CEJ
COMPLIANCE
ELLIANCE
JOURNAL

OVERCOMING THE SECURITY QUAGMIRE: BEHAVIOURAL SCIENCE AND MODERN TECHNOLOGY HOLD THE KEY TO SOLVING THE COMPLEX ISSUE OF LAW FIRM CYBER SECURITY

David O'Donovan & Alexandra Marshakova

AUTHORS

David O'Donovan is a trainee lawyer with U.S. firm Orrick, Herrington & Sutcliffe LLP in their London office and is currently completing the academic stage of training. Alexandra Marshakova is an IT Project Leader with the Boston Consulting Group also in London. David and Alexandra participated together in LawWithoutWalls in 2015 and were recognised for their Project of Worth, a spearphishing training model for law firm personnel, which the pair have since incorporated in the UK as Fissure Security. David and Alexandra have spoken about aspects of law firm cyber security and organizational behaviour at IE University Madrid, University of Miami and Harvard Law School.

ABSTRACT

While all industries that handle valuable data have been subject to increasing levels of cyber attack, there is a set of inter-related factors in the law firm cyber security ecosystem that makes such firms more susceptible to attack and also serves to prevent them from taking action to counteract attack vulnerability. As a result of the inter-related external and internal factors affecting law firm cyber security, the human element of firm security infrastructure has been neglected, thereby making humans, at once law firms' greatest asset, their main cyber security weakness. [1]There has been some movement of late, and regulators and clients alike are right to demand law firms do more to improve their cyber security posture.[2] However, much of the scrutiny to which their conduct has been subjected has tended to overlook the complexities of the law firm cyber security quagmire, and unless these issues are addressed in the context of a potential solution, meaningful change is not

---

1 Russell G. Pearce & Eli Wald, *The Relational Infrastructure of Law Firm Culture and Regulation: The Exaggerated Death of Big Law*, 42 HOFSTRA L. REVIEW, 109 (2013).

2 Julie Sobowale, *Law firms must manage cybersecurity risks*, American Bar Association Journal (Mar. 29, 2018, 12:37 PM), http://www.abajournal.com/magazine/article/managing_cybersecurity_risk; See also: McNerney, Michael & Emilian Papadopoulos, *Hacker's Delight: Law Firm Risk and Liability in the Cyber Age*, AMERICAN UNIVERSITY LAW REVIEW 62, 1243-1272 (2013).

likely. Part 1 of this paper outlines the current threat landscape and details the integral role of human error in successful cyber breaches before turning to discuss recent cyber security incidents involving law firms. In Part 2, we analyse elements of law firm short-termism and the underregulation of law firm cyber security conduct and how these, when combined, play a key role in shaping law firm cyber security posture. Finally, in Part 3 we outline a realistic solution, incorporating principles from behavioural science and modern technological developments.

TABLE OF CONTENTS

I. PART 1 – THE CURRENT THREAT LANDSCAPE

A. Attacks on the rise

In recent years, cyber attacks have been growing in frequency, intensity and complexity. Notable examples of breaches include household names such as Equifax, Uber, Yahoo!, Sony, Netflix, JP Morgan, Target, Anthem, and Epsilon[3], as well as prominent international sports stars, politicians, members of the British monarchy and Russian oligarchy.[4] With a more diverse range of perpetrators than ever before, including (amongst others) nation states, hacktivists, and individual private contractors, and a wider variety of attacks ranging from denial-of-service to ransomware, 2017 may just be the year in which the world reached peak cyber attack. An inordinate number of breaches were recorded - some on a very public stage, particularly WannaCry and Petya - which affected government departments, international law firms and brought the UK National Health Service to a standstill. Initial reports of cyber attacks this year suggest that 2018 has continued in much the same vein, with high profile and diverse breaches affecting everything from the market for cryptocurrencies to the 2018 Winter Olympic Games in Pyeongchang, South Korea. By one count, in January alone, over 7 million successful breaches were recorded.[5]

B. Consequences of breach

It is clear that cyber attacks have very real practical consequences for organizations. Reports of the WannaCry and Petya incidents make for almost apocalyptic reading: "shipping containers could not be loaded, lawyers were locked out of their computers and a production line was prevented from churning out chocolates".[6] Another account begins "[in Britain], doctors could neither access their patients' files nor make appointments to see those patients. In Russia, hundreds of the interior ministry's workers sat idle. In China, students were locked out of their theses".[7]

---

3 Taylor Armerding, *The 17 biggest data breaches of the 21st century*, CSO (Mar. 29, 2018, 12:26 PM), https://www.csoonline.com/article/2130877/data-breach/the-biggest-data-breaches-of-the-21st-century.html.

4 ICIJ Investigation, *Paradise Papers: Secrete of the global elite*, International Consortium of Investigative Journalistst (Mar. 29, 2018, 12:29 PM), https://www.icij.org/investigations/paradise-papers/.

5 Lewis Morgan, *List of data breaches and cyber attacks in January 2018*, IT Governance (Mar. 29, 2018, 12:31 PM), https://www.itgovernance.co.uk/blog/list-of-data-breaches-and-cyber-attacks-in-january-201-2/.

6 Hannah Kuchler, *Cost of cyber crime rises rapidly as attacks increase*, Financial Times (Mar. 29, 2018, 12:31 PM), https://www.ft.com/content/56dae748-af79-11e7-8076-0a4bdda92ca2.

7 The Economist Group Limited, *A large-scale cyber-attack highlights the structural dilemma of the NSA*, The Economist (Mar. 29, 2018, 12:31 PM), https://www.economist.com/news/science-and-technology/21722026-americas-national-security-agency-torn-between-defending-computer-systems-and.

The key concern for most organizations is the financial cost of cyber breaches. At its current rate, the cost of breaches to businesses worldwide is expected to reach $6 trillion by 2021.[8] Such financial consequences for organizations usually manifest themselves by way of regulatory action and/or market response. Take for example the Epsilon breach, which was disclosed to shareholders on 30 March 2011. Here, one of United States' most prominent email service providers succumbed to a spearphishing attack[9] and the email addresses of its clients were obtained by hackers who in-turn subjected these organizations to a sustained spearphishing campaign consisting of an estimated 6 billion spam emails. The estimated cost of the breach to Epsilon emanating from, amongst other factors, reputational damage suffered, when last calculated was projected to top $4 billion.[10] Additionally, Uber are currently under investigation and facing the prospect of hefty fines from the Information Commissioner's Office (ICO) in the UK as well as equivalent regulatory bodies in the United States and Italy for their handling of a data breach in 2016. Instead of reporting a breach, which compromised the personal information of 57 million drivers and customers, the company paid a ransom to hackers and the company proceeded to cover up the incident.[11]

Many professional services organisations are now turning to cyber risk insurance as a means of lessening the inevitable financial damage caused by a potential breach. The Financial Times notes that the London insurance market, the largest in the world, saw a 50% rise in the number of companies and individuals taking out cyber risk insurance policies in 2016. It estimates that the current total written premium amount of $2.5 billion could reach $20 billion by 2025.[12] Due in-part to the ever-increasing quantity and complexity of attacks, cyber risk insurance is typified by high cost and complex coverage terms.[13] Yet, the lack of data about cyber risks poses a problem of coverage for those seeking or currently holding such policies and means that current cyber risk policies are both

---

8 The Editors at Cybersecurity Ventures, *Cybercrime Report*, Cybersecurity Ventures (Mar. 29, 2018, 12:35 PM), https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/.

9 Spearphishing is an email or electronic communications scam targeted towards a specific individual, organization or business. Although often intended to steal data for malicious purposes, cybercriminals may also intend to install malware on a targeted user's computer - *What is Spear Phishing?*, Kaspersky (Mar. 29, 2018, 02:59 PM) https://www.kaspersky.co.uk/resource-center/definitions/spear-phishing.

10 Ross Kerber & Brenton Cordeiro, *Analysis: Alliance Data may face high Epsilon breach costs*, Reuters (Mar. 29, 2018, 12:45 PM), https://www.reuters.com/article/us-alliance-epsilon-costs/analysis-alliance-data-may-face-high-epsilon-breach-costs-idUSTRE7393E320110411.

11 Financial Times Reporters, *Uber faces investigations by regulators over massive data breach*, Financial Times (Mar. 29, 2018, 12:50 PM), https://www.ft.com/content/20d98370-cf68-11e7-9dbb-291a884dd8c6.

12 Madhumita Murgia & Oliver Ralph, *Boom in cyber attack insurance predicted to gather pace,* Financial Times (Mar. 29, 2018, 12:51 PM), https://www.ft.com/content/a767e518-c91e-11e6-8f29-9445cac8966f.

13 Sean B. Cooney, *Untangling the Mystery of Cybersecurity Insurance*, Keesal, Young & Logan (Mar. 29, 2018, 12:31 PM), http://www.kyl.com/2017/02/01/untangling-the-mystery-of-cybersecurity-insurance/ originally appeared in, Law Journal Newsletters (Mar. 29, 2018, 12:54 PM), http://www.lawjournalnewslet-

increasingly expensive and inadequate for many organisations' needs. A report from the SANS Institute highlights the coverage gaps caused by uncertainty in the buying and underwriting relationship between information security personnel (InfoSec personnel) from organisations and insurers. Gaps include: i) technology – InfoSec personnel have a diverse understanding of risk and think in terms of eliminating threats and vulnerabilities by way of policies and programmes, while insurers see risk as the financial loss to a firm from a breach; (ii) assessment – insurers prefer quantitative assessment models, while only 25% InfoSec personnel opt for quantitative models when measuring and benchmarking defences; (iii) communication – gaps in (i) and (ii) have created communication gaps between the InfoSec personnel and the insurer, the InfoSec personnel and risk manager and between the insurer and brokers; and (iv) investment – lack of transparency in underwriting criteria and complex terminology in written policies has resulted in misaligned investment by buyers and the rejection of claims. [14]

C. Human behavior as an aspect oy cyber security

One defining feature of organisational cyber security that has emerged in recent years is that the weakest link in defence infrastructure is humans. When perimeter software defences, such as firewalls, are circumvented, the next – and often last – layer of defence is made up of the employees. This places a premium on their ability to detect and appropriately deal with the attack. Not surprisingly, because the implementation of software protection - when compared with the changing of employee behaviour toward good cyber security - is easier to do, organizations have tended to focus on software protections as a means of defence in the hope of insulating employees from attack. However, software protections carry issues of their own. They are dated by their very nature, and so once rolled out, hackers will set to work developing programmes to hone in on perceived weaknesses. Furthermore, there is evidence of human weakness in the coding of such software protections. A study produced by researchers at the University of Florida, Pennsylvania State University and NYU, puts forward that developers have a heuristics-based decision-making process, which is a computational model of solving problems without considering all the information available. Software vulnerabilities can be explained as elements left out of this mental computational model, or blind spots. [15]

---

ters.com/sites/lawjournalnewsletters/2017/02/01/untangling-the-mystery-of-cybersecurity-insurance/?kw=Untangling%20the%20Mystery%20of%20Cybersecurity%20Insurance&et=editorial&bu=Law%20Journal%20News&cn=20170201&src=EMC-Email&pt=Cybersecurity%20Law%20%26%20Strategy&slreturn=20180229065318.

