Annual ADFSL Conference on Digital Forensics, Security and Law
2018 Proceedings

May 18th, 1:00 PM - 1:35 PM

A Survey of Lawyers' Cyber Security Practises in Western Australia

Craig Valli
Edith Cowan University, c.valli@ecu.edu.au

Mike Johnstone
Edith Cowan University, m.johnstone@ecu.edu.au

Rochelle Fleming
Edith Cowan University, r.fleming@ecu.edu.au

A SURVEY OF LAWYERS' CYBER SECURITY PRACTISES IN WESTERN AUSTRALIA

Craig Valli, Mike Johnstone, Rochelle Fleming
Edith Cowan University Security Research Institute
{c.valli, m.johnstone, r.fleming} @ecu.edu.au

ABSTRACT

This paper reports on the results of a survey that is the initial phase of an action research project being conducted with the Law Society of Western Australia. The online survey forms a baseline for the expression of a targeted training regime aimed at improving the cyber security awareness and posture of the membership of the Society. The full complement of over 3000 members were given the opportunity to participate in the survey, with 122 members responding in this initial round. The survey was designed to elicit responses about information technology use and the awareness of good practices with respect to cyber security within the legal profession. The legal profession is one of the most sensitive with respect to loss of information that would affect legal professional privilege where exposure can have catastrophic consequences. We found that, comparable with other professions, lawyers do claim to use effective countermeasures on their laptops, but largely ignore their mobile phones, which highlights a particular class of risks for the profession.

Keywords: Cyber Security, Lawyers

1. INTRODUCTION

The primary principles of information security are confidentiality, integrity and availability. It is not surprising that these principles are important in the legal profession. Confidentiality, with respect to the protection of client information is paramount. Integrity is imperative, as maintaining the chain of evidence is critical. Availability or rather lack of availability is a hidden cost, as lawyers often work on complex cases or multiple matters where case data must be available to several practitioners.

According to Morgan (2016), the global cost of cybercrime quadrupled in the period 2013-15, with Lloyds estimating a cost of USD$400B in 2015. In 2016, it was reported that dozens of law firms in the USA had been compromised for a nation-state to gain access to sensitive client information regarding mergers and acquisitions. The recent successful Wannacry cyber-attack on the multi-national law firm DLA Piper demonstrates that law firms are not immune.

This is a study conducted in co-operation with the Law Society of Western Australia, a professional association with over 3000 members. The membership was surveyed using an online questionnaire, with 122 respondents to the questionnaire. This paper analyses the collected data and provides insight into the habits of lawyers with respect to their use of information technology, and more importantly, their attitudes and use of cyber security to secure their information.

2. GENERAL DEMOGRAPHICS

The questionnaire first sought to examine the demographics of the cohort who responded. The age of the respondents was broken down into various age strata as displayed in Table 1. The majority of respondents were aged between 40 and 59.

Table 1
Age range of Respondents.

Age	**18-30**	**31-39**	**40-49**	**50-59**	**60-69**	**70 plus**
	17.21%	16.39%	27.87%	24.59%	13.93%	0.00%

The questionnaire also asked respondents to identify the type of organisation in which they are currently employed. Table 2 indicates that over half of the respondents work individually or in small partnerships. This may have ramifications for the amount of resources that such firms can put towards cyber security, thus potentially increasing their risk profile.

Table 2
Respondent's Organisation Profile.

	%	Count
A single person practice	27.97%	33
Small partnership < 10	36.44%	43
Medium size partnership	10.17%	12
Large Partnership/Corporate	15.25%	18
National Corporate	2.54%	3
Multi-National	7.63%	9
Total		118

All respondents except one used the Internet to conduct business. When asked what devices they used to connect to the Internet they were allowed multiple answers to cover individuals who use multiple devices. There was a total of 337 responses, 94 used a Desktop PC, 83 used a smart phone, 79 used a laptop, 40 used a tablet, 39 used a corporate network computer and 2 identified as using Internet Cafés. Using number of respondents vs. responses to calculate average devices per person, the result is 2.85. ABS (2017) figures for mobile handset subscriptions across the general population show that there were 26.3 million handsets subscribed at 30/06/2017 (+3.6% from December 2016). Allowing for the segment of the population that is able to hold a subscription and is aligned to the age demographic of the survey, this still means that lawyers are high-volume users of technology.

