**Robert D. Brownstone** Co-Chair, Privacy & Cybersecurity
rbrownstone@fenwick.com

**Kevin K. Moore** Chief Security Officer

Fenwick & West LLP, California

# Striving for legal compliance in cyber security: tech solutions

Robert D. Brownstone and Kevin K. Moore, of Fenwick & West LLP, here leverage their 'law plus technology synergy' that the pair offer in their practice to provide a unique perspective on cyber security defence, focusing on the ways that law, technology and employee-training intersect.

Like the decades before it, the start of the 21st century has seen exponential growth in data volumes and data repositories/platforms. As a result, bad actors have ratcheted up their illicit international efforts to access troves of valuable data. In turn, worldwide rules and regulations have proliferated and developed stricter protections as to personally identifiable information ('PII'). Yet, as always, legal developments lag behind 'in the trenches' realities. In addition, not only data security technology but also related employee training are in a never-ending race to try and defend against the ever expanding universe of schemes deployed by hackers.

The two of us spend many of our waking hours focused on cyber security defence, and especially the ways that the triad of law, technology and employee-training intersect in that realm. This article addresses three of our expectations:

1. In the coming years, privacy and data security legal requirements will continue to get stricter;
2. The persistence of a prior trend, whereby directives, statutes and regulations will remain silent or at most vague (e.g., merely mentioning 'encryption') as to technology solutions. Therefore, executives, security officers, lawyers and others will need to keep abreast of new technologies; and
3. Technology will remain unable to provide a magic bullet. Each organisation will need to maintain a sustained strategy for implementation and for training individuals in order to be vigilant.

## The legal landscape - vaster but still vague

Worldwide, the body of privacy (and thus data security) law keeps growing. We cannot possibly cover all the regimes here. But some highlights follow:

In Europe, on 25 May 2018, the General Data Protection Regulation[1] ('GDPR') will take effect, replacing the old Data Protection Directive of 1995[2]. Consequently, across the EU the already strong privacy rules will become even stricter, including by tying penalties to the violator's worldwide revenue, going farther as to notice of breach duties and beefing up the requirements for obtaining valid 'consent' from an individual for access to his/her data. Previously, in part as fallout of the June 2013 Edward Snowden revelations about the US Government, the old EU-US Safe Harbor was struck down by the CJEU and has been replaced by the more rigorous Privacy Shield[3]. Under the new regime, a US based company that self-certifies that it adequately protects personal data transferred to the US from the EU must provide free and accessible dispute resolution, cooperate with the US Department of Commerce, and ensure accountability for data transferred to third parties.

Elsewhere in the world, various laws protective of individual privacy continue to crop up and proliferate. In the first quarter of 2018, Australia and Israel will join the group of countries that have data breach notification laws. Moreover, between now and the date the UK's EU exit negotiations conclude (likely in 2019), the UK seems likely to alter its Data Protection Act to ensure compliance with the GDPR's protective provisions[4].

In the US, there is still no omnibus data privacy legal framework. Instead, data privacy law is a mosaic of sector specific laws concerning personal health information, financial information and various sorts of consumer protection. The last category entails in part the prohibition of deceptive and unfair business practices by Section 5 of the Federal Trade Commission ('FTC') Act as well as states' consumer protection laws.

In addition to the Privacy Shield being more restrictive than its predecessor framework, privacy protections have continued to expand in the US. As to US Government activity, the FTC has remained quite vigilant in enforcing not only the FTC Act but also other federal privacy laws. As to US private plaintiff lawsuits, a current hot topic in federal decisional law is 'standing'; namely the extent to which individuals must allege an 'injury' to be able to pursue a statutorily based claim. Some, but not all, of the onslaught of judicial opinions in this arena have opened the door wider for the viability of various privacy claims, even in the absence of allegations of actual identity theft.

In other US developments, now almost every state has its own set of notice of breach laws such that there is a greater patchwork of baseline requirements. Meanwhile, some states are in various stages of interjecting themselves into the regulation of how financial institutions protect private information. Most notable is New York's Regulations of the

Superintendent of Financial Services (Cybersecurity Requirements for Financial Services Companies) (1 March 2017)[5].

In summary, the international body of legal requirements, some overlapping and some disparate, continues to grow exponentially.

**Tech solutions - not usually in the law; you'll need to seek them out**

Directions as to specific protective measures are typically nowhere to be found in privacy laws. Even when some mention is made of a specific measure, such as encryption, there are no details. For example, while encryption is sometimes an express requirement, and other times an implicit one by providing an exemption from a notice of breach obligation, we are not aware of any legal rule that describes the type or level of encryption to be deployed. There is some hope that the US State of Colorado will follow through on its plan to enact some more specific rules in the context of broker dealers and investment advisers[6]. Even more optimistically, perhaps new rules such as these will have a spillover effect into other contexts, not just the investment industry.