14 Barbara Filkins, *Bridging the Insurance/InfoSec Gap: The SANS 2016 Cyber Insurance Survey*, SANS Institute (Mar. 29, 2018, 12:57 PM), https://www.sans.org/reading-room/whitepapers/analyst/bridging-insurance-infosec-gap-2016-cyber-insurance-survey-37062.

15 Justin Cappos, Nicole Morin, Daniela Oliveira, Marissa Rosenthal, Martin K.-C Yeh., & Yanyan Zhuang, *It's the Psychology Stupid: How Heuristics Explain Software Vulnerabilities and How Priming can Illuminate Developer's Blind Spots*, Proceedings of 30th Annual Computer Security Applications Conference, ACSAC (2014).

While software protections are a crucial part of any organization's cyber defence infrastructure, the above vulnerability notwithstanding, they are only a part. A part which is breached from time to time, and once hackers are inside these perimeter defences, unskilled and unaware employees are powerless to stop them. The IBM Security Intelligence Index 2014 noted that 95% of all cyber breaches involve some element of human error.[16] This data was backed up by the Verizon 2016 Data Breach Investigations Report, which also gave examples of how human error manifests itself in a cyber breach.[17] The report notes that basic cyber defences, policies and defence action plans are sorely lacking within organizations; 63% of attacks involve the use of weak, default or stolen passwords; and that a sizeable portion of attacks exploit known vulnerabilities that the target has not patched, despite the patch being available to the user. The report notes that the top 10 known vulnerabilities accounted for 85% of successful breaches. [18]

We have seen that the dominant – and most successful – means of exploiting human weakness in an organization is by way of social engineering attacks (those which involve psychological deception and manipulation) such as spearphishing. As computer security specialist, Bruce Schneier commented back in 2000, "only amateurs attack machines; professionals target people".[19] The Symantec 2017 Internet Security Threat Report notes that in 2016, Business Email Correspondence (BEC) spearphishing emails targeted over 400 organizations per-day and had yielded over $3 billion in stolen information in the years 2013 to 2015.[20] Many of the most prominent data breaches in recent years have relied on this very technique. These include, as mentioned above, the Panama and Paradise Papers hacks of law firms Mossack Fonseca and Appleby respectively. Perhaps one of the best examples of the simplicity of spearphishing and the cataclysmic effect it can have should it be successful, is the Sony hack from late 2015. In the run up to the attack, Sony had been promoting its upcoming feature film 'The Interview', a comedy parodying North Korean leader Kim Jong Un and a plot by American agents to assassinate him. North Korea, infuriated by this apparent show of disrespect, commissioned a hacking group to infiltrate Sony's network in the lead up to the film's release, as confirmed by the FBI.[21] However, the hackers did not attack the organization's perimeter defences, such as firewalls. Instead,

16 *IBM Security Services 2014 Cyber Security Intelligence Index*, IBM Global Technology Services (Mar. 29, 2018, 12:57 PM), https://media.scmagazine.com/documents/82/ibm_cyber_security_intelligenc_20450.pdf.

17 *2016 Data Breach Investigations Report*, Verizon (Mar. 29, 2018, 01:00 PM), http://www.verizonenterprise.com/resources/reports/rp_DBIR_2016_Report_en_xg.pdf.

18 Ibid.

19 Bruce Schneier, *Crypto-Gram*, Schneier on Security (Mar. 29, 2018, 01:02 PM), https://www.schneier.com/crypto-gram/archives/2000/1015.html#1.

20 *Internet Security Threat Report (ISTR) 2018*, Symantec (Mar. 29, 2018, 01:04 PM), https://www.symantec.com/security-center/threat-report.

21 Kara Scannell, *FBI details North Korean attack on Sony*, Financial Times (Mar. 29, 2018, 01:06 PM), https://www.ft.com/content/287beee4-96a2-11e4-a83c-00144feabdc0.

they sent carefully crafted emails to Sony employees purporting to be from Apple, demanding that they confirm their Apple ID credentials as they had detected unauthorised activity. Unwitting employees who clicked on the link in the email were then taken to a page resembling account verification pages used by Apple, where they proceeded to enter their credentials – data which was collected by the hacking group, who then used these stolen credentials to enter the network and upload malware, crippling the system.[22] As Stuart McClure, former CTO of McAfee, notes, many of those who had their data corrupted and then hard-wired in to the malware that was created had significant access to the Sony network.[23] The fallout of the breach has been well documented. Hackers obtained: every employee email for the previous 10-year period, including embarrassing email traffic between executives and Hollywood stars that were subsequently published online; the salaries and personnel records of thousands of Hollywood stars; and several unreleased feature films. It also laterally affected other organizations. For example, secret acquisitions by the social media organization Snap were made public, having been detailed in the leaked emails.[24] The Interview was subsequently pulled by Sony and never made it to the big screen.

In addition to the propensity of unaware employees to fall for a spearphishing attack, decision making within the organization concerning critical elements of security infrastructure demonstrates a glaring lack of awareness of, and appreciation for the risk. Decisions are often based on heuristics, or incomplete mental models similar to the programmer blind spot referred to above, which try to take a reductionist approach to cyber security investment and strategy decisions.[25] One example is the ransom payment and cover-up operation attempted by Uber in the wake of a breach suffered in 2016. Failings in security infrastructure decision making played a key role in a high-profile breach in 2017 involving the National Health Service in the UK, which fell afoul of the WannaCry attack. The WannaCry attack was a worldwide self-propagating cyber attack (having the ability to spread and cause widespread infection without any user interaction) that exploited a vulnerability in Microsoft Windows operating system using a hacking tool called EternalBlue. While Microsoft had, months in advance, release a patch and notification to warn users to repair the vulnerability[26], a number of organizations did not heed the warning, and it was these organizations – from FedEx to various state governments of India -

---

22 Gregg Keizer, *Sony hackers targeted employees with fake Apple ID emails*, Computerworld (Mar. 29, 2018, 01:07 PM), https://www.computerworld.com/article/2913805/cybercrime-hacking/sony-hackers-targeted-employees-with-fake-apple-id-emails.html.

23 Ibid.

24 Alex Altman & Alex Fitzpatrick, *Everything We Know About Sony, The Interview and North Korea*, Time (Mar. 29, 2018, 01:08 PM), http://time.com/3639275/the-interview-sony-hack-north-korea/.

25 Vaibhav Garg & Jean Camp, *Heuristics and biases: implications for security design*, 32, IEEE TECHNOLOGY AND SOCIETY MAGAZINE, 73–79 (2013); see also: Heather Rosoff, Jinshu Cui & Richard S. John, *Heuristics and biases in cyber security dilemmas*, 33, ENVIRONMENT SYSTEMS AND DECISIONS, 4 (2013).

26 *MS17-010: Security update for Windows SMB Server: March 14, 2017*, Microsoft (Mar. 29, 2018, 01:10 PM), https://support.microsoft.com/en-us/help/4013389/title.

that were inevitably affected. For the UK National Health Service, which is publicly funded and chronically over-stretched in terms of resources, warnings about the vulnerability caused by running Windows XP operating system – perhaps the most likely operating system to succumb to an attack that exploited basic weaknesses such as the WannaCry attack – were received even before Microsoft issued the patch notification.[27] Once the WannaCry attack spread to the UK National Health Service, more than 70,000 devices including computers, MRI machines, blood-storage refrigerators and theatre equipment was affected and hospitals and trusts across the UK were forced to turn away non-critical patients.[28] To be sure, this was not a software issue. This was a prime example of the impact of human error on the cyber defence posture of an organization.

D. Legal services

Behind every headline-grabbing IPO, market-shaping antitrust dispute, sub-Saharan hydro-electric dam project, and even the commercial aircraft traversing the skies, there are law firms undertaking mission-critical work to ensure such projects secure financing, comply with regulatory requirements and helping their clients deliver on time and within budget. Owing to law firms' heavy involvement in such matters, and the client rosters that firms boast, they inevitably play host to vast troves of crucial commercially sensitive information. Law firms also serve to filter out information that is not relevant to a particular transaction or dispute, in effect honing the information they hold down to only the most important. It is little wonder then that law firms have become a prime target for hackers in recent years. In 2011, the FBI briefed 200 of the largest US law firms, warning them that hackers see attorneys as the back door to valuable client data, and stressed that such firms were beginning to experience an uptick in spearphishing attacks.[29] This prediction turned out to be startlingly accurate. The opening paragraph of the ABA Tech Report on Security 2015 reads: "law firm data breaches are continuing. It was recently reported that at least 80% of the largest 100 law firms, by revenue, have been hacked since 2011"[30]. The trend has been mirrored in the UK, with a new report from the National Cyber Security Centre noting that 65% of all UK legal services firms have been hacked. [31]

---

27 Mark Evans, Leandros A. Maglaras , Senior Member, IEEE, Ying He & Helge Janicke, *Human behaviour as an aspect of cybersecurity assurance*, 9, SECURITY AND COMMUNICATION NETWORKS, 17 (2016).

28 Amyas Morse, *Investigation: WannaCry cyber attack and the NHS*, National Audit Office (Mar. 29, 2018, 01:13 PM), https://www.nao.org.uk/report/investigation-wannacry-cyber-attack-and-the-nhs/.

29 Ivan Hemmans & David G. Ries, *Cybersecurity: Ethically Protecting Your Confidential Data in a Breach-A-Day World*, American Bar Association (Mar. 29, 2018, 01:14 PM), https://www.americanbar.org/content/dam/aba/multimedia/cle/materials/2016/04/ce1604lpi.authcheckdam.pdf.

