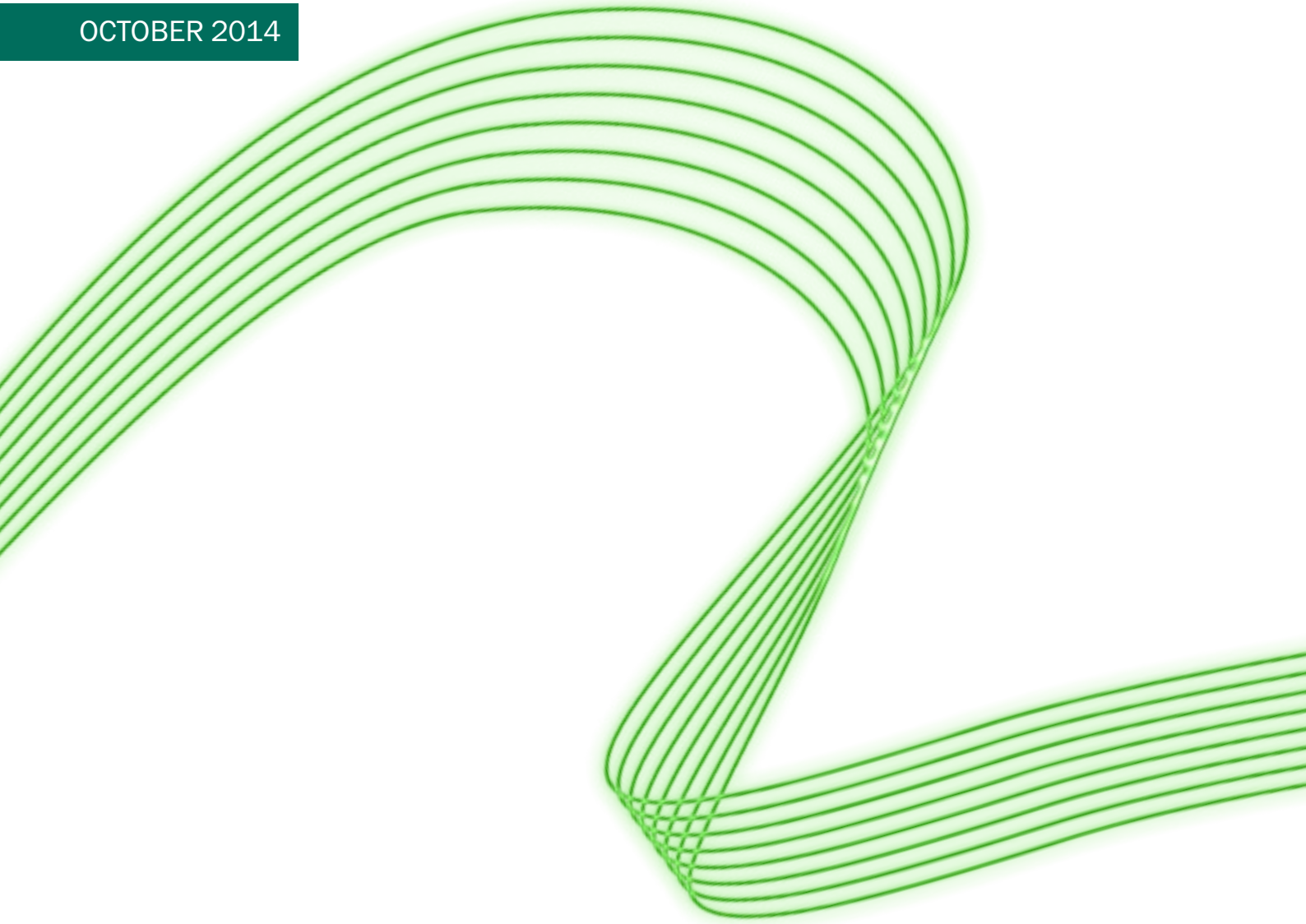
OCTOBER 2014



INFORMATION SECURITY AND LEGAL COMPLIANCE: FINDING COMMON GROUND IN A MOBILE ENVIRONMENT

A whitepaper exploring the common threads of information security laws and regulations; confidentiality, integrity and availability.

Written by Michael R. Overly Esq., CISA, CISSP, CIPP, ISSMP, CRISC

Empower business through security
kaspersky.com/business #securebiz

KASPERSKY lab

Contents

Introduction

1.0

Reconciling all legal obligations can be, at best, a full time job and, at worst, the subject of fines, penalties, lawsuits, and adverse and unwanted publicity.

Businesses today are faced with the almost insurmountable task of complying with a confusing array of laws and regulations relating to data privacy and security. These can come from a variety of sources: local, state, national, and, even, international law makers. This is not just a problem for big businesses. Even a small business with a localised geographic presence may be subject to laws from other states and, possibly, other nations by virtue of having a presence on the internet, including interacting with the internet through mobile devices and apps.

In many instances, these laws and regulations are vague and ambiguous, with little specific guidance as to compliance. Worse yet, the laws of different jurisdictions may be, and frequently are, conflicting. One member state or country may require security measures that are entirely different from those of another state or country. Reconciling all of these legal obligations can be, at best, a full time job and, at worst, the subject of fines, penalties, lawsuits, and adverse and unwanted publicity.