A number of organisations have developed frameworks that can help an organisation self-audit and/or prepare for an outside audit. Even so, IT, information security and privacy leaders need to remember that information security revolves around three key areas: people, process and technology. Technology is not the 'silver bullet' when it comes to information security, but it will allow an organisation to orchestrate and automate some processes due to lack of staff resources. We will look at the technology aspect in the below mentioned areas of information security and provide some insight into the hunt for hardware and/or software solutions. There are times when there is a need to employ outside consulting services not only to do periodic penetration and vulnerability tests, but also to help make data security tools interact effectively in a given IT environment or web based platform.

With that said, here is a list of some categories of technology that could be deployed and, where apt, some non-exhaustive lists of examples of pertinent respective products:

*Email protection*

**Why?** Generally, email is the largest data set a company possesses. It is also the most susceptible to being compromised in a way that causes harm. This is due to the sheer amount of communications and the speed at which people use it, often without taking time to reflect or revise before hitting 'send.'

**What to use?** Enforced Transport Layer Security ('TLS') of TLS 1.1 or higher, which ensures that messages and attachments are encrypted end to end.

*Encryption*

**Why?** Encryption is not only needed for email and email attachments. It is highly recommended to encrypt data in all locations, whether at rest or in transit. Ensure that:

1. All data storage locations are utilising Advanced Encryption Standard ('AES') 256-bit keys as the minimum level of disk/drive encryption.
2. All transport points are using encryption of Secure Socket Layer ('SSL') or TLS 1.1 or higher (Note that by their very nature, a virtual private network ('VPN') connection, used for remote login to a network or to a remote desktop, entails encryption of data in transit via SSL, TLS or Internet Protocol Security ('IPSec')).
3. All sharing locations such as websites, extranet servers, cloud sites and file transfer protocol ('.ftp') sites entail the use of encryption for data in transit and at rest.

**What to use?** Encryption of data at rest on servers, desktop computers, laptops and portable media: BitLocker[7] (Windows) and FileVault[8] (MAC).

**Encryption level for data to be uploaded to sharing locations:** AES 256-bit keys.

**Encryption of data in transit between your environment and sharing locations:** SSL or TLS 1.1 or higher.

**Encryption level for data at rest in sharing locations:** AES 256-bit keys.

*Phishing protection*

**Why?** Phishing, which includes spear phishing, whaling and the like, is the number one threat to a company's information security and is involved in the vast majority of data breaches.

**What to use?** Sender Policy Framework ('SPF')[9], DomainKeys Identified Mail ('DKIM')[10] and Domain-based Message Authentication, Reporting & Conformance ('DMARC')[11] protocols. These mechanisms provide spoofing protection from messages pretending to come from one's own domain, and from other threats (e.g. malware). DMARC is an email authentication protocol that authenticates the author's ('From') domain. See the Request for Comment ('RFC') 7489[12], one of a series of publications by the Internet Engineering Task Force ('IETF'). While internal administrators can implement DMARC there are companies that will manage it for you, such as ValiMail[13].

Spam, malware/virus protection provided by a cloud based service, such as Proofpoint[14].

PhishMe[15] suite of tools, including waves of tests to train executives and staff to be discerning.

*Password rules and management*

**Why?** These processes guard against hackers' automated password cracking as a means of gaining an inroad into your network.

**What to use/enforce?** If at all possible in your environment, implement two factor authentication for remote access, e.g. to a virtual desktop via a VPN connection. Products: RSA SecurID® Suite[16] - hard and soft tokens. Duo Security[17] products - two-factor, device identification and Single Sign-On ('SSO'). Okta[18] solutions and products - two-factor and SSO. Basic password hygiene, namely set the parameters for user authentication passwords to the following: complex; at least eight characters; periodic changes (every 90 days?), and re-use restrictions or prohibitions.

Also implement a sponsored password management software for all users, such as: 1Password[19], KeePass Password Safe[20], and LastPass[21].

*Access control*

**Why?**

- Minimise the chances that a [set of] data file(s) gets copied to too many locations. Strive to ensure that each user (inside or outside of the organisation) only has access to the resources necessary to perform his/her respective tasks, while preventing access to resources that are not relevant to that user. Limit who can get to what based on 'need to know[22].'
- Follow the Principle of Least

Privilege ('POLP'), which limits user access to the minimum number of corporate resources needed for immediate job functions. POLP has become crucial in access control.

**What to use for Least Privilege implementation?** BeyondTrust[23] solutions; CyberArk® Privileged Account Security Solution[24]; Microsoft Least-Privilege Administrative Models[25].

*End-point protection, detection and remediation*

**Why?** Protection of the computing environment needs to extend beyond the core infrastructure equipment to the end user computing devices such as laptops, tablets and mobile devices. These devices provide a means of mobility for the end user and at times are not encompassed by your normal information security safeguards. Your organisation needs to be able to sense, analyse and respond in real time to anomalous activity.

**What to use?** Threat detection and protection: Cisco Advanced Malware Protection ('AMP')[26], Cisco OpenDNS products and services[27], CrowdStrike Falcon™ Platform[28], Cylance PROTECT[29] and Cylance V[30].