30 David Ries, *Security*, American Bar Association Techreport 2015 (Mar. 29, 2018, 01:17 PM), https://www.americanbar.org/content/dam/aba/publications/techreport/2015/security/Security.authcheckdam.pdf.

31 *Cyber threats to the legal sector and implications to UK businesses*, National Cyber Security Centre (Mar. 29, 2018, 01:19 PM), https://www.ncsc.gov.uk/content/files/protected_files/guidance_files/Cyber-threats-to-the-legal-sector-and-implications-to-UK-businesses.pdf.

While the majority of law firm data breaches go unreported – for reasons we will consider later – some breaches have played out on a very public stage. In early 2016, unsealed criminal charges revealed that a small group of Chinese hackers pinpointed 48 prominent UK and US law firms with expertise in M&A work for the majority of the Fortune500, including Cravath, Swaine & Moore LLP and Weil Gotshal & Manges LLP, and subjected them to a sustained spearphishing campaign over 3 consecutive months.[32] At least one employee at two of the organizations targeted inadvertently granted the hackers access by clicking on a malware-loaded link in an spearphishing email. Once inside the firms' systems, the hackers proceeded to peruse client files and communications relating to at least 10 ongoing or potential deals. The Financial Times notes that in one particularly successful instance, the hackers obtained information relating to Pitney Bowes' offer for Borderfree and Intel's acquisition of Altera and were able to trade ahead of the deals reaching fruition, generating approximately $4 million in the process. [33]

April 2016 also saw the announcement of what has since been dubbed "the biggest leak in data journalism history", the Panama Papers.[34] Here, an internationally operating law firm, Mossack Fonseca, was running two websites. One front facing and one acting as a client interface, the latter of which shared its IP address with the firm's email server, which itself was running a version of Microsoft Outlook not updated since 2009. This effectively meant that obtaining access to the firm's already extremely vulnerable email server would accelerate access to the firm's customer interface, thereby unlocking confidential client information. When this vulnerability was inevitably exploited, 11.5 million documents containing 2.6 terabytes of data were exposed, principally detailing the tax affairs of high profile figures across the world from Russian oligarchs to the Icelandic prime minister.[35] A similar, but unrelated, incident occurred later in 2016, and which was publicly disclosed in October 2017, when major offshore firm Appleby, was breached in an "illegal computer breach"[36], believed to have been carried out using similar techniques to those deployed in the Panama Papers breach. In this instance, 13.4 million documents compris-

---

32 *United Strates of America vs. Iat Hong, Bo Zheng & Chin Hung*, United States District Court Southern District of New York (Mar. 29, 2018, 01:23 PM), https://www.justice.gov/usao-sdny/press-release/file/921006/download.

33 Brooke Masters, *Lawyers and accountants are prime targets for cyber attacks*, Financial Times (Mar. 29, 2018, 01:26 PM), https://www.ft.com/content/f52f6fee-ccf4-11e6-864f-20dcb35cede2.

34 Barb Darrow, *How Tech Made the Pulitzer Prize-Winning Panama Papers Coverage Possible*, Fortune (Mar. 29, 2018, 01:27 PM), http://fortune.com/2017/05/30/panama-papers-data-tools/.

35 *Offshore Leaks Database*, The International Consortium of Investigative Journalists (Mar. 29, 2018, 01:07 PM), https://offshoreleaks.icij.org/.

36 John Hyde, *Paradise Papers firm Appleby: We've done nothing wrong*, The Law Society Gazette(Mar. 29, 2018, 01:30 PM), https://www.lawgazette.co.uk/practice/paradise-papers-firm-appleby-weve-done-nothing-wrong/5063566.article.

ing 1.4 terabytes of data were obtained and published, exposing the tax workings of companies such as Nike and Apple, as well as high profile figures such as F1's Lewis Hamilton and the Queen of England. [37]

"Consider litigators unable to access motions on a deadline. Trial lawyers preparing for arguments without key documents. Transactional lawyers unable to communicate with clients attempting to close multibillion-dollar deals".[38] This was reality for global heavyweight DLA Piper in June 2017 when the firm fell victim to the Petya attack, another aggressively self-propagating attack similar to the earlier WannaCry attack, which also exploited vulnerabilities in Microsoft operating systems. Interestingly, experts noted that the malware used in the attack was not designed to make money, but instead to spread fast and cause damage.[39] While DLA Piper may not have been held to ransom, the damage caused to the firm by way of disruption of its global operations nevertheless caused significant financial damage. With an estimated 24 hours without phones, 2 days with no access to email and up to 6 weeks without full access to previous emails and other documents, not to mention the lasting reputational damage that comes with such a high-profile breach, it is not surprising that this 'disaster' is likely to end up costing the firm millions in lost earnings.[40]

Cyber attacks are not reserved for only large law firms. Information presented in the ABA Tech Report 2016 demonstrates that while 26% of firms with 500 or more attorneys, and 20% of firms with 100 or more reported successful data breaches in 2015, 25% of firms with between 10 and 49 attorneys and 8% of solo practitioners reported successful breaches over the same period.[41] When one considers that of the 1,300,705 practicing attorneys in 2015, 45% were solo practitioners and only 16% comprised of firms with 100 or more attorneys, it becomes clear that private practice entities of all sizes are under attack.[42] For

---

37 *The Long Twilight Struggle Against offshore Secrecy*, The International Consortium of Investigative Journalists (Mar. 29, 2018, 01:32 PM), https://www.icij.org/investigations/paradise-papers/.

38 Roy Storm, *Ransomware Attack on DLA Piper Puts Law Firms, Clients on Red Alert*, The American Lawyer (Mar. 29, 2018, 01:33 PM), https://www.law.com/americanlawyer/almID/1202791614770/Ransomware-Attack-on-DLA-Piper-Puts-Law-Firms-Clients-on-Red-Alert/.

39 Iain Thomson, *Everything you need to know about the Petya, er, NotPetya nasty trashing PCs worldwide*, The Register (Mar. 29, 2018, 01:35 PM), https://www.theregister.co.uk/2017/06/28/petya_notpetya_ransomware/.

40 https://blog.barkly.com/dla-piper-petya-ransomware-attack; See also: Barney Thompson, *DLA Piper still struggling with Petya cyber attack*, Financial Times (Mar. 29, 2018, 01:38 PM), https://www.ft.com/content/1b5f863a-624c-11e7-91a7-502f7ee26895.

41 David Ries, *Security*, American Bar Association Techreport 2016 (Mar. 29, 2018, 01:41 PM), https://www.americanbar.org/content/dam/aba/publications/techreport/2016/security/security.authcheckdam.pdf.

42 *ABA National Lawyer Population Survey*, American Bar Association (Mar. 29, 2018, 01:45 PM), https://www.americanbar.org/content/dam/aba/administrative/market_research/Total%20National%20Lawyer%20Population%201878-2017.authcheckdam.pdf.

example, in addition to major law firm data breaches referred to above, QBE, a UK insurance company, in a piece with the Financial Times disclosed 150 incidences of successful 'Friday fraud' whereby hackers had learned that UK property lawyers tended to close deals on Fridays and move money between accounts. Hackers proceeded to gain access to firms' email servers via spearphishing campaigns, and once inside, send emails from the server pretending to be the lawyer on the file for that particular transaction and direct closing monies to be transferred to a particular bank account. The claims manager of QBE is quoted as saying "anyone with half a brain could carry out these sorts of email scam ... high street conveyancing firms are not necessarily going to have the latest data security systems". The company estimates that upward of £85 million was stolen over an 18-month period from 2015. This also serves to highlight that there is now a broader spectrum of perpetrators of attacks which range from government-funded hacking groups, such as the Chinese group behind the Canadian Seven Sisters law firm breach in 2010[43], to non-tech-savvy individuals who can buy and distribute malware that even comes with a money-back guarantee should the programme be caught by antivirus systems.

II. PART 2 – THE LAW FIRM CYBER SECURITY QUAGMIRE

While all industries that handle valuable data are subject to increasing levels of cyber attack, there is a set of inter-related factors in the law firm cyber security ecosystem that makes law firms more susceptible to attack and also serves to prevent such firms from taking action to counteract attack vulnerability. As a result of the inter-related external and internal factors affecting law firm cyber security, the human element of firm security infrastructure has been neglected, thereby making humans, at once law firms' greatest asset, their main cyber security weakness.[44] There has been some movement of late, and regulators and clients alike are right to demand law firms do more to improve their cyber security posture.[45] However, much of the scrutiny to which their conduct has been subjected has tended to overlook the complexities of the law firm cyber security quagmire, and unless these issues are addressed in the context of a potential solution, meaningful change is not likely. What follows is an analysis of current issues concerning law firm cyber security and how these, together, create human vulnerabilities ranging from increased susceptibility to spearphishing attempts to a complete lack of awareness of good cyber practice generally, that have the potential, when exploited, to cripple a firm's IT infrastruc-

43 Jeff Gray, *Hackers linked to China sought Potash deal details: consultant*, The Globe and Mail (Mar. 29, 2018, 01:37 PM), https://www.theglobeandmail.com/technology/tech-news/hackers-linked-to-china-sought-potash-deal-details-consultant/article534297/.

44 Russell G. Pearce & Eli Wald, *The Relational Infrastructure of Law Firm Culture and Regulation: The Exaggerated Death of Big Law*, 42, HOFSTRA LAW REVIEW 109 (2013).

45 Julie Sabowale, *Law firms must manage cybersecurity risks*, American Bar Association Journal (Mar. 29, 2018, 01:47 PM), http://www.abajournal.com/magazine/article/managing_cybersecurity_risk; See also: McNerney, Michael & Emilian Papadopoulos, *Hacker's Delight: Law Firm Risk and Liability in the Cyber Age*, AMERICAN UNIVERSITY LAW REVIEW 62, 1243-1272 (2013).

ture, jeopardize client information, and negatively affect reputational capital in the process.

