yet to develop the level of digital literacy and focus to prioritise a program like eSmart.

The feedback from librarians and local authority officials has been broadly positive, such as this statement from the mayor of Bayside:

> In our community one of the greatest barriers to the uptake of digital technology is fears about safety online, particularly among older adults. Running regular cybersafety education programs and providing resources via eSmart Libraries helps us achieve our aim of increasing community access to digital technologies.

The Young and Well Cooperative Research Centre has begun an independent evaluation that will likely be published later in 2015. This will include feedback from patrons and data on the impact of the program on cybersecurity incidents in public libraries.

CONCLUSION

Cybersecurity issues are becoming more pervasive and prevalent in our lives as technology infiltrates more of our experience. These issues have many facets. Our lives are complicated and we have to balance the opportunities with the risks that greater connectivity offers. It is not simply a matter of guarding against criminal gangs, rather we need to be more aware and more vigilant in how we manage our information and our activities online. As initiatives like eSmart Libraries demonstrate, information professionals have a key role to play here as educators within their communities, be they public libraries, schools, government or the private sector. We need to begin by understanding the risks for ourselves and then reach out to those around in a sensible, non-alarmist manner. We need to make practical suggestions that can make an immediate difference and we need to do so in a manner and language that is understandable to all.