In response to the growing threat to data security, regulators in literally every jurisdiction have enacted or are scrambling to enact laws and regulations to impose data security and privacy obligations on businesses. Even within a single jurisdiction, a number of government entities may all have authority to take action against a business that fails to comply with applicable standards. That is, a single security breach may subject a business to enforcement actions from a wide range of regulators, not to mention possible claims for damages by customers, business partners, shareholders, and others. The U.S. for example uses a sector-based approach to protect the privacy and security of personal information (e.g., separate federal laws exist relating to healthcare, financial, credit worthiness, student and children's personal information). Other approaches, for example in the European Union, provide a unified standard, but offer heightened protection for certain types of highly sensitive information (e.g., healthcare information, union membership etc). Actual implementation of the standards into law is dependent on the member country. Canada uses a similar approach in its Personal Information Protection and Electronic Documents Act (PIPEDA). Liability for fines and damages can easily run into millions of dollars. Even if liability is relatively limited, the company's business reputation may be irreparably harmed from the adverse publicity and loss in customer and business partner confidence.

While most privacy and security-related laws today are written broadly and intended to be technology neutral (i.e., they don't focus on any particular type of technology to avoid having their laws quickly become outdated as technology evolves), there is a growing trend on the party of law makers to look at particular 'means' of collecting, processing, storing, and transmitting information. An obvious example that already exists is the wide range of laws specifically directed at email, particularly the transmission of unsolicited email (e.g., anti-spam laws). More recently, law makers have started developing laws directed at mobile devices and their applications. Last year, for example, the European Union Article 29 Data Protection Working Party issued Opinion 02/2013 On Apps On Smart Devices. In addition, in both the United States and the European Union, regulators are already working on regulations and guidances for use of mobile devices in the healthcare context (e.g., European Directive 93/42/EEC on Medical Devices). Finally, some countries are even updating their anti-spam laws to more particularly address use of mobile devices and apps (see, e.g., Canada's new anti-spam law, which became effective July 1, 2014).

42% of businesses currently conduct sensitive transactions on their mobile devices.[1]

Laws and regulations are directed at having businesses to do what is reasonable and appropriate, not what is impracticable or unreasonable.

Data security threats are at an all-time high. Seldom a week goes by without another story appearing in the news describing the latest company to become the subject of a data security breach. While the threat from hackers is substantial, according to the American Federal Bureau of Investigation (FBI), the incidence of 'insider' misappropriation or compromise of confidential information has never been higher. Insiders include not only a company's own personnel, but also its contractors and business partners. It is for this reason that this whitepaper focuses on two of the most substantial insider threats: situations in which a business' partners and vendors are entrusted with sensitive corporate data and Bring Your Own Device (BYOD) programmes where corporate data is accessed on devices over which the company has little control. In the first, insiders who are third-parties (i.e., vendors and business partners) create the risk that must be mitigated. In the second, insiders who are employees create the risk.

While there are no easy solutions, this whitepaper seeks to achieve several goals:

- To make clear that privacy relating to personal information is only one element of compliance. Businesses also have obligations to protect a variety of other types of data (e.g., trade secrets, data and information of business partners, non-public financial information, etc.).
- To sift through various privacy and security laws and regulations to identify three common, relatively straightforward threads that run through many of them:
    1. Confidentiality, Integrity, and Availability (CIA) requirement
    2. Acting 'Reasonably' or taking 'Appropriate' or 'Necessary' measures
    3. Scaling security measures to reflect the sensitivity of the information and magnitude of the threat

  By understanding these general, high-level concepts, businesses can better understand their overall compliance obligations. One point, however, bears emphasis: information security and privacy laws do not require the impossible. Perfect security, while a goal, is not the requirement. Rather, as will be repeatedly stressed in the discussion that follows, laws and regulations in this area are directed at having businesses do what is reasonable and appropriate, not what is impracticable or unreasonable. If a business achieves that standard and a breach nonetheless occurs, it will not generally have a compliance problem.
- To highlight the potential risks of non-compliance (e.g., lawsuits, fines, sanctions, etc.) and discuss common misconceptions about information security and privacy laws.
- To provide two real-world examples of how these principles can be put into action, including specific steps to mitigate risk and satisfy compliance obligations:
    1. The first example discusses how to better integrate information security into vendor and business partner relationships.
    2. The second example focuses on controlling risk in implementing a Bring Your Own Device (BYOD) programme.

1 Kaspersky Lab – Global IT Risks Report 2014

What Kind of Data Should be Protected?

2.0

Losing the ability to operate is a major cause for concern after a data breach or security attack. Of the companies who had experienced data loss, about a third were left without the ability to trade.[2]

In thinking about information security law and regulations, most people immediately think of personally identifiable data or personal information. While it is certainly true that most laws and regulations focus on personal information, this is only one type of data for which businesses may have legal obligations. Almost every business will have a wide variety of highly sensitive information that must be secured. Some examples include:

General Confidential Information of the Business

This could include financial information, marketing plans, potential promotional activities, business contact information, investor information, new product plans, customer lists, etc.

Intellectual Property

Intellectual property frequently comprises one of the most, if not the most, substantial asset of businesses. A breach of security could result in the business forever losing its ability to enforce its intellectual property rights. For example, trade secrets are defined as sensitive information of a business that has value because it is not generally known in the industry and is the subject of efforts by the business to ensure it remains confidential (e.g., the formula for Coca-Cola®). If a trade secret is revealed to the public, it loses its status and value as a trade secret. Almost every business has at least some trade secrets. A customer list, software source code, formulas, methods of doing business, etc. can all be trade secrets. These must be secured to ensure the information remains protected as a trade secret.

Healthcare Information

Healthcare information is one of the most highly regulated and sensitive types of information. In the United States, for example, the Health Insurance Portability and Accountability Act (HIPAA) regulates the privacy and security of personal health information. In some jurisdictions, it is afforded the highest protection in comparison with other types of personal data. In the European Union, healthcare information is afforded heightened protection under the European Union Data Protection Directive, as reflected in the member countries' implementing laws. See also the Australian Privacy Act 1988 and recent Privacy Amendment (Enhancing Privacy Protection) Act. A business may be in the healthcare industry and have possession of actual patient records, but even a business that has nothing to do with the healthcare industry may have healthcare information of its employees (e.g., insurance claim information) that it is obligated to protect.