A. The buyer's market for legal services

Commentators such as Ribstein[46] and Galanter and Henderson[47] make the point that the information asymmetry that once existed between law firm and client and was the "bread and butter"[48] of large law firms' reputational capital, which enabled firms to demand high fees, has now been eroded. This is due to in-house legal teams becoming larger and more sophisticated, and because of the variety of service providers on offer in the market, from other law firms to legal technology companies. Clients now have less need to purchase legal services based on personal relationships or sole-provider agreements with traditional firms and are empowered to shop around for the best fit for their particular needs.[49] It is true to say that we now find ourselves in a buyer's market for legal services, where clients' have more control than ever when it comes to who is providing the service and on what terms. Law firms face unprecedented competition from competitor firms, new technologically-enabled entrants and alternative business model (ABS) providers.[50] This shift towards a buyer's market for services was accelerated by the Great Recession and has since seen in-house teams commanding greater bargaining power while operating within tighter budgetary constraints and demonstrating an increased willingness to unbundle work and source it to the most cost-efficient provider. The knock-on effect for traditional law firms is that they have been forced to adapt quickly, or face forfeiting market share. In order to do so, as well as being more receptive to fixed and alternative fee arrangements, law firms have enthusiastically championed a culture of round-the-clock availability to clients, made possible by remote mobile devices[51], and have begun to engage legal process outsourcing and artificial intelligence tools as part of an efficiency and innovation drive.[52]

While law firms have benefitted greatly from modern technological developments, a disparity exists between the hyper rate at which law firms are adopting new technologies and the level of competence of their security infrastructure, which greatly increases the risk of cyber attacks. One example is with regard to smartphones. The ABA Tech Report 2016

---

46 Larry E. Ribstein, *The Death of Big Law*, WISCONSIN LAW REVIEW, 749 (2010).

.47 Henderson William D. & Galanter Marc, *The Elastic Tournament: The Second Transformation of the Big Law Firm*, MAURER SCHOOL OF LAW: INDIANA UNIVERSITY (2008).

48 Russell G. Pearce & Eli Wald, *The Relational Infrastructure of Law Firm Culture and Regulation: The Exaggerated Death of Big Law*, 42, HOFSTRA LAW REVIEW 109 (2013).

49 Ibid.

50 *The Future Of Legal Services*, The Law Society (Mar. 29, 2018, 01:48 PM), https://www.lawsociety.org.uk/news/documents/future-of-legal-services-pdf/.

51 Eli Wald, *Legal Ethics' Next Frontier: Lawyers and Cybersecurity*, 19, CHAPMAN LAW REVIEW 501 (2016).

52 Ibid; See also McNerney, Michael & Emilian Papadopoulos, *Hacker's Delight: Law Firm Risk and Liability in the Cyber Age*, AMERICAN UNIVERSITY LAW REVIEW 62, 1243-1272 (2013).

notes that 93% of lawyers use a smartphone for work outside of the office, and only 43% of lawyers reported having a mobile technology policy for their firm, meaning that most firms do not have a policy for how mobile devices should be used or client data transmitted or stored on them.[53] As McNerney and Papadopoulos point out, "client relations require near-constant accessibility to attorneys and online access to important documents that might otherwise stay secured in the office".[54] While adequate for meeting modern client availability demands in this way, remote connected devices without robust security measures also "means easier access to sensitive information for adversaries and creates opportunities for hackers to enter onto corporate networks by breaking into remote systems or compromising mobile devices".[55]

B. Lack of regulatory scrutiny and effective ethics rules

In the United States, most state-level legislation requires law firms to notify clients if they reasonably believe a third party has gained unauthorized access to their data, and federal laws apply to particular industries, imposing data security requirements which may apply to lawyers operating within that industry.[56] 47 states have enacted data breach notification statutes which require private entities to notify affected individuals of data breaches compromising their information. The regulations, however, vary wildly as regards which entities must comply, the definition of breach, the definition of reasonable and notification requirements. In the absence of an established federal-level standard of law firm cyber regulation, states have promulgated their own rules. However, few legal standards apply to law firm data breaches, and those that do, such as an obligation to notify clients if one reasonably believes there has been a data breach compromising client information, come with little by way of guidance. This precipitates imprecise and inconsistent interpretation, thereby stifling enforcement.[57] In the UK, the situation is somewhat more straightforward in terms of the regulatory framework, but similar issues persist, particularly regarding notification requirements. Under the Data Protection Act 1998, which is enforced by the Information Commissioner's Office (ICO), the Seventh Principle stipulates that 'appropriate technical and organizational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data,' mandating the implementation of some form of cyber defence by law firms. While in the United States there is a basic requirement in most states to notify

53 Aaron Street, *Mobile Technology*, American Bar Association Techreport 2016 (Mar. 29, 2018, 01:49 PM), https://www.americanbar.org/groups/law_practice/publications/techreport/2016/mobile.html.

54 McNerney, Michael & Emilian Papadopoulos, *Hacker's Delight: Law Firm Risk and Liability in the Cyber Age*, AMERICAN UNIVERSITY LAW REVIEW 62, 1243-1272 (2013).

55 Ibid.

56 McNerney, Michael & Emilian Papadopoulos, *Hacker's Delight: Law Firm Risk and Liability in the Cyber Age*, AMERICAN UNIVERSITY LAW REVIEW 62, 1243-1272 (2013).

57 Madelyn Tarr, *Law Firm Cybersecurity: The State of Preventative and Remedial Regulation Governing Data Breaches in the Legal Profession*, 15, DUKE LAW & TECHNOLOGY REVIEW 234-252 (2017).

affected clients of data breaches (which is seldom enforced for reasons explained above), there is no legal obligation to report breaches which result in loss, release or corruption of client data under the UK regime.[58]

Wald highlights the consequences that a lax regulatory environment for law firm cyber security conduct has had for the ability for market controls – such as action by clients (e.g. firing and/or suing their legal service provider) – to have an impact. Law firms are under no general duty to report attacks or breaches to clients and often have insufficient information about such attacks or breaches to allow for comprehensive reporting to clients in any event. He notes that "a plaintiff in a malpractice lawsuit must establish four elements: the existence of a duty, breach of the duty owed, causation, and damages. Yet a plaintiff in a malpractice suit alleging negligence in failing to protect information is unlikely to be able to prove damages because of the challenges in answering key questions about cyber security breaches: who perpetrated the cyber attack; what information did they steal; what is the value of that information to them or others; and what other harms, such as operational disruption, competition, or reputational damage, resulted for the victim? Consequently, there are hardly any cases litigating attorney (or even corporate) negligence for failure to protect confidential information".[59] That is, of course, if the client is even told about the breach in the first place. Wald refers to this issue as the 'underregulation' of law firm cyber security conduct, or "the inability of clients to effectively utilize liability rules and market controls to ensure that lawyers face appropriate cyber incentives."[60] He goes on to emphasise that "as lawyers face insufficient incentives to implement appropriate cyber security measures and report attacks to clients, data about attacks and their consequences goes uncollected, diminishing the prospect of effective liability rules and market controls developing in the future. This is the kind of market failure that is unlikely to resolve itself without regulatory intervention, except that liability rules are not likely to constitute an effective regulatory response. It is also the kind of market failure that prevents the collection of the very data we need to better understand the extent of the problem we are facing."[61]

Ethics rules, while having a potentially important role to play in improving law firm cyber security conduct should they be upgraded to account for failings in the current regulatory landscape, do little to improve the situation at present. The ABA Model Rules of Professional Conduct have been revised in recent years to take account of the permeation of technology throughout the practice of law and to acknowledge the increased risk of cyber

58 *Notification of data security breaches to the Information Commissioner's Office (ICO)*, International Commissioner's Office (Mar. 29, 2018, 01:53 PM), https://ico.org.uk/media/for-organisations/documents/1536/breach_reporting.pdf.

59 Eli Wald, *Legal Ethics' Next Frontier: Lawyers and Cybersecurity*, 19, CHAPMAN LAW REVIEW 501 (2016).

60 Ibid.

61 Ibid.

attacks on law firms. In particular, new Rule 1.6(c) states that "[a] lawyer shall make reasonable efforts to prevent . . . the unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client," and is accompanied by Comments 18 and 19 for guidance on interpretation. However, Wald makes the point that efforts to enable ethics rules to fill the void left by fragmented state and federal law firm cyber security regulations fall short of the mark.[62] The Rule and Comments fail to require law firms to put in place a cyber security plan to monitor cyber defences for breach, do not provide guidance on what constitutes "reasonable efforts" and "reasonable precautions", and stop short of mandating disclosure requirements to clients regarding breaches which concern client data.[63] In the UK, lawyers are under an obligation contained in the Solicitor's Regulatory Authority's Code of Conduct 2011 to protect client confidentiality. In particular, Outcome (4.5) stipulates that law firms have effective systems and controls in place to enable them to adequately identify risks to client confidentiality and to mitigate those risks, and Indicative Behaviour (4.1) requires that "your systems and controls for identifying risks to client confidentiality are appropriate to the size and complexity of the firm or in-house practice and the nature of the work undertaken, and enable you to assess all the relevant circumstances". Yet interestingly a recent CenturyLink white paper concerning law firm cyber security in the UK puts forward that only 1% of all complaints received by the SRA are in relation to data security.[64] This serves to reinforce Wald's point that the uncertainty surrounding cyber attacks on law firms – who perpetrated the attack, what information was compromised, and what damage, if any, did clients suffer as a result of the attack - which persists because of uncollected data owing to underregulation, renders liability and market controls ineffective means of regulating lawyers' cyber security conduct.[65]

C Changes in the regulatory environment and client demands

The introduction of the General Data Protection Regulation (GDPR) in May 2018 introduces far more stringent regulatory standards and obligations on firms to protect data. The GDPR will apply not only to organizations within the EU, but also organizations located outside the EU if they offer services to EU data subjects. With over 100 US law firms located in London alone, the majority of which have European entities on their respective client lists, it is clear that the GDPR is an initiative with global reach. Obligations under the GDPR include mandatory breach notification reporting to the relevant national regulatory body (e.g. the UK ICO) within 72 hours and 'privacy by design' which

62 Ibid.

63 Ibid.

64 *Law firms and cybersecurity: how can lawyers keep their client data confidential?*, CenturyLink (Mar. 29, 2018, 01:51 PM), http://www.centurylink.co.uk/asset/business/enterprise/white-paper/centurylink-law-firms-and-cybersecurity-wp170692.pdf.