There were 233 responses to a (multiple selection) question about technology used to access the Internet. The results were: 66 use 3G/4G, 53 use ADSL fixed network, 47 use ADSL wireless, 35 Corporate Network, 15 NBN, 6 Cable and 11 Did not know. Of the respondents, 113 used wireless-based technologies.

3. CYBER SECURITY COUNTERMEASURES DEPLOYED BY RESPONDENTS

There were questions asked about the use of traditional cyber security countermeasures on each device type used. This allowed us to survey and gauge practices by device type previous studies (Valli, Martinus, & Johnstone, 2014) had shown that usage of countermeasures was different across device classes in SMEs.

The first question dealt with countermeasures used on a PC or a laptop device, in essence this could be viewed as "traditional business computer" use. In selected use cases this would mean three decades of use

of this technology for some respondents. There was a total of 312 responses, again it should be noted it was possible to give more than one answer. The results are displayed in Table 3.

Table 3
What cyber security countermeasures do you use on your laptop/PC n=94

Anti-Virus	84	89.36%
Firewall	69	73.40%
Malware Scanner	61	64.89%
Spam killer	31	32.98%
Corporate/Managed Service	55	58.51%
Do not know	12	12.77%

The alarming results here are that 11% of lawyers surveyed do not have basic anti-virus protection on their PC/Laptop and that 27% do not use firewalls. Equally coupled with this is that around 13% did not even know what protection they had on their PC/laptop, although this may be an artefact of the use corporate/managed services and warrants further investigation.

As shown in Table 4, when asked what countermeasure they deployed on their smart phone the responses were significantly lower by comparison.

Table 5
What cyber security countermeasures do you use on your smart phone n=40

Anti-Virus	23	27.71%
Firewall	12	14.46%
Malware Scanner	9	10.84%
Spam Killer	4	4.82%
Managed/Restricted by Corporate	8	9.64%
Do not know	34	40.96%

The most important result here is that one in two tablet users have no idea what cyber security countermeasures are deployed on their tablet device. With tablets replacing laptops for use in businesses as the primary information device this result is of significant concern. Comparative to laptops and desktops also the level of corporate governance and control indicates there is some way to go to get to the same levels of cyber security into tablets as evinced in this survey.

Combining these results into a single representation by technology type is informative and this is represented by Table 6. The percentages are calculated against number of respondents to the questions.

Table 6
Use by countermeasure type by technological platform

	Laptop	***n=94***	**Phone**	***n=83***	**Tablet**	***n=40***
Anti-Virus	84	89.4%	26	31.3%	23	57.5%
Firewall	69	73.4%	13	15.7%	12	30.0%
Malware Scanner	61	64.9%	15	18.1%	9	22.5%
Spam killer	31	33.0%	11	13.3%	5	12.5%
Corporate/Managed Service	55	58.5%	17	20.5%	8	20.0%
Do not know	12	12.8%	36	43.4%	20	50.0%

Table 6 shows that there is a significant and manifest change in percentage uptakes of cyber security countermeasures by broad technology category. The level of ignorance is significant in phone- and tablet-based deployment of standard cyber security countermeasures applied to their devices. The phones are at 43.4% but the zenith of this measurement is 50% for tablets, a worrying trend indeed.

The non-deployment of anti-virus countermeasure is highest on smart phones, which in of itself is problematic on a number of levels. Couple this survey result with the fact that most new malicious code (malware) is produced for phone and tablet platforms and there is a significant but also easily addressable issue with smartphone and tablet use by lawyers. Installing anti-viral software and turning on firewalls will significantly change cyber security posture positively and increase target hardness.