Personal Financial Information

Like healthcare information, personal financial information is also heavily regulated and highly sensitive. In the United States, the Gramm-Leach-Bliley Act (GLBA) addresses the privacy and security of personal financial information. In other countries, personal information is broadly defined in overarching laws so as to encompass almost anything identifiable to an individual, including, of course, financial information. See, for example, Japan's Personal Information Protection Act. As with healthcare information, a business need not be in the financial services industry to possess this type of information. Every employer has sensitive financial information of its employees (e.g., salary information, social security and other personal identification numbers, bank account numbers, etc.).

2 Kaspersky Lab – Global IT Risks Report 2014

Security Information

Even security information, itself, is sensitive and should be protected. A business's security policies, security audit reports, disaster recovery and business continuity plans, and other similar information are all highly sensitive. If compromised, the information could be used to exploit vulnerabilities in the business.

The explosive growth of mobile devices and the multitude of applications available for them present particular risk. The European Union Article 29 Working Party emphasised this risk in its Opinion 02/2013 on Apps on Smart Devices: "Apps are able to collect large quantities data from the device (e.g. data stored on the device by the user and data from different sensors, including location) and process these in order to provide new and innovative services to the end user. However, these same data sources can be further processed, typically to provide a revenue stream, in a manner which may be unknown or unwanted by the end user." That is, mobile apps present unprecedented opportunities for the accumulation of data, but present an equally significant opportunity for risk.

Why Protections are Important

3.0

54% of companies revealed that data loss had had a negative impact on their reputation, reducing their perceived reliability in the eyes of customers, stakeholders and the wider business world.[3]

Legal compliance is certainly at the very top of every business's list in terms of reasons to implement information security measures to protect sensitive data. However, there are other, very significant, reasons for businesses to address this risk.

Protecting Corporate Assets

As noted in the preceding Section, in addition to personally identifiable data, every business also has other, highly proprietary information that it must protect (e.g., intellectual property, marketing plans, new product plans, investor information, financial information, etc.). These are all valuable assets of the business, deserving of protection.

Establishing Diligence

Many laws and regulations include the concept of requiring the business to act with due diligence in protecting sensitive data. The same concept exists more generally in the obligation of corporate management to act with due care and to exercise reasonable judgment in conducting the business, which would include acting with due diligence in protecting corporate information assets. Neither applicable law nor this more general corporate governance standard require perfection. Rather, the business and its managers must be able to demonstrate they acted reasonably, appropriately, and with due diligence in protecting their information assets. By implementing and documenting a thoughtful approach to mitigating information security risks, the business and its managers will have evidence to support they did just that in the event of a breach.

Protecting Business Reputation

Being the subject of a security breach can dramatically harm a business's reputation. Adverse publicity of this kind could seriously harm a business. Customers and business partners may lose confidence in the business's ability to protect their information and secure their systems.

Minimise Potential Liability

Finally, the most obvious reason for implementing a thoughtful approach to information security is minimising potential liability. Liability can take many forms: fines by a variety of regulators, statutory sanctions, shareholder lawsuits, and civil suits by business partners and customers (including the possibility of costly class action lawsuits) against both the business and, potentially, against its management.

3 Kaspersky Lab – Global IT Risks Report 2014

Common Misconceptions about Information Security Compliance

4.0

“

The laws and regulations in this area do not require perfection – they are directed at having businesses do what is reasonable and appropriate.

There is much confusion and many misconceptions when it comes to information security compliance. The two biggest misconceptions are that ‘it’s *all* about the data’ and ‘it’s *all* about confidentiality’. While data and confidentiality are certainly of critical importance, a more holistic approach is required. A business must be concerned about its data, but it must be equally concerned about the systems on which the data resides. In addition, confidentiality is only one of the three key protections required for true security.

Anyone involved in information security should be familiar with the acronym ‘CIA’. For data to be truly secure, each of these three elements must be satisfied. ‘Confidentiality’ means the data is protected from unauthorised access and disclosure. ‘Integrity’ means the data can be relied upon as accurate and that it has not been subject to unauthorised alteration. Finally, ‘Availability’ means the data is available for access and use when required. It does no good to have data that is confidential and the integrity maintained, but the data is not actually available when a user requires it. To achieve this last requirement, the systems on which the data resides must have specific service levels for availability, response time, etc. This is particularly important when a third party vendor may be hosting the data for the benefit of the business.

The importance of CIA cannot be overstated. It is not just a concept in information security treatises. Law makers have directly incorporated that very language into certain information security laws and regulations. Businesses that fail to achieve CIA with regard to their data, may be found in violation of those laws.

A final misconception about information security and privacy laws is that they require perfection (i.e., any breach, regardless of how diligent the business has been, will create liability). This is not true. The laws and regulations in this area are directed at having businesses do what is reasonable and appropriate. If the business achieves that standard and a breach nonetheless occurs, it will not generally have a compliance problem.

Finding Common Threads in Compliance Laws and Regulations

5.0

The sheer number and variety of laws and regulations that can apply to even small businesses handling sensitive information can be daunting, if not overwhelming. In some instances, it may be almost impossible for even a large, sophisticated organisation to identify all applicable laws, reconcile inconsistencies, and then implement a compliance programme. In this section, the goal is not to discuss any specific laws or regulations, but to identify three common threads that run through many of them. By understanding those common threads, businesses can more easily understand their baseline compliance obligations.