65 Eli Wald, *Legal Ethics' Next Frontier: Lawyers and Cybersecurity*, 19, CHAPMAN LAW REVIEW 501 (2016).

involves implementing appropriate security measures with regard to systems and personnel, and introducing policies and procedures governing data management by staff.[66] Much has been made of the penalties which can be levied against organizations found to breach provisions of the GDPR. A non-compliant firm could face a fine of €20 million or 4% of turnover, whichever is greater. This is doubtless a positive development, and it will be interesting to observe the impact it has on law firm cyber conduct. In-light of the above issues concerning the collection of data on law firm cyber incidents and the issues faced by law firms in identifying breaches in the first place, there is reason to be sceptical. The concern is that law firms will adopt the bare minimum standard of compliance within the realms of their perceived regulatory threat level, which is arguably lower than average organization given the enigmatic nature of law firm cyber security data. However, Article 24 of the GDPR, which concerns the implementation of appropriate technical and organizational measures to protect information, also requires affected organizations to demonstrate compliance with the GDPR. With a recent report highlighting that approximately 25% of UK based law firms believing themselves to be compliant with the provisions of the GDPR, it is true to say that law firms, at a minimum, will be subjected to increased regulatory scrutiny under the GDPR, the above scepticism notwithstanding. It may well be the case that national regulatory bodies turn to use the GDPR in an attempt to force better law firm cyber security – time will tell.

With respect to ethics rules, Wald has made clear that the recent revision of the ABA Rules of Professional Conduct – particularly Rule 1.6(c) and accompanying Comments 18 and 19 stop short of being an effective means of mandating better cyber security in the fact of inadequate liability rules and market pressure. He advocates for a further revision of the Rules to require stronger cyber protections within law firms, provide for mandatory breach disclosure requirements to clients, and delineation on the meaning of 'reasonable' in the context of cyber protections and disclosure requirements upon breach.[67] While it is agreed that the "promulgation of robust rules of professional conduct" concerning security protection in law firms and data breach reporting to clients would in theory incentivise law firms to take action, such radical overhaul – which would need to be an internationally co-ordinated effort on behalf of national regulatory authorities in order to affect globally operating law firms – is not immediately on the horizon.[68]

In addition to the - albeit piecemeal - movements taking place with regard to the regulatory environment and ethics rules concerning law firm cyber security, clients too are beginning to exert market pressure on their legal service providers. The ABA Tech Report on security 2016 suggests that increased pressure from clients – who are themselves examining their cyber security posture and that of their supply chain – is causing firms to focus on cyber risk. 62.8% of law firms with 500 or more and 30.7% of all law firms reporting

66 The EU General Data Protection Regulation (GDPR) (Mar. 29, 2018, 01:50 PM), https://www.eugdpr.org/.

67 Eli Wald, *Legal Ethics' Next Frontier: Lawyers and Cybersecurity*, 19, CHAPMAN LAW REVIEW 501 (2016).

68 Ibid.

that actual or prospective clients had provided them with security requirements.[69] We know little about the actual figures, however. Some initial research in to law firms in the United States suggests that 40% of firms intend to increase their cyber security spend somewhat in 2018[70], but aside from this, data remains opaque. Liability rules may also inform law firm cyber conduct, notwithstanding the potential issues with compliance highlighted above. Firms which stand accused of poor cyber conduct may simply settle with the affected client instead of having the issue played out in public, which could stand to harm both organizations[71]. Such settlement serves as a form of damage limitation, whereby the firm may pay compensation to an affected client and, in the worst case, lose that client's business, but crucially, information about the breach is kept private in order to protect the firm's reputation.

A potentially important development came by way of a class action suit brought in the District Court for the Northern District of Illinois in April 2016, when a client sued its law firm, not for damage resulting from breach, but because their technology systems were not up to "industry standards", leaving open the possibility that client data could be jeopardised should the firm's systems be breached.[72] While the dispute was eventually arbitrated, meaning that all further information remained private, the initial complaint was unsealed by the court in December 2016. This is interesting for a number of reasons. Firstly, it demonstrates a willingness on behalf of a client to take a proactive approach to enforcement of malpractice liability further upstream than what is usually associated with a malpractice suit. Second, it highlights the effectiveness of the use of alternative dispute resolution provisions in retainers as a means of keeping malpractice issues relating to client information out of public view, meaning that it is likely that data regarding law firm cyber security breaches and disputes will continue to go uncollected. The likely consequence is that there will persist little by way of judicial exposition of aspects of malpractice suits emanating from law firm cyber security conduct, such as what is 'reasonable' in the context of firm's cyber security protections or data breach disclosure requirements to clients, even if we do see an uptick in malpractice actions.

Recent cyber security incidents involving law firms such as the DLA Piper hack and the

---

69 David Ries, *Security*, American Bar Association Techreport 2016 (Mar. 29, 2018, 01:52 PM), https://www.americanbar.org/content/dam/aba/publications/techreport/2016/security/security.authcheckdam.pdf.

70 Robert Half, *Survey: Four In 10 Lawyers Plan To Boost Cybersecurity Spending In Next 12 Months; Budgets To Increase 13 Percent On Average*, Robert Half Legal (Mar. 29, 2018, 01:55 PM), http://rh-us.mediaroom.com/2017-10-19-Survey-Four-In-10-Lawyers-Plan-To-Boost-Cybersecurity-Spending-In-Next-12-Months-Budgets-To-Increase-13-Percent-On-Average.

71 Eli Wald, *Legal Ethics' Next Frontier: Lawyers and Cybersecurity*, 19, CHAPMAN LAW REVIEW 501 (2016).

72 Sedgwick LLP, *United States: Professional Services Firms Beware: Just Because You Haven't Suffered A Data Breach Doesn't Mean You Won't Be Sued – And the Worst Part, There May Not Be Coverage*, Mondaq (Mar. 29, 2018, 12:41 PM), http://www.mondaq.com/unitedstates/x/575630/Insurance/Professional+Services+Firms+Beware+Just+Because+You+Havent.

Panama and Paradise Papers, which implicated Mossack Fonseca and Appleby respectively, have highlighted what we already know about attacks on law firms, according to Wald. We know law firms are aggressively being targeted, we know more about the type of hackers and why they are attacking law firms. Firms even know more about how to protect themselves from such attacks and how to mitigate damage caused. Importantly, however, we are still none the wiser as to whether law firms are actually acting on this data to improve cyber defences and thereby protect client information.[73]

D The law firm partnership model, PEP success and reliance on the billable hour

As with the original Cravath model, large law firm success continues to be underpinned by time-based billing and billable hour budgets today. The billable hour has itself raised a range of issues since its inception, from the impact that billable hour culture has on lawyers' health, morale and work-life balance to the proposition that it actually tends to reward inefficiency and other unethical practices.[74] As Parker and Ruschena note, the junior lawyers of today in large law firms are under the strong and consistent impression that the value of their work is judged based on the fees they generate in the form of billing and when faced with an employer whose goal is revenue generation for the partners, non-partner lawyers may feel a disconnect in-terms of loyalty to the firm, precipitating issues such as unethical behaviour in relation billing practices and de-motivation regarding firm initiatives.[75] The core decision making of the firm is controlled by the inner-circle of equity partners, who also control access to key clients. Molot notes that because an equity partner's stake vanishes upon retirement, his/her only real reward for partnership is the annual draw on profits during productive years at the firm, meaning they are ill-equipped to make long-term investment decisions in the firm and have a decidedly short-term bias.[76] Law firm partnerships can therefore be said to be short-termist by nature and because firms are obsessed with current comparative performance metrics such as the 'profit-per-equity-partner' (PEP) marker of success, by which firms are ranked against competitors, there is a clear and definite focus on maximizing profits.[77]

This also serves to reinforce a point alluded to earlier with respect to the changing nature of the profession toward a buyer's market for services: that there now exists a culture of 24/7 availability to clients, enabled by remote devices. Lawyers are effectively always connected to the network, and by consequence there is optimal opportunity to generate more fees by way of billing. Molot argues that this development has served to alienate lawyers

---

73 Ibid.

74 Christine Parker & David Ruschena, *The Pressures of Billable Hours: Lessons From a Survey of Billing Practices Inside Law Firms*, 9, UNIVERSITY OF ST. THOMAS LAW JOURNAL 619 (2011).

75 Ibid.

76 Jonathan T. Molot, *What's Wrong with Law Firms? A Corporate Finance Solution to Law Firm Short-Termism*, 88, SOUTHERN CALIFORNIA LAW REVIEW 1 (2015)

77 Ibid.

and clients alike. The, now 24/7, billable hour model serves to maximize current profits, thereby boosting a firm's PEP standing, but leaves clients feeling deeply dissatisfied. Firms' have the wrong financial incentives to do the work and clients also feel overcharged due to inherent inefficiencies of their work practices, while lawyers themselves feel overworked and undervalued.[78]

'Autonomous self-interest' – seeking to maximize one's own atomistic good without regard for others - has replaced 'relational self-interest' – prioritising the inter-relatedness of actors and that maximization of self-interest cannot occur in isolation - as the dominant culture of the legal profession. This has served to undermine both the economic and professional conduct of firms.[79] Galanter and Henderson highlight a further impact of this new model, which is particularly relevant for our purposes: "notwithstanding its formidable size, the 'firm' itself has remarkably little autonomy to pursue noneconomic objectives, such as ... the training and mentoring of the next generation of lawyers. Although the partnership shares the benefits of successful recruitment, the lack of credible risk sharing reduces the willingness of individual lawyers to invest in firm-wide initiatives that do not simultaneously optimize their own practice".[80]

We would add that in an autonomous self-interest culture where partners often strive to 'own' their client relationships and 'eat what they kill' in terms of maximising their own profits based on those 'owned' relationships, there is often a perverse incentive for information hiding and for keeping things from the rest of the partners and the firm. This in turn can lead to riskier and often unethical practices that are often not visible at Firm level. Furthermore, due to law firms' lack of permanent equity, current equity partners, or the decision making core of the firm, have little incentive to invest in projects that are long-term in nature, such as investments in firm IT and infrastructure, as it is likely the benefits of such investment will be seen also in the long term – perhaps after the particular partners charged with making such decisions have retired or moved on to pastures anew. This is despite, as Molot notes, corporate finance literature being replete with evidence that short-termism does not, in fact, serve to maximize returns for equity stakeholders.[81]

E The product of short-termism and underregulation combined

Short-termism, coupled with the underregulation of cyber security conduct, has created a plethora of negative consequences that characterise the current internal law firm cyber security environment. Issues such as the lack of investment in IT and infrastructure projects has severely limited firms' ability to implement adequate cyber security protections,

78 Ibid.

79 Larry E. Ribstein, *The Death of Big Law*, WISCONSIN LAW REVIEW, 749 (2010).

80 Henderson William D. & Galanter Marc, *The Elastic Tournament: The Second Transformation of the Big Law Firm*, MAURER SCHOOL OF LAW: INDIANA UNIVERSITY (2008).