4. CYBER SECURITY PRACTICES

There was a series of questions that investigated practises that surveyed actions that the lawyers would possibly undertake during a day's work. These questions were designed to elicit responses around practices that at face value would seem harmless, however, if one considers 2nd and 3rd order consequences of these actions they could easily be catastrophic in outcome for a lawyer and his/her clients.

The first of these seemingly innocent actions is connection to a wireless network at home or free public Wi-Fi access provided by businesses that lawyers would likely frequent or have cause to use e.g., restaurant, airport, other business or Internet Café. The first part of the question saw that of the 101 lawyers who responded to that question 64% were in the affirmative and 36% in the negative for connection to home wireless.

The second part of the question asked about phishing scams with a perfect response score with 121 respondents answering yes, with 110 of these receiving such emails. Of the 110 who responded 90 have been offered money, 73 were related to a free prize, 67 had been lottery winners and 60 other responses related to other types of phishing email contact. Phishing scams are rarely so clumsy and successful scams are often targeted, sophisticated, multi-layer exercises. Nonetheless, the fact that these emails successfully pass through a mail scanner is a concern.

The next section contained a series of questions about updates and maintenance of systems and devices which is a core requirement for cyber resilient systems. The first question in this section related to frequency of updates on a laptop/PC. Automatic updates were the highest at 71 (58.7%) responses, the 2nd was Do not know at 13 (10.74%), Once a Month 9.09% 11, 2-3 Times a Month 7.44% 9, Less than Once a Month/2-3 Times a Week both at 4.96% 6 and Once a Week 4.13% 5. These results are grim, essentially 41% of PCs/laptops do not have automatic updates which are not ideal in today's cyber space for maximum protection and resilience. Of course, it may be that updates are handled automatically by a corporate IT group, which may explain end users lack of knowledge about updates, as reflected in the responses.

Only 24% of smartphones or tablets have anti-virus installed on them, dismal. However, updates have been applied to 88% of respondent's phone and tablet. 92% of phone or tablet owners download apps and 88% of these only download from Google, Apple or official sites. Less than 10% download from any site which is still problematic in that 1 in 10 users are engaging in potentially dangerous cyber security practices.

When users download the apps 36.5% of respondents actually read the permissions, with

a further 28.7% claiming sometimes. Rarely is the preferred modus operandi for 24.3% and 10.5% never read the permissions. This result comparative to other user studies is high (Cotton & Bolan, 2011), this maybe as a result of respondents chosen profession.

Respondents asked had they accessed any cyber security initiatives by Government, the responses were bleak given that lawyers are sometimes first responders to cybercrime or cyber-related crime. The lowest was the Federal Government ACORN (ACORN, 2017) and StaySmartOnline (Department, 2017) at 5.6% each respectively. The WA State Government website ScamNet (Anonymous, 2017), however, had a comparatively stellar outcome with 30.2% of respondents having accessed it. The grim news is that 58.8% have never accessed any of these cyber security or cybercrime initiatives.

The respondents were asked about the primary provider of cyber security for their business. 21% of respondents administer themselves, 65.4% relied on corporate IT to provide cyber security services, 8.3% employed a cyber security specialist, 3% used a trusted family member and 2.2% did not have anyone.

The question relating to a "cyber attack" and its remedy by participants garnered the following responses. Self-help ran at 21% consistent with primary provider response, 72.5% IT support fixed it, less than 3% either reported it to police or employed the services of a cyber security specialist. No one at all reported the incident to ACORN, and one respondent simply rebooted the machine, and all is well.

Email practices were queried and 94.1% of respondents used email to send confidential documents. The highest response was a frequency of several times a day at 58.4%, followed by 4-6 times a week 17.7%, 2-3 times a week 11.5%, once a week 5.3% and rarely 7.1%. To protect this email in transit only 9.4% of respondents use any form of encryption, with 62.4% using none at all and the remaining 28.2% who do not know. It would be safe to say that 90.6% of respondents do not use any encryption to protect client data in transit.