These threads run not only through laws and regulations, but also contractual standards such as the Payment Card Industry Data Security Standard (PCI DSS) and, even, common industry standards for information security published by organisations like CERT at Carnegie Mellon and the International Standards Organization (ISO). Embracing these common threads in designing and implementing an information security programme will greatly increase a business's ability to achieve overall compliance with the laws, regulations, and other requirements (e.g., PCI DSS, industry standards, etc.) applicable to it.

Confidentiality, Integrity, and Availability (CIA)

As discussed in Section 4, the age-old concept of CIA found in every handbook on information security has now been codified into many laws and regulations. The three prongs of this concept address the most fundamental goals of information security: the data/information must be maintained in confidence, it must be protected against unauthorised modification, and it must be available for use when needed. The lack of any of the foregoing protections, would materially impact compliance and the value of the information asset.

Acting 'Reasonably' or Taking 'Appropriate' or 'Necessary' Measures

The concept of acting 'reasonably' is used in many state and federal laws in the United States, Australia, and many other countries. The related concept of acting so as to take 'appropriate' or 'necessary' measures is used in the European Union and many other areas. Together, they form the heart of almost every information security and data privacy law. A business must act reasonably or do what is necessary or appropriate to protect its data. Note that this does not require perfection. Rather, the business must take into account the risk presented and do what is reasonable or necessary to mitigate that risk. If a breach, nonetheless, occurs, provided the business has established this basic requirement, it will not be generally found in violation of the applicable law or regulation.

Scaling Security Measures to Reflect the Nature of the Data and Threat

A concept that is closely related to acting reasonably or doing what is appropriate is the idea of scaling security measures to reflect the nature of the threat and sensitivity of the data. That is, a business need not spend the entirety of its security budget to address a low risk threat. But, if the risk is substantial, particularly in light of the volume and/or sensitivity of the data, the level of effort and expenditure by the business to address that risk must increase. A database with only names and physical addresses may not require as much security as a database of names, addresses and Social Security numbers. To better understand this concept, the following are excerpts from two laws that incorporate 'scaling':

First Example

A business should implement *safeguards that are appropriate to (a) the size, scope and type of business of the person obligated to safeguard the personal information under such comprehensive information security programme; (b) the amount of resources available to such person; (c) the amount of stored data; and (d) the need for security and confidentiality of both consumer and employee information'*

Second Example

Security efforts should take into account:
(i) The size, complexity, and capabilities of the business.
(ii) The business's technical infrastructure, hardware, and software security capabilities.
(ii) The costs of security measures.
(iv) The probability and criticality of potential risks to the data.

In the next two sections, these concepts are discussed in the context of two real-world situations applicable to almost every type and size of business. The first discusses how to better integrate information security into vendor and business partner relationships. That is, when a vendor of a business will have access to or possession of a business's most sensitive information, what that business should do to ensure that information will be protected. The second focuses on controlling risk in implementing a Bring Your Own Device (BYOD) programme for a business's employees.

Addressing Information Security in Business Partner and Vendor Relationships

6.0

Almost every week, there is an instance in which a business has entrusted its most sensitive information to a vendor or business partner only to see that information compromised because the vendor failed to implement appropriate information security safeguards. Worse yet, those same businesses are frequently found to have performed little or no due diligence regarding their vendors and have failed to adequately address information security in their vendor contracts, in many cases leaving the business with no remedy for the substantial harm they have suffered as a result of a compromise.

In the current regulatory environment, businesses must be far more rigorous in entering into vendor relationships where sensitive information will be placed at risk. In this Section, three tools are described that businesses can immediately put to use to substantially reduce the information security threats posed by their vendors and business partners, ensure proper due diligence is conducted and documented, and provide remedies in the event of a compromise.

Those tools are:

- **Vendor Due Diligence Questionnaire**
- **Key Contractual Protections**
- the use in appropriate circumstances of an **Information Security Requirements Exhibit**.

Whenever a vendor or business partner has access to a business' network, facilities, or data, one or more of these tools should be used.

By using these tools, businesses can achieve the level of CIA with regard to their data, demonstrate they acted reasonably/appropriately in addressing risk, and scaling their approach to reflect the level of that risk (e.g., requiring stronger contractual protections and deeper due diligence when the vendor has possession of substantial amounts of highly sensitive data versus requiring less strict protections and diligence when the vendor has only incidental contact with sensitive data.

This ad hoc approach to due diligence is no longer appropriate or reasonable in the context of today's business and regulatory environment.

Due Diligence: The First Tool

While most businesses conduct some form of due diligence before entrusting vendors with their sensitive information or access to their systems, the due diligence is often done informally, in a non-uniform manner, and not clearly documented. In very few instances is the outcome of that due diligence actually incorporated into the parties' contract. This ad hoc approach to due diligence is no longer appropriate or reasonable in the context of today's business and regulatory environment.

To ensure proper documentation and uniformity of the due diligence process, businesses should develop a standard 'Due Diligence Questionnaire' that each prospective vendor or business partner with access to confidential or sensitive business data or personal information must complete. Areas covered by the questionnaire include: corporate responsibility, insurance coverage, financial condition, personnel practices, information security policies, physical security, logical security, disaster recovery and business continuity, and other relevant areas.

Use of a standardised questionnaire has a number of significant benefits:

- It provides a uniform, ready-made framework for due diligence
- It ensures a 'like-for-like' comparison of vendor responses
- It ensures all key areas of diligence are addressed and none are overlooked
- It provides an easy means of incorporating the due diligence information directly into the contract. The completed questionnaire is generally attached as an exhibit to the final contract.