81 Jonathan T. Molot, *What's Wrong with Law Firms? A Corporate Finance Solution to Law Firm Short-Termism*, 88, SOUTHERN CALIFORNIA LAW REVIEW 1 (2015)

while a culture of 24/7 availability to clients enabled by remote connected devices increases vulnerability. In any event, given the absence of effective liability rules and market pressure, law firms are not being forced to change. It is true to say that law firms are taking steps to improve their cyber defences, given the current threat environment. Improving software protections such as firewalls appears to be the obvious first step, but some firms have also moved to tackle the human element of cyber security with awareness campaigns such as 'Cyber Security Month', spearphishing penetration testing (where test spearphishing emails are sent to staff and responses recorded), and corporate training exercises such as tutorials and accompanying exercises. Additionally, some lawyers, as Wald notes, may respond to peer pressure and organically evolving security norms within firms.[82] However, these approaches are inadequate to deal with the persistent and systematic problems caused by law firm short-termism and underregulation generally, but especially the most important aspect of cyber defence - humans. The current approach adopted by law firms means that staff, from administrative staff to partners, are fundamentally under-skilled and unprepared to guard against cyber attacks.

It has been true for some time that cyber security is more a human issue than an IT issue.[83] Improving cyber security conduct therefore necessitates behavioural change on behalf of those within the organization. Such change is a painstaking and slow process, requiring persistent effort and monitoring over time to adjust a current feedback loop to fit the desired behaviour. [84] A short tutorial video, an awareness campaign, or standalone spearphishing penetration testing will not achieve such change. In a recent conversation with the Chief Information Officer of a major UK law firm, the authors learned that the average annual time spent training lawyers within the organization was as little as 8 minutes per year - presumably the length of the mandatory tutorial video and questionnaire, and this was predicted to be the same across the majority of large UK law firms. It has also been well documented that awareness campaigns do not affect behaviour when it comes to cyber security. Analogous data is provided by Evans et al, with respect to the healthcare industry in the UK. The authors note that the National Health Service was successfully breached across its various organizations over 7000 between 2011 and 2014, with an increase in the number of breaches of 101% between 2013 and 2014, all despite 75% of such organizations receiving standard security awareness material over the same period.[85] Finally, spearphishing penetration testing, while perhaps one of the more effective means of monitoring firm cyber security vulnerability to attack, can do little beyond monitoring if not accompanied by regular training in order to affect meaningful behavioural change. This is a development in law firm cyber defence that has been hamstrung by the

---

82 Eli Wald, *Legal Ethics' Next Frontier: Lawyers and Cybersecurity*, 19, CHAPMAN LAW REVIEW 501 (2016).

83 *The Human Factor in IT Security: How Employees are Making Businesses Vulnerable from Within*, Kaspersky Daily (Mar. 29, 2018, 02:06 PM), https://www.kaspersky.com/blog/the-human-factor-in-it-security/.

84 Shari Lawrence Pfleefger & Deanna D. Caputo, *Leveraging Behavioural Science to Mitigate Cyber Security Risk*, 31, COMPUTERS & SECURITY 4 (2012).

85 Mark Evans, Leandros A. Maglaras , Senior Member, IEEE, Ying He & Helge Janicke, *Human behaviour as an aspect of cybersecurity assurance*, 9, SECURITY AND COMMUNICATION NETWORKS, 17 (2016).

billable hour culture, as firms fail to reconcile effective and regular cyber security training with 24/7 availability to clients.

As we have seen, lawyers unskilled to deal with, and unaware of the dangers of, cyber attacks are the greatest threat to a law firm's security, with many large data breaches in recent years – such as DLA Piper and Appleby – emanating from spearphishing campaigns. The impact of such breaches was exacerbated by the lack of a clear cyber security policy or response plan within the individual firm. In addition to the above issues of short-termism and underregulation being contributing factors to cyber security issues which persist in law firms, an underlying issue that plays a key role in lawyers' susceptibility to attack is their personality type. Research by Halevi, Memen and Nov has demonstrated that conscientious personality types are far more susceptible to spearphishing than other personality types.[86] Conscientiousness is associated with being stable, trustworthy, thorough, analytical and factual – key personality and skills traits of lawyers. The study found that "while conscientiousness people are hardworking and have high self-control ... an appeal to efficiency and order will overcome the participants self-control and raise the likelihood of responding to a spear-phishing attack".[87] The study also showed a negative correlation between respondents' perceived risk of attack versus their actual susceptibility to attack, thereby demonstrating that not only are conscientious types more vulnerable to attacks, they actually underestimate the likelihood of falling victim to an attack.[88] This underlying behavioural weakness is doubtless amplified by the current issues of law firm short-termism and the underregulation of law firm cyber security conduct.

It should be noted that the consequences of inadequate training are not just limited to failing to spot attacks, however. They extend to dangerously ignorant cyber security conduct by personnel online. A recent report released by RepKnight in January, which studied the dark web footprint of the 500 biggest UK law firms, showed that over 1 million leaked, hacked or stolen credentials – including firm email address and password combinations (80% of the credentials) – were available for sale on the dark web. That is an average of 2,000 credentials per firm, and at least 1 from every firm. What is most worrying about this development, notwithstanding the sheer size of the confidential data available, is that most of said data was obtained from third-party breaches, or breaches unconnected to the firm itself. This means that lawyers had been using their work credentials to sign up to these third parties' sites or offerings, apparently completely oblivious to the risk.[89]

---

86 Tzipora Halevi, Nasir Memon & Oded Nov, *Spear-Phishing in the Wild: A Real-World Study of Personality, Phishing Self-Efficacy and Vulnerability to Spear-Phishing Attacks*, SSRN (Mar. 29, 2018, 02:14 PM), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2544742.

87 Ibid.

88 Ibid.

89 *Securing the Law Firm: Dark Web footprint analysis of 500 UK legal firms*, RepKnight (Mar. 29, 2018, 02:16 PM), https://www.repknight.com/wp-content/uploads/2018/01/White-Paper-Securing-the-Law-Firm-January-2018-Website-LM.pdf.

Lack of investment also means that firms are understaffed in terms of specialist IT personnel to manage cyber risk. Large law firms, especially those spoken to by the authors, operate with small teams of between 4 and 10 cyber risk professionals, severely curtailing their ability to affect cultural change within such large organizations. An interesting consequence of this, which to a large extent is explained by the organizational environment of law firms, is that legal and IT teams operate in silos almost completely disconnected from each other. Legal teams or departments are characterised by autonomous self-interest, prioritising the team instead of the firm as the collective in the pursuit of revenue maximization by way of billing, and the IT team is so small that it is a rare occurrence for the legal team to ever have sight of them, beyond their 8-minute yearly compliance video, of course. At present, IT and cyber security matters are delegated to the IT or IT Risk team, who fix the matter and enable the lawyer to get back to work, with little or no integration or information sharing between the teams. When the IT team attempt to introduce new measures, they are likely to meet resistance on budgetary and personnel fronts. For example, the implementation of new cyber security systems can entail considerable expense and the time spent training-in personnel on such systems (or time not spent billing) would be hard to recover.[90] Additionally, the introduction of security measures such as limiting access to networks or mandating frequent password changes, or the implementation of internal cyber security policies intended to improve conduct within legal teams are likely to be perceived as cumbersome, time-consuming and intrusive for lawyers and therefore are less likely to be followed.[91] Wald refers to these as 'Holmesian bad people', or those who will attempt to get away with not implementing appropriate cyber security measures owing particularly to an acute awareness of the underregulation of law firm cyber security conduct.[92]

III. PART 3 – THE SOLUTION

A The inadequacy of the current approach to training

It should now be clear that law firm cyber security, while in need of drastic improvement, faces significant challenges in order to overcome the inter-related complexities that have curtailed such improvement over time before any real progress can be made. Law firms are moving to shore up cyber defences, but current approaches revolve around software protection, spearphishing penetration testing, inadequate and expensive cyber risk insurance, awareness alliances, sponsored seminars and formal tick-box compliance training for minutes per year. None of these approaches are effective at impacting the human behaviour aspect of cyber security defence, as is clear by the mounting evidence of continued cyber breaches experienced by law firms and lack of appreciation for cyber risk in lawyers'

---

90 Alex Blau, *The Behavioral Economics of Why Executives Underinvest in Cybersecurity*, Harvard Business Review (Mar. 29, 2018, 02:17 PM), https://hbr.org/2017/06/the-behavioral-economics-of-why-executives-underinvest-in-cybersecurity.

91 Eli Wald, *Legal Ethics' Next Frontier: Lawyers and Cybersecurity*, 19, CHAPMAN LAW REVIEW 501 (2016).

92 Ibid.

online behaviour, all attributable to human error. These protections represent the best and the most extensive in the legal profession at present.

As outlined earlier, the most effective means of attack is spearphishing. A recent FireEye whitepaper highlights that the most effective means of preventing spearphishing is to first and foremost, "train users to recognise, avoid and report suspicious emails"; second is to "maintain and update security technology and processes to prevent, detect and respond to ever-evolving spear-phishing threats" and thirdly striving "to stay ahead of attackers by investing in actively updated threat intelligence and expertise to meet their needs".[93] The second and third elements of this strategy pose an issue owing to the short-termist nature of law firms, aversion to investment and the difficultly of overhauling systems for globally operating firms. However, the first issue is by some way the most crucial but also the most troublesome for law firms. Effective means of training employees to deal with spearphishing requires persistent testing backed up with context-specific educational training so that employees are regularly educated as to the dangers of spearphishing, know how to detect an attack and what to do when they suspect one, and their susceptibility to attack is constantly tested to promote vigilance and defence skills development[94]. Training is the most important element of defence against spearphishing primarily because it builds skills and awareness to deal with attacks if and when a firm's software defences are penetrated. Additionally, training and awareness are crucial in establishing the foundations of a culture of good cyber practice, with such skills and awareness positively permeating throughout the organization and subsequently impacting the investment decisions of the partnership. A recent report by PhishMe highlights the importance of such training. They note that training employees to spot and report spearphishing emails reduced the average time it took to detect a breach from 146 days to 1.2 hours.[95] In its absence, the partnership is likely to compartmentalise IT and infrastructure spend (including training) as just another budgetary consideration, without the added consideration that such a business risk warrants. Law firms are doubtless aware of the need for such training, and yet it is has almost no prominent role to play within the organization. The reality of short-termism has meant that, for law firms, hourly billing and 24/7 availability to clients and such training are perceived to be mutually exclusive. This consideration also holds true for the other 2 elements of the FireEye whitepaper, with firm-wide IT infrastructure updates likely to be perceived as disruptive and precipitate further lost time. In the face of underregulation of their cyber security conduct, law firms have had little incentive to find a solution to this issue.