*Third party (vendor) risk management*

**Why?** Every organisation must ensure it has identified the outside parties with access to the organisation's systems and data. Then it should implement and deploy:

- secure procedures;
- strict policies for those outside users to follow; and
- effective monitoring technology to detect if the third parties are putting the organisation at risk.

**What to use?** BitSight[31] products and solutions. Prevalent[32] vendor risk management automation software.

## Effective implementation requires training and vigilance

Cyber security has three pillars (three P's): legally compliant Process, effective technology Platforms, and educated, vigilant People. We have provided some insights into the law and technology aspects of data security but the People pillar is at least as important, if not more so. The human element of the cyber security triad needs continuous monitoring and improvement through the use of policies and a cyber security awareness program.

*Some key policies*

**Technology Acceptable Use Policy ('TAUP')** - Defines what is acceptable use of company computing resources but also includes what is not acceptable. In the United States, a TAUP can take away from employees any 'reasonable expectation of privacy.' A TAUP can also explain 'netiquette' such as the dangers of Bcc's, sending company-wide emails, clicking on 'Reply All,' and using auto-complete.

**International travel policy** - Defines what is permitted in terms of equipment when travelling, key behaviour do's and don'ts when abroad, and how to interact with a country's border patrol/customs personnel.

**Social media policy** - Addresses permissible and impermissible postings on social networking pages, whether sponsored by the employee themselves or maintained by the individual employees. Examples of impermissible posts would include: expressly or implicitly divulging highly confidential information unrelated to the worker's conditions of employment, or disclosing in text or via a photo personal information about an individual such as a patient, customer or co-worker.

*Ongoing education*

It is insufficient to train employees upon onboarding and at each juncture when a key policy is rolled out or amended. A security awareness program provides a continuous learning environment for all areas of cyber security of which end users of all organisations need to be reminded. Examples of modules within an awareness program include, without limitation, passwords, phishing, travelling (business and personal), email usage, and malware vigilance. Generally, each module consists of a short five to ten minute video clip followed by a short quiz and a takeaway document for the user. Examples of services that develop such modules are KnowBe4[33] and OnGuard[34].

## Conclusion

An organisation of any shape or size can do its best to tackle cyber security by following the three P's.

1. http://www.eugdpr.org/
2. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML
3. https://www.privacyshield.gov/welcome
4. Mathew J. Schwartz, 'Data Privacy After Brexit: Keep Calm and GDPR On,' Bank Info Security, http://www.bankinfosecurity.com/blogs/data-privacy-after-brexit-keep-calm-gdpr-on-p-2453 (20 April 2017).
5. http://www.dfs.ny.gov/legal/regulations/adoptions/adoptdfs.htm
6. See Ed Silverstein, 'Colorado Latest State to Propose Cybersecurity Compliance Rules,' Legaltech News http://www.legaltechnews.com/id=1202784952922/Colorado-Latest-State-to-Propose-Cybersecurity-Compliance-Rules?mcode=0&curindex=0&curpage=ALL (1 May 2017) (discussing proposed Code of Colo. Regs. Div. of Secs. Rules 51-4.8, and Rule 51-4.14(IA)) https://drive.google.com/file/d/0BymCt_FLs-RGUWI5c3lDUVlzeDg/view
7. https://docs.microsoft.com/en-us/windows/device-security/bitlocker/bitlocker-use-bitlocker-drive-encryption-tools-to-manage-bitlocker
8. https://support.apple.com/kb/PH25553?viewlocale=en_US&locale=en_US
9. http://www.openspf.org/
10. http://www.dkim.org/
11. https://dmarc.org/
12. https://www.rfc-editor.org/info/rfc7489
13. https://www.valimail.com/
14. https://www.proofpoint.com/us/product-family/email-protection
15. https://phishme.com/
16. https://www.rsa.com/en-us/products/rsa-securid-suite
17. https://duo.com/
18. https://www.okta.com/
19. https://1password.com/
20. http://keepass.info/
21. https://www.lastpass.com/
22. See, e.g., Keith Lipman, 'Need to Know' Security: New Standard of Care, New Competitive Advantage, Legaltech News (24 April 2017), http://www.legaltechnews.com/id=1202784351877/Need-to-Know-Security-New-Standard-of-Care-New-Competitive-Advantage?mcode=0&curindex=0&curpage=ALL
23. https://www.beyondtrust.com/products/
24. https://www.cyberark.com/products/privileged-account-security-solution/
25. https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/implementing-least-privilege-administrative-models
26. http://www.cisco.com/c/en/us/products/security/advanced-malware-protection/index.html
27. https://www.opendns.com/
28. https://www.crowdstrike.com/products/
29. https://www.cylance.com/en_us/products/our-products/protect.html
30. https://www.cylance.com/en_us/products/our-products/cylancev.html
31. https://www.bitsighttech.com/
32. https://www.prevalent.net/
33. https://www.knowbe4.com/
34. https://www.travelingcoaches.com/onguard