From the outset, vendors must be on notice that the information they provide as part of the due diligence process and, in particular, in response to the Vendor Due Diligence Questionnaire will be (i) relied upon in making a vendor selection; and (ii) incorporated into and made a part of the final contract. To be most effective, the questionnaire should be presented to potential vendors at the earliest possible stage in the relationship. It should be included as part of all relevant RFPs or, if no RFP is issued, as a stand-alone document during preliminary discussions with the vendor.

Key areas for the Vendor Due Diligence Questionnaire include the following:

- **Vendor's financial condition.** Is the vendor a private or public company? Are copies of the most recent financial statements available? Financial condition may not appear to be a critical factor for information security purposes, but the possibility a vendor may file bankruptcy or simply cease to do business while in possession of a business's most sensitive information presents a substantial risk. In such instances, it may be difficult, if not impossible, to retrieve the data and ensure it has been properly cleansed from the vendor's systems. Similarly, the ability to sue a bad vendor for damages will be thwarted if the vendor does not have the financial ability to pay for damages awarded.
- **Insurance coverage.** What types of coverage does the vendor have? What are the coverage limits and other terms? Is the coverage claims made or occurrence based? As commercial general liability policies typically do not cover information security breaches, consider requiring the vendor to have cyber-risk or network security insurance. These types of policies are becoming more common.
- **Corporate responsibility.** Are there any criminal convictions, or recent material litigation, instances in which the vendor has had a substantial compromise of security, privacy violations, adverse audit results, etc.?

- **Subcontracting.** Will the vendor require the use of any subcontractors or affiliates in the performance of its services? Will the vendor use subcontractors or affiliates outside of their country? Where are the subcontractors and affiliates located? What types of services will they provide? What information, if any, belonging to the business will be sent to these entities?
- **Organisational security procedures.** Does the vendor have a comprehensive and well-documented information security programme? What are the vendor's information handling policies? Does the vendor have a dedicated information security team? Is there an incident response team? What are the vendor's information security practices with contractors and agents (e.g., due diligence, requiring non-disclosure agreements, specific contractual obligations relating to information security, etc.)?
- **Physical Security; Logical Controls.** What physical security measures and procedures does the vendor employ? Does the vendor use system access control on its systems to limit information access to only the personnel who are specifically authorised?
- **Software Development Controls.** If the vendor is a software developer, what are its development and maintenance procedures? What security controls are used during the development lifecycle? Does the vendor conduct security testing of its software? Does the vendor maintain separate environments for testing and production? Does the vendor licence code from third parties for incorporation into its products? If so, what types of code?
- **Privacy Issues.** If personal information of customers, consumers or other individuals is at risk, does the vendor have a privacy policy? What is the revision history of the policy? Are there any instances where the vendor has had to contact consumers regarding a breach of security? Does the vendor conduct specific training for its employees regarding handling of personal information? If so, how often? If data is to be collected from individuals, has the vendor complied with applicable law in obtaining all relevant consents and permissions? This is particularly important when mobile devices and apps are involved (see the European Union Article 29 Data Protection Working Party issued Opinion 02/2013 On Apps On Smart Devices). Also, businesses must ensure they understand every use the vendor will make of data collected using the apps. This is not always clear. Many vendors include in their contracts vague and largely undefined rights to use the data they collect. The Article 29 Working Party has specifically stated that transparency and knowing consent from consumers is a key risk: "The key data protection risks to end users are the lack of transparency and awareness of the types of processing an app may undertake combined with a lack of meaningful consent from end users before that processing takes place. (Opinion 02/2013 On Apps On Smart Devices)."
- **Disaster Recovery and Business Continuity.** What are the vendor's business continuity/ disaster recovery plans? When was their last test? When was their last audit? Were there any adverse findings in the audit? Have deficiencies been corrected? What is the revision history of their plan? What security procedures are followed at the recovery site?

Key Contractual Protections: The Second Tool

In the overwhelming majority of engagements, the contract entered into between a business and its vendors has little or no specific language relating to information security. At most, there is a passing reference to undefined security requirements and a basic confidentiality clause. Today's best industry practices (e.g., CERT and ISO) and information security laws and regulations suggest far more specific language is required in vendor relationships. The following protections should be considered for inclusion in relevant vendor contracts:

Confidentiality. A fully-fleshed out confidentiality clause should be the cornerstone for information security protections in every agreement. The confidentiality clause should be broadly drafted to include all information the business desires to be held in confidence. Specific examples of protected information should be included (e.g., source code, marketing plans, new product information, trade secrets, financial information, personal information, etc.). While the term of confidentiality protection may be fixed for, say, five years -- ongoing, perpetual protection should be expressly provided for personal information and trade secrets of the business. Requirements that the business mark relevant information as 'confidential' or 'proprietary' should be avoided. These types of requirements are unrealistic in the context of most vendor relationships. The parties frequently neglect to comply with these requirements, resulting in proprietary, confidential information being placed at risk.