External access of email via personal devices (home computer, phone) is at 82.6% of respondents to the survey. The implication is that security of these devices will be less rigorous than corporate protections in place. It also begs the question what happens to the documents when an employee leaves the practice. The respondents were asked if they forwarded any work-related emails to a personal non-business account on Gmail or Hotmail 52.9% of users did. When asked as to the frequency of this forwarding 69.8% it was once a week or better, 42.9% overall on a daily basis, there was some respite with 30.2% at rarely.

5. DISCUSSION

There are some concerning results in the survey, however, none of the identified issues are insurmountable. The provision of training and some simple in-servicing and adoption of best practices will significantly lower the risk for most lawyers and improve the lot for their clients. It should be noted that most of the following identified issues require small financial input but will yield significant and profound uplift of cyber security posture. The following are the identified and fixable issues:

1. **Lack of updates**

   One of the core issues uncovered was the lack of consistent updating of platforms. It is fundamental that all operational devices automatically update systems and applications-based patches to ensure maximum cyber resilience.

   Furthermore, updating of actual cyber security countermeasures (virus scanners, malware detectors) is also crucial and should be conducted

preferably automatically or if not at least daily.

2. **Lack of cyber security countermeasure deployment**

   A lack of cogent, cognisant deployment of cyber countermeasures was apparent in the responses. Given that the profession of law lives and dies on protection of information this attitude clearly has to change. In defence of the survey respondents though, IT and cyber security is not the traditional domicile or skill set of lawyers, that again must change-we live in a connected world. Concomitant with enjoying the business benefits of this connected world comes a recognition of the risks and an acknowledgement of responsibility.

   Many modern operating systems on PC, laptop, tablet and smart phones provide good countermeasures to deploy as standard including basic malcode detection, firewall services and file encryption services. They simply need to be turned on and ensure that automatic updating occurs. Results from the survey indicate this is not occurring and should be by default. This study has also uncovered issues where new technology types are not receiving the same level of protection due to a lack of awareness for risk by the asset owner about phones and tablets.

   In cases where the lawyers are in corporate environments this a governance issue, in partnerships and single lawyer practices this will be an education and resourcing issue.

3. **Exposure of client data**

   The lack of use of encryption services to send confidential documents is alarming given the nature of a lawyer's business and how value is derived. Sending unencrypted confidential documents via email is an unsafe practice. Interception of these documents by criminal elements becomes a trivial technical exercise, even more so if the document is sent via a wireless connection at a fixed address i.e., office or home. This issue is aggravated when devices are interconnected via Cloud services in a technology-enabled smart city environment (Baig et al., 2017). This is not unreasonable as law firms would be expected to be early adopters of smart contract technology.

   Even when wireless connections are secured with WPA2 (one of the strongest protections for WiFi wireless transmission), it is simply a matter of when, not if, the data can be stolen. Given the release of the new KRACKEN attack (Vanheof & Piessens, 2017) on WPA2 this is now further exacerbated.

   Encryption, by the nature of the data and information that lawyers handle and transmit, is one technology that can resolve many current issues with practice. Encryption of files in storage using Windows Encrypting File Service (EFS) or BitLocker services, the Macintosh FileVault or Android Phone Encryption should be enforced default behaviours either by individual users or through corporate policy.

   The use of fixed disk encryption software such as Veracrypt (IDRIX, 2016) will prevent loss of data from USB attachable drives including flash drives and spinning disk drives. One of the added benefits of Veracrypt is that the tool runs across all major operating platforms.

   The use of Mailvelope (Mailvelope, 2017) or other encryption services should become rapidly the standard practice for the transmission of client

data via email services. Strict or default enforcement of Virtual Private Network (VPN) services for remote network operations should also be enacted.

4. **Use of third party services**

   There was an alarming use of third party email services by respondents. There are several risks in this behaviour particularly with email, firstly the intellectual property (emails) of the business are stored in an ungoverned location and recovery alone could be significantly problematic. Subsequently unauthorised disclosure of materials is a significant risk with compromise of email accounts a significant possibility given announcements by providers of these email services around account compromises. Furthermore, dependent on the mail provider there maybe incursion into end user accounts routinely to gather intelligence by actual foreign intelligence actors or even cyber-criminal gangs who have been known to provide "free" services to glean information from end users.