93 *Best Defense Against Spear Phishing*, FireEye (Mar. 29, 2018, 02:19 PM), https://www.fireeye.com/current-threats/best-defense-against-spear-phishing-attacks.html.

94 Ibid.

95 *Phishing Defense Guide 2017*, PhishMe (Mar. 29, 2018, 02:20 PM), https://www.ciosummits.com/PhishMe-Phishing-Defense-Guide_2017.pdf.

B Cause for improvement

Arguments abound as to why law firms need to improve cyber security defences. We have noted some key reasons above: attacks are increasing in quantity and complexity; breaches are becoming more common and more high-profile; the impending introduction of the GDPR; clients are demanding a certain standard of cyber protection at the beginning of the relationship; data privacy and data stewardship awareness and perception are becoming much more commonplace; there is a prospect of malpractice suits by aggrieved clients for lax cyber security practices and breach of fiduciary duty to protect information. Furthermore, a successful breach that plays out on the public stage will serve to erode a firm's reputation. For example, in 14 March 2018, Mossack Fonseca – the firm implicated in the Panama Papers – announced that it was to shut down at the end of the month, citing the "reputational deterioration" that occasioned "irreversible damage" on the firm.[96] We would also add that strong cyber defence capability now has key differentiating potential in an ultra-competitive buyer's market for legal services. While law firm cyber security is underregulated, the conduct of their clients, for the most part, is not and carries with it enormous non-compliance costs. For example, organizations in the financial services and healthcare sectors are subject to strict data security laws, which are destined to become more-so upon the introduction of the GDPR this year. Such organizations are under an obligation to require their supply chain to attain a certain level of cyber security protection in order to comply with provisions of the GDPR. If law firms can demonstrate adequate cyber defences when compared to competitors, during the pitch process for example, their chances of being perceived favourably by prospective clients who see cyber security as a critical business risk, are likely to be substantially higher than firms with weaker cyber defences. Firms typically need to show that they have technical expertise, geographical reach, project management protocols and tools to accurately control scope, cost and timing, but now also need to ensure and demonstrate that client information will be subject to the highest standards of information security. Incredibly, should a law firm be in a position to demonstrate the 3 elements of spearphishing protection detailed in the FireEye whitepaper, they would be perceived as market-leading in terms of cyber security protections. As Wald notes 96% of attacks employ simple techniques, such as spearphishing, and yet 97% of attacks can be blocked entirely by the use of common cyber security defence practices that are entirely within reach of law firms today. Such approaches comprise of the technological and human alike: "using current virus scanners and firewalls, installing patches and updates, using cryptographically strong passwords, avoiding risky software downloads from the Internet, eschewing the use of public cloud providers or file sharing services for sharing documents, avoiding the use of web-based e-mail services and public Wi-Fi, replacing the default passwords on network hardware, and training employees to recognize deceptive ("phishing") attacks".[97]

---

96 Reuters Staff, *Panama Papers law firm Mossack Fonseca to shut down after tax scandal*, Reuters (Mar. 29, 2018, 02:21 PM), https://www.reuters.com/article/us-panama-corruption/panama-papers-law-firm-mossack-fonseca-to-shut-down-after-tax-scandal-idUSKCN1GQ34R.

97 Eli Wald, *Legal Ethics' Next Frontier: Lawyers and Cybersecurity*, 19, CHAPMAN LAW REVIEW 501 (2016).

C. A human problem – insights from behavioral science

The technological protections described by Wald are a must, and to a large extent, already exist in law firms today. The human protections are significantly more important. Given that the vast majority of data breaches (95%) involve some aspect of human error, it is clear that cyber security is a human problem that requires a human solution, with effective training being the most critical component of the passport to success. But how do law firms reach this promised land, given the complex and crippling effects of short-termism and underregulation? To be sure, fundamental tenets of good cyber defence posture will inevitably require investment on behalf of the partnership – in-terms of systems and personnel, and also the implementation and enforcement of stringent cyber security policies, in a coordinated effort by legal and IT teams working together. It is our contention that the most important aspect of law firm cyber defence for our purposes – training employees to deal with spearphishing – which is a crucial defence mechanism in its own right, but also serves to underpin the likely success of such other aspects as policy development and enforcement within legal teams, does not require a dismantling of the short-termism/underregulation conundrum in order to arrive at a workable solution. Instead, what is needed is a change in how such training is perceived and delivered. The current e-learning approach to spearphishing training in law firms (a video tutorial and 'click next' test) is a concept first introduced in the late 1990s[98], and is in dire need of updating. Additionally, we note that some law firms have now made regular spearphishing penetration testing part of their defence protocol. The common approach is to send employees a suspicious email to their work email address and record the response, i.e. whether the recipient clicks on a link contained in the email, marks the email as spam, or ignores the email. One such email that one of the authors received while working for a large UK law firm related to the establishment of a mentoring scheme sponsored by Amazon, whereby Amazon customers who are professionals would sign up to mentor school children and other children from youth organizations in their community. The email immediately raises suspicion. The author concerned did not have an Amazon account set up with the firm's email, and there was therefore no reason for Amazon to send an email to this address, and so the email was duly marked as spam. Later, in a conversation with the Chief Information Officer of the firm (the same conversation where the authors uncovered the 8 minutes per year training figure), we learned that the spearphishing test sent to the majority of employees in the London office tricked 42% in to clicking on the bogus link in the email. Interestingly, spearphishing awareness information was circulated to those respondents that clicked on the link in the initial test, and when the test was repeated 1 week later with a different template, 75% of those respondents again clicked on the link. This serves to reinforce the point that spearphishing penetration testing, while an effective means of gauging vulnerability to spearphishing attack at any given time, is not effective at developing the skills and awareness needed to adequately defend against attack if not supported and reinforced by effective training with an element of duration.

---

98 Holly Faurot, *LMS 101: The Evolution Of Corporate Learning*, Forbes (Mar. 29, 2018, 02:23 PM), https://www.forbes.com/sites/paycom/2017/02/07/learning-management-systems-101-the-evolution-of-corporate-learning/#48b3e8105e25.

Daniel Solove sums up the need for a change in training methodology as follows: "Security is complicated because it essentially requires each employee to act with a high level of awareness and vigilance, a state that is hard to sustain. Over time, corners tend to get cut more, busy people tend to do more careless things, practices tend to become sloppy. That's human nature. Complacency sets in. Being on one's toes isn't an easy state to maintain. These problems are best addressed through training. Merely showing people a PowerPoint or putting them through a program that's the equivalent to an airline safety video is a waste of time. People must be engaged. They must care. And the message must be repeated over and over and over. People aren't robots, after all. They forget quickly ... The fact is, cyber security training is vastly undercapitalized, and the lack of investment in quality cyber education programs is manifest in the sheer volume of breaches that continue to be rooted in human failure ... To be clear, technology is a critical piece of the cyber security puzzle, but just as with a car containing all the latest safety technology, the best defence remains a well-trained driver".[99]

Appeals to employee engagement and incentivising them to care about security are themes rooted in the behavioural science work of Nobel Economics laureate Dr Richard Thaler and before him Daniel Kahneman and Amos Tversky.[100] Dr Thaler's work with Cass Sunstein on 'nudging', improving behaviour by arranging choice architecture without removing an individual's freedom of choice, has important application for cyber security within organizations. Thaler and Sunstein make the point that an organization's policies are predicated on the principle that its people do not intentionally behave irrationally and yet we fail to recognise our own biases, even if we consider ourselves to be completely rational. At work we don't always do the things that might improve our organization's security.[101]

The concept that nudging can improve organizational cyber defence has been adopted by the UK Centre for the Protection of National Infrastructure (CPNI), who have issued guidance to organizations on how to improve security defences, underpinned by the '5Es' framework: educate employees on why threats exist, the form they take and why they are vulnerable; enable employees to demonstrate the cyber defence skills expected of them; shape the environment to make it easier to demonstrate good cyber defence skills; encourage action by providing feedback to employees to encourage good cyber defence behaviour and skills development while highlighting errors and discouraging undesired actions

---

99 Daniel Solove, *Cybersecurity vs. Humans: The Human Problem Requires a Human Answer*, TeachPrivacy (Mar. 29, 2018, 02:23 PM), https://teachprivacy.com/cybersecurity-vs-humans-human-problem-requires-human-answer/.

100 Daniel Kahneman & Amos Tversky, *Prospect Theory: An Analysis of Decision under Risk*, 47, THE ECOMETRIC SOCIETY 263-292 (1979).

101 Philip Ebert & Wolfgang Freibichler, *Nudge Management: Applying behavioural science to increase knowledge worker productivity*, 6 JOURNAL OF ORGANIZATIONAL DESIGN 4 (2017); See also: RICHARD H. THALER & CASS R. SUNSTEIN, NUDGE: IMPROVING DECISIONS ABOUT HEALTH, WEALTH, AND HAPPINESS (2008).

and behaviours; and evaluate the impact on employee behaviour by tracking progress in skills development as against the time and resources committed to improving defence skills.[102] The guidance also highlights the importance of endorsement from credible sources in the organization's hierarchy such as C-suite executives as crucial to supporting the success of the framework.[103] Pfleeger and Caputo make the point in their survey paper which illustrates that leveraging behavioural science theory in establishing a defence infrastructure by catering for such elements as cognitive dissonance[104], the bystander effect[105] and confirmation bias[106], leads to clear improvements in employee cyber defence skills and awareness as well as an overall improvement in the effectiveness of organizational cyber defence. They note "most efforts to improve cyber security focus primarily on incorporating new technological approaches in products and processes. However, a key element of improvement involves acknowledging the importance of human behaviour when designing, building and using cyber security technology".[107]

D. Heads-up: A new approach to training using aspects of modern technology

The question remains: how can law firms move to a model that allows for effective spearphishing defence skills development and also establish the key foundations of a culture of good cyber security behaviour generally without detracting from lawyers' availability to clients or disrupting their work environment, which would negatively impact billable targets. We contend that modern technological innovations, when applied to current training methodologies to deal with spearphishing, have a key role in developing a realistic solution to the issue of spearphishing training in law firms. This, in-turn, allows

---

102 *Embedding Security Behaviours: using the 5Es*, Centre for the Protection of National Infrastructure (Mar. 29, 2018, 02:25 PM), https://www.cpni.gov.uk/system/files/documents/98/dc/Embedding-Security-Behaviours-Using-5Es.pdf.