Warranties. In addition to any standard warranties relating to how the services are to be performed and authority to enter into the agreement, the following specific warranties relating to information security should be considered:

- A warranty requiring the vendor to comply with 'best industry practices relating to information security'.
- Compliance with all applicable information security, privacy, consumer protection, and other similar laws and regulations.
- Compliance with the business's privacy policy in handling and using personal information. If the vendor is responsible for collecting personal information, it should warrant it has obtained all necessary consents and permissions to ensure compliance with applicable law.
- If personal information is to be collected through mobile devices and apps, the vendor should warrant it will use that data solely in connection with the performance of the agreement. Be mindful of requests by vendors to use the data they collect for other purposes, including potential resale of that data. If those rights are to be granted, very clear contractual language should be added requiring the data to be 'anonymised' such that it is incapable of being identified to any individual or entity. Anonymisation should also comply with any applicable laws and regulations. Finally, the vendor should be required to fully indemnify the business against any liability arising from the vendor's failure to properly anonymise the data.
- A warranty against making the business's confidential information available to offshore subcontractors or affiliates, unless specifically authorized to do so by the business in writing.
- A warranty stating that the vendor's responses to the Vendor Due Diligence Questionnaire, which should be attached as an exhibit to the contract, are true and correct, will be updated upon the business's reasonable request, and will remain true and correct through the term of the parties' agreement.

General Security Obligations. Consider including generalised language in the contract relating to the vendor's obligations to take all reasonable measures to secure and defend its systems and facilities from unauthorised access or intrusion, to periodically test its systems and facilities for vulnerabilities, to immediately report all breaches or potential breaches of security to the business, to participate in joint security audits, and cooperate with the business's regulators in reviewing the vendor's information security practices, etc.

The vendor should protect the business from lawsuits and other claims that result from the vendor's failure to adequately secure its systems.

Indemnity. In situations where a breach of the vendor's security may expose the business to potential claims by third parties (e.g., a breach of personal information may result in claims by the business's customers), the agreement should include an indemnity provision requiring the vendor to hold the business harmless from claims, damages, and expenses incurred by the business resulting from a breach of the vendor's security. That is, the vendor should protect the business from lawsuits and other claims that result from the vendor's failure to adequately secure its systems.

Limitation of Liability. Most agreements have some form of 'limitation of liability' – a provision designed to limit the type and extent of damages the contracting parties may be exposed to. It is not uncommon to see these provisions disclaim the vendor's liability for all consequential damages (e.g., lost profits, harm to the business' reputation, etc.) and limit all other liability to some fraction of the fees paid. These types of provisions are almost impossible to remove from most agreements, but it is possible to require the vendor to exclude from the limitations or, at least, provide for heightened liability for damages following on from the vendor's breach of confidentiality and their indemnity obligation for claims the vendor, itself, causes because of its failure to adequately secure its systems. Without those exclusions, the contractual protections described above would be essentially illusory. If the vendor has no real liability for breach of confidentiality because the 'limitation of liability' limits the damages the vendor must pay to a negligible amount, the confidentiality provision is rendered meaningless.

Information Security Requirements Exhibit: The Third Tool

The final tool in minimising vendor information security risks is the use of an exhibit or statement of work to specifically define the security requirements relevant for a particular transaction. For example, the information security requirements exhibit may prohibit the vendor from transmitting the business's information over internal wireless networks (e.g., 802.11a/b/g) or from transferring that information to removable media that could be easily misplaced or lost. The exhibit may also contain specific requirements for use of encryption and decommissioning hardware and storage media on which the business's information was stored to ensure the information is properly scrubbed from the hardware and media. Other specific physical and logical security measures should be identified as relevant to the particular transaction.

Given the volume of potential data arising from use of mobile devices and related apps, particular attention should be given to specifying the security measures to be followed in collecting, storing, processing, and transmitting data in the mobile context. In particular, the security risks arising from interaction of apps should not be neglected. The Article 29 Working Party has pointed out that "[a] high risk to data protection comes from the degree of fragmentation between the many players in the app development landscape." They have also highlighted that "[t]he close interaction with the operating system allows apps to access significantly more data than a traditional internet browser. Apps are able to collect large quantities of data from the device (location data, data stored on the device by the user and data from the different sensors) and process these in order to provide new and innovative services to the end user." In developing security standards for mobile app development and use, these issues should not be overlooked.

Businesses are presented with unique risks when they entrust their proprietary and confidential information to their vendors, business partners, and other third parties. Those risks can be minimised by employing the tools discussed above: appropriate and uniform due diligence, use of specific contractual protections relating to information security, and, potential, use of exhibits or other attachments to the agreement detailing unique security requirements to be imposed on the vendor.

Bring Your Own Device (BYOD) Programmes

7.0

“

As the company size increases, so does the concern over BYOD security risks. 28% of very small businesses believe it presents an increased threat, rising to 47% and 49% for medium-sized businesses and large enterprises respectively.[4]

BYOD refers to corporate programmes that authorise employees to utilise their own personal device (e.g., smartphone, tablet computer, laptop, netbook) for both personal and work-related activities. The employee is also generally permitted to use their personal device to connect with their employer's corporate network.

There are a number of key benefits of BYOD programmes: potential overall decrease in the business's cost of keeping and maintaining information technology resources, better enabling mobile workers, supporting the new 24/7 work environment at many companies, and increasing collaboration, and employee morale. A recent study by Unisys highlights some of the benefits:

- 71% of respondents believe BYOD will increase morale
- 60% believe it will increase productivity
- 44% would find a job offer more attractive if the company provides support for iPads

The risk of BYOD programmes is inherent in their nature: allowing corporate and personal data to be stored/accessed on the same device – a device where the company has little or no control. This risk is shown in the results of two recent studies:

- **Dell KACE Study:** 87% of companies unable to effectively protect corporate data and intellectual property because of employees who use some kind of personal device for work -- including laptops, smartphones, and tablet computers.
- **eWeek Study:** 62% of IT administrators feel they don't have the tools to properly manage personal devices.

By focusing on the common threads for compliance discussed above, this risk can be mitigated.

Key Risks Presented by BYOD Programmes

In deciding to implement a BYOD programme, a business should consider the following key risks and ensure the benefit to the organisation in costs savings, employee morale, etc.; outweighs those risks.