   Furthermore, from a corporate governance perspective this behaviour should be reined in to reduce risk. The malicious insider looms large in this scenario with staff having access to sensitive documents in repositories for later "access" or distribution needing careful management. It would be prudent for any law firm of any size to have full file auditing occurring at all times.

5. **Lack of use of government initiatives**

   The survey also probed the participant's knowledge of federal and state government initiatives to assist them with respect to cyber security issues in their professional and personal life. The most significant outcome was that even respondents who had indicated they had been cyber attacked had not reported these attacks to the Australian CyberCrime Online Reporting Network (ACORN) a fundamental service provided by the Australian Federal government. This outcome is not only troublesome from the lack of reporting by the legal sector, but also one has to ask the question if they don't do it themselves would they be advising their clients who may have sustained a cyber attack to report the incident to ACORN.

6. CONCLUSION

This survey is the first part of a training and education initiative to enhance the cyber security posture and capability of lawyers through continuing professional development (CPD) activity with their professional association. Overall, the survey has uncovered issues relating to the use of cyber security countermeasures by lawyers (although we acknowledge that this initial survey represents a small sample). The severity of the issues uncovered warrants an interventionist approach to ameliorate the risks that current behaviours present for lawyers and more importantly, their clients.

Many of the issues can be overcome through targeted training and education initiatives. The focus of the engagement by the researchers with the Law Society is to increase the cyber security skills of lawyers through action research, thus the researchers are immersed in the problem situation.

The survey has uncovered a need to educate lawyers particularly about the use of encryption to help protect client data in-transit and at rest. There is also a need to intervene around quasi-established practices such as the use of third-party services for storage of documents e.g., email services and file storage not controlled by

the enterprise. Practices related to password hygiene, remote use of devices, connection to foreign networks and other baseline good practice cyber security behaviours, will need reinforcement through a focused training regime.

REFERENCES

ACORN. (2017). Australian Cybercrime Online Reporting Network (ACORN). Retrieved from https://www.acorn.gov.au/

Anonymous. (2017). WAScamnet. Retrieved from http://www.scamnet.wa.gov.au/scamnet/Home.htm

Baig, Z. A., Szewczyk, P., Valli, C., Rabadia, P., Hannay, P., Chernyshev, M., ... Peacock, M. (2017). Future challenges for smart cities: Cyber-security and digital forensics. Digital Investigation, 22, 3-13. doi:10.1016/j.diin.2017.06.015

Cotton, Hamish, & Bolan, Christopher. (2011). *USER PERCEPTIONS OF END USER LICENSE AGREEMENTS IN THE SMARTPHONE ENIVRONMENT.* Proc. 9th Australian Information Security Management Conference, Citigate Hotel, Perth, Western Australia.

Department, Attorney-General's. (2017). Stay Smart Online. Retrieved from https://www.staysmartonline.gov.au/

IDRIX. (2016). Veracrypt (Version 1.19). France: IDRIX. Retrieved from veracrypt.codeplex.com

Mailvelope. (2017). Mailvelope (Version 2.0.0): Mailvelope GmbH. Retrieved from http://www.mailvelope.com

Morgan, S. (2016). Cyber Crime Costs Projected to Reach $2 Trillion by 2019. Retireced from: https://www.forbes.com/sites/stevemorgan/2016/01/17/cyber-crime-costs-projected-to-reach-2-trillion-by-2019/#7e3f4f983a91

Valli, C., Martinus, I. C., & Johnstone, M. N. (2014). *Small to Medium Enterprise Cyber Security Awareness: An Initial Survey of Western Australian Business.* Paper presented at the 2014 International Conference on Security and Management, Las Vegas, USA.

Vanheof, Mathy, & Piessens, Frank. (2017). *Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2.* Proc. ACM Conference on Computer and Communications Security Dallas USA.