103 Ibid.

104 Cognitive dissonance is the feeling of discomfort that comes from holding two conflicting thoughts in the mind at the same time. Cognitive dissonance is central to many forms of persuasion to change beliefs, values, attitudes and behaviours. To get users to change their cyber behaviour, we can first change their attitudes about cyber security. For example, a system could emphasize a user's sense of foolishness concerning the cyber risks he is taking, enabling dissonant tension to be injected suddenly or allowed to build up over time. Then, the system can offer the user ways to relieve the tension by changing his behavior.

105 The bystander effect is a psychological phenomenon in which someone is less likely to intervene in an emergency situation when other people are present and able to help than when he or she is alone. During a cyber event, users may not feel compelled to increase situational awareness or take necessary security measures because they will expect others around them to do so. Thus, systems can be designed with mechanisms to counter this effect, encouraging users to take action when necessary.

106 Once someone takes a position on an issue, she is more likely to notice or give credence to evidence that supports that position than to evidence that discredits it. Users may have initial impressions about how protected (or not) the information infrastructure is that they are using. To overcome their confirmation bias, the system must provide users with an arsenal of evidence to encourage them to change their current beliefs or to mitigate over-confidence.

107 Shari Lawrence Pfleefger & Deanna D. Caputo, *Leveraging Behavioural Science to Mitigate Cyber Security Risk*, 31, COMPUTERS & SECURITY 4 (2012).

for realistic behavioural change over time and the establishment of a key component of effective law firm cyber defence infrastructure without infringing on the constraints imposed by short-termism and underregulation. It is important to note this is not an abstract or theoretical solution suggested by the authors in light of the above analysis. This technology is already being applied to create non-disruptive, behavioural science-based spearphishing training, with real solutions available to organizations on the market today[108]. The approaches adopted by companies such as Cofense, Wombat and Fissure Security purport to upgrade the current standard of spearphishing training, which at present consists of sporadic spearphishing penetration testing, educational tutorials and the circulation of awareness material, which has little impact on employee cyber security behaviour and competence. These organizations propose continuous, non-disruptive training, as well as behavioural analytics to arrive at a scenario where employees can be tested and trained to improve cyber defence and awareness 24/7 and be provided with accurate feedback on their progress, while also maintaining availability to clients 24/7, as such training does not necessitate employees being removed from their normal work environment and is instead integrated with their work routine.

Such training involves a combination of i) spearphishing penetration testing in the form of distributing fictitious quick-action spearphishing emails (short context specific email containing a link or attachment) and using data analytics to track responses, and ii) an overlay on employees' computer screens that runs when the email application such as Outlook is open, and provides subtle but clear indicators of spearphishing (e.g. drawing users' attention to the email address, reminding users to consider whether any links in the email re-direct to an external website, and whether any attachments are referred to or described in the email or that the email and its attachments were expected by the user). These indicators or pockets of information, such as 'Security Tips', are displayed on screen but in a non-disruptive manner (e.g. small info boxes or coloured indicators in the margins of emails) and also do not require interaction in the form of 'click-to-agree' in order to avoid click fatigue. This training is then continually reinforced with regular spearphishing training emails (similar to the spearphishing penetration testing referred to above) which would target a particular aspect of spearphishing to test employees. Employees are tasked with reporting suspicious emails and rewarded with positive automated feedback should their detection be accurate. Those who fail the spearphishing penetration test receive automated feedback on why they failed and what to look out for next time, again in a non-disruptive manner. This method becomes all the more effective when employees are aware of the training and that they are likely to receive test emails skills feedback at any given moment. The net effect is that employees are always on the look-out for suspicious emails and adopt a 'report-in-any-case' default position. This is a response promoted by the perception that an employee may fail the test and receive negative feedback, a reaction

108 See for example: (Mar. 29, 2018, 02:26 PM), https://cofense.com/; https://www.wombatsecurity.com/; and http://fissuresecurity.com/.

explained by fear appeal and protection motivation theory.[109] Nobody wants to fail a test and receive negative feedback, especially not high-conscientious and highly-competitive lawyers. Furthermore, with the overlay running on real work emails in addition to spearphishing test emails, employees are constantly having their skills of detection topped-up. Add to this the circulation of context-specific awareness material about various aspects of cyber security threats, and the likelihood of catching a real attempt at spearphishing increases dramatically.

The application of technology with respect to the overlay in this context is best described with reference to airline pilots' heads-up displays: "As the key source of information for pilots, the human visual system has necessarily driven much of the evolution in cockpit technology. In contrast to the complicated, gauge-based systems of the past, the electronic flight displays of today's modern airliners are testament to advances in human factors engineering. The next step in flight instrumentation, although already used for some 50 years in the military, is just beginning to emerge in civil transport aircraft. Head-up displays (HUD) allow pilots to see key flight instrumentation while viewing the outside world. The need to look down at the flight instruments is removed by the HUD, resulting in increased situational awareness and greater precision in aircraft control ...The primary flight displays of modern transport aircraft do an excellent job of presenting information to pilots in a way that promotes efficiency and good situational awareness. However, the need to transition from the use of head-down displays to outside visual reference at certain points in the flight continues to create an attentional division, often during critical management periods. The use of HUD brings primary flight management information and outside visual reference into the same visual scene, increasing the usefulness and relevance of displayed symbology".[110]

Training such as this, which helps employees identify aspects of an attack; gives them an opportunity to report suspicious emails; receive demonstrable feedback on their cyber defence competence level; and regularly tests for weaknesses in order to reinforce good cyber defence skills and awareness certainly holds promise for law firms. This is especially so because the training can be conducted consistently over any desired period of time or for as long as it takes for a clear improvement in cyber defence competence and behaviour and is done so on a non-disruptive basis and within lawyers' normal work environment. This, it is argued, circumvents the issues caused by law firm short-termism, such as the billable hour culture and 24/7 availability to clients, but also can bring a positive change to the issue of underregulation of law firm cyber security conduct. Firms that can demonstrate effective cyber defence of their personnel can use this to win new clients who have set requirements high for cyber security standards of their supply chain, and also bolster existing client relationships for the same reason.

---

109 Sebastian Schuetz, Paul Benjamin Lowry and Jason Thatcher, Defending Against Spear-Phishing: Motivating Users Through Fear Appeal Manipulations (June 27, 2016). 20th Pacific Asia Conference on Information Systems (PACIS 2016), Chiayi, Taiwan, June 27–July 1.

110 Nichol RJ (2015) Airline Head-Up Display Systems: Human Factors Considerations. Int J Econ Manag Sci 4: 248.

Training such as this, which helps employees identify aspects of an attack; gives them an opportunity to report suspicious emails; receive demonstrable feedback on their cyber defence competence level; and regularly tests for weaknesses in order to reinforce good cyber defence skills and awareness certainly holds promise for law firms. This is especially so because the training can be conducted consistently over any desired period of time or for as long as it takes for a clear improvement in cyber defence competence and behaviour and is done so on a non-disruptive basis and within lawyers' normal work environment. This, it is argued, circumvents the issues caused by law firm short-termism, such as the billable hour culture and 24/7 availability to clients, but also can bring a positive change to the issue of underregulation of law firm cyber security conduct. Firms that can demonstrate effective cyber defence of their personnel can use this to win new clients who have set requirements high for cyber security standards of their supply chain, and also bolster existing client relationships for the same reason.[111]

IV. CONCLUSION

As Wald notes, stopping all cyber attacks is impossible to do. Yet, 96% of hacking attacks employ simple techniques, and 97% of attacks can be blocked by common security practices that are within the reach of even small law firms and solo practitioners. Chief among these common cyber security practices is training employees to recognize deceptive attacks, known as spearphishing.[112] Law firms face unprecedented danger from cyber attack owing to the increase quantity, quality and diversity of attacks and attack sources, and are also more vulnerable to attacks, presenting a 'lower hanging fruit' to hackers, in terms of size of the prize (and therefore potential liability costs to law firms) vs. effort to break in, than organizations in other industries. While it is true that law firms need to do more to protect client information, the issue is far more complicated than first appears. Law firm cyber defence has been stymied by a mix of short-termism and underregulation of cyber security conduct, which manifests itself in the form of external factors, including lax regulatory standards and ethics rules as well as non-existent client pressure, and internal factors, such as the partnership model and PEP marker of success which is underpinned by the billable hour. We have outlined that as well as a recent spate of high-profile law firm data breaches, there is a regulatory shift is underway with the introduction of the GDPR and an incoming wave of future, similarly inspired measures around data protection in the Digital era and also a change in client attitudes toward protection of their confidential information, meaning that law firms are now under pressure to improve defences. We have made clear that while law firms traditionally have been unable to train employees to deal with spearphishing owing to the requirements of the billable hour and culture of 24/7 availability to clients, modern technological innovations hold the potential to update spearphishing training methodologies to both address and dramatically improve the

---

111 McNerney, Michael, and Emilian Papadopoulos. "Hacker's Delight: Law Firm Risk and Liability in the Cyber Age." American University Law Review 62, no.5 (2013): 1243-1272.

112 Ibid.

human behaviour aspect of cyber defence through skills and awareness development, and also be non-disruptive in-terms of delivery, allowing lawyers to stay in their normal work environment and maintain availability to clients. However, this is only one aspect of an effective cyber defence infrastructure. A collective effort is needed on behalf of all personnel within law firms – lawyers and non-lawyers, at every level of the hierarchy, to implement and manage a comprehensive governance framework that promotes good, proactive, cyber security practice that permeates the firm's culture. Effective training that caters for the human aspect of cyber defence by comprising behavioural science principles and which can be delivered within the present constraints of law firm short-termism and underregulation, coupled with the development, implementation and enforcement of effective cyber security policies and procedures are the first steps in establishing the foundational aspects of good cyber practices and defence competence. A culture of sustainable, incentive-aligned cyber security embedded into everyday practice, fit for the digital age law firm.