Mixing Business and Personal Data. This issue is clearly one of the most important. At present there are solutions, for example Kaspersky's mobile product, to help 'containerise' personal and business data on a BYOD device. But there are few that separate security policy enforcement (i.e., in the event the device is lost or stolen, a remote wipe/erasure initiated by the company would not only delete all business information, but also all personal information). Businesses and their employees must be sensitive to these issues.

4 Kaspersky Lab – Global IT Risks Report 2014

Some examples, drawn from real-world situations, of what can go wrong:

- **The Wedding Photos:** In one case, an employee's smartphone was thought lost. The business performed a remote wipe of all data on the phone to ensure sensitive information wasn't compromised. It turned out the phone wasn't, in fact, lost, but merely misplaced. The employee's spouse made a claim against the company alleging they had deleted the only copy of their most prized family photos. Putting aside the fact that the employee and his spouse should have backed up these important photos, the company was put in a difficult position because it did not have any protection against a claim by the spouse for deleting the photos. See the discussion, below, about 'friends and family'.
- **The Next Great Novel:** In another case, an employer permitted employees to use their own laptops. While the employer was installing some new security software on each of the laptops, a particular employee claimed his employer had caused a data loss that included the only copy of the novel the employee had been working for several years. The employer failed to have an appropriate policy in place that would have protected against employee claims of this nature. The company ended up settling with the employee.
- **It's in the Cloud:** Online backup services are becoming commonplace. Many work with and some are directly incorporated into smartphone operating systems. In several recent cases, employees have used these 'Bring Your Own Cloud' services to back-up their personal data while also, inadvertently, backing up sensitive business data (i.e., business data was copied to third party servers over which the business had no control or, even, knowledge, with the third parties potentially using subpar security safeguards).

Software Licencing Issues. Businesses must be sensitive to ensuring third party software used by the employee in connection with their BYOD devices is properly licenced: an employee cannot licence a 'home' version of a word-processing programme and then use that programme on a daily basis on their BYOD laptop to perform work for their employer. Doing so would almost certainly violate the third party licence agreement for the software. As another example, the BYOD device may use a virtual private network (VPN) connection to access certain third party software installed on the employer's systems (e.g., an accounting application, CRM software, order-entry software, etc.). The relevant third party licence agreements should be reviewed in every instance to ensure the scope of the licence permits such remote access.
In some instances, additional licence fees may be required.

An employee must assess not only the benefit of using their own device, but also what they will be giving up.

Discovery/Litigation. In considering whether to participate in their employer's BYOD programme, an employee must assess not only the benefit of using their own device, but also what they will be giving up. Specifically, the employee must understand that the employer and, potentially, others may need to inspect the device and review its contents in the context of litigation. That information may include a review of email, photos, geo-location data, etc. In addition, the employee must understand that under certain circumstances the employer may have good cause to remotely wipe the contents of the device. Unless the employee has backed-up the device, the wipe could result in the complete loss of the employee's personal data. These are important factors – which should be carefully considered before agreeing to participate in a BYOD programme.

Repetitive Stress And Other Workplace Injuries. 'Blackberry thumbs' and other conditions that may result from repetitive stress using laptops, smartphones, tablet computers, and other similar devices must be taken into account in drafting an effective BYOD policy. For example, participants in the programme should be urged to review the ergonomics information provided with most devices, acknowledge the employer is not responsible for injuries incurred in using these devices, etc. The business should also review its worker's compensation and other insurance to confirm coverage extends to these types of injuries resulting from non-company provided devices.

Shared Use Of Devices With Non-Employees: The Friends and Family Problem. In almost every instance, employees will permit friends and family members to use their BYOD devices. Those 'friendly' third parties will have potential access to any and all business related information stored on the device. This cannot be avoided. Worse yet, the risk cannot be readily mitigated with current technology.

The problem is that the business will have no non-disclosure or other confidentiality obligations with these third parties, nor will the third party have signed the business's policy regarding use of the BYOD device. This means the business has no contractual protections with the third party.

If, for example, the third party sends and receives personal email using the device and the device must later be reviewed by the company in the context of litigation, the company may be violating the third party's privacy rights in reviewing, even accidentally, their email. Similarly, if the company has good cause to remotely wipe the device, the employee may have no claim against the company because the employee signed a policy acknowledging this possibility, but the friends and family have signed no such policy. In that case, if the wipe destroys valuable information of the third party, they could, conceivably, make a claim against the business for damages.

Employee Disposal of Device. Procedures should be put in place to ensure the employer has an opportunity to confirm removal of all sensitive business data from a device before it is disposed of. Businesses must be aware that employees are always looking toward the next new smartphone, tablet, or laptop and that their existing device may be traded-in, sold on eBay, or otherwise disposed of with little or no notice to the employer. Review of the device may be particularly difficult in situations where the employment relationship has ended badly. The employee may refuse to produce the device for review. In those cases, the employer may be left with no alternative other than to perform a remote wipe of the device.

Key Elements of BYOD Strategy

To address the three common threads of compliance discussed above (CIA, reasonableness/appropriateness, and scaling), an effective BYOD programme should have three components: policy, training, and technology/enforcement.

Policy. The governing document for any BYOD programme is a clear, understandable policy. The policy details the employee's rights and obligations with regard to the programme, including putting the employee on notice that by participating in the programme he or she will be giving up certain rights. For example the contents of their mobile device, including personal data, may be reviewed in the event of litigation as part of the discovery process or personal data on a device might be irretrievably lost if a remote erasure/wipe of the device is made to protect corporate information in the event the device is lost or otherwise compromised.

Most businesses distribute the policy and require employee sign off before the employee is permitted to participate in the programme. The policy must make clear that participation in the programme may be revoked by the company at any time. For example, the company may decide to discontinue the programme or it may determine that a particular employee's use of the device presents too great a security risk. In those instances, the business must have the unfettered right to terminate the programme or a particular employee's participation in the programme.

Many organisations send out follow-up memos from time-to-time highlighting particular points in the policy. For example, an employer might send a memo describing the particular risks or prohibitions against allowing corporate data to be backed-up to an employee's own online backup accounts (e.g., DropBox, iCloud, etc.).

Training. Employee training is another critical component of an effective BYOD programme. It is generally not enough to simply provide employees with a policy they may or may not read. Rather, it is a preferred practice to conduct one or more training sessions for employees to specifically educate them on their rights and obligations arising from participation in the programme. Depending on the sensitivity of information the employee may have access to, this training may be repeated on a periodic basis.

Technology/Enforcement. The final component is the use of technology and other means to enforce the policy. This can be as simple as requiring employees to use only BYOD devices that have the capability of remote security policy enforcement (e.g., required passwords, timeout, remote wipe, etc.). Other, more advanced, technologies are also becoming available including the inherent ability to separate personal and business data.

As was shown in the discussion of the three common compliance threads, the investment a business must make in addressing these components depends on the type of information that will be placed at risk by the BYOD programme.

Conclusions

8.0

While the number and complexity of privacy and information security laws and regulations is ever increasing, businesses should appreciate certain common threads that run through them. In this whitepaper, three of the most common and most important threads are presented. By understanding that current law does not require perfection, but only due care, reasonableness, and scaling measures to reflect the sensitivity of the data being placed at risk, businesses can go a long way to achieving compliance.

As reflected in the discussion of information security in vendor relationships and the development of an effective BYOD programme, businesses can see how these common threads can be applied to real-world situations. The thoughtful use of training, policies, and technology can greatly diminish overall compliance risk.

About the author
Michael R. Overly is a partner in the Information Technology and Outsourcing Group in the Los Angeles office of Foley & Lardner LLP. Mr Overly writes and speaks frequently regarding negotiating and drafting technology transactions and the legal issues of technology in the workplace, email, and electronic evidence. He has written numerous articles and books on these subjects and is a frequent commentator in the national press (e.g., the New York Times, Chicago Tribune, Los Angeles Times, Wall Street Journal, ABCNEWS.com, CNN, and MSNBC). In addition to conducting training seminars in the United States, Norway, Japan, and Malaysia, Mr Overly has testified before the U.S. Congress regarding online issues. Among others, he is the author of A Guide to IT Contracting: Checklists, Tools and Techniques (CRC Press 2012), e-policy: How to Develop Computer, E-mail, and Internet Guidelines to Protect Your Company and Its Assets (AMACOM 1998), Overly on Electronic Evidence (West Publishing 2002), The Open Source Handbook (Pike & Fischer 2003), Document Retention in The Electronic Workplace (Pike & Fischer 2001), and Licensing Line-by-Line (Aspatore Press 2004).

Kaspersky Endpoint Security for Business

Kaspersky delivers a comprehensive security platform to help protect your business — whether you are looking to manage, protect and control all your endpoints (physical, mobile and virtual), secure your servers and gateways, or remotely manage your entire security environment.

Kaspersky Endpoint Security for Business boasts a comprehensive list of technologies from anti-malware, endpoint controls, encryption, mobile device management (MDM), to systems management including patch management and licence inventories. And as more and more businesses are realising the benefits of rolling out a Bring Your Own Device (BYOD) initiative, which lets employees use their personal mobile devices for business activities, you can enable BYOD through both mobile security and MDM.

Kaspersky products are designed so that the administrator can view and manage the entire security landscape from one 'single pane of glass'. They all work together seamlessly, supported by the cloud-based Kaspersky Security Network, to deliver world-class protection businesses need to combat evermore sophisticated and diverse cyber threats.

Built from the ground up, Kaspersky makes it easy for IT administrators to see, control and protect their world. Kaspersky's security modules, tools and administration console are developed in-house. The result is stability, integrated policies, useful reporting and intuitive tools.

Kaspersky Endpoint Security for Business is the industry's only true integrated security platform.

GET STARTED NOW: FREE 30 DAY TRIAL

Discover how our premium security can protect your business from malware and cybercrime with a no-obligation trial.

Register today to download full product versions and evaluate how successfully they protect your IT infrastructure, endpoints and confidential business data.

GET YOUR FREE TRIAL NOW

JOIN THE CONVERSATION

#securebiz

Watch us on YouTube

View us on Slideshare

Like us on Facebook

Review our blog

Follow us on Twitter

Join us on LinkedIn

Learn more at kaspersky.com/business

ABOUT KASPERSKY LAB

Kaspersky Lab is the world's largest privately held vendor of endpoint protection solutions. The company is ranked among the world's top four vendors of security solutions for endpoint users*. Throughout its more than 17-year history Kaspersky Lab has remained an innovator in IT security and provides effective digital security solutions for large enterprises, SMBs and consumers. Kaspersky Lab, with its holding company registered in the United Kingdom, currently operates in almost 200 countries and territories across the globe, providing protection for over 300 million users worldwide. Learn more at www.kaspersky.com.

* The company was rated fourth in the IDC rating Worldwide Endpoint Security Revenue by Vendor, 2012. The rating was published in the IDC report "Worldwide Endpoint Security 2013–2017 Forecast and 2012 Vendor Shares (IDC #242618, August 2013). The report ranked software vendors according to earnings from sales of endpoint security solutions in 2012.