Information Security and Privacy – What Business Leaders Need To Know

By Libby Benet, JD, CIPP US
Principal Benet Consulting
https://www.linkedin.com/in/libbybenet/
January 9, 2019

The time to ask questions is before an event occurs. Do you know what questions to ask?

It is tempting for management to feel that they have properly safeguarded their systems and data because they invest in the security of their information through the IT department. If that is your company's main tactic for to securing information assets, that feeling of security is misplaced. Management has the responsibility to understand that there is more involved in managing the informational assets of the company than firewalls, anti-virus software, complex passwords and encryption. Business Continuity Plans (BCPs), Incident Response Plans (IRPs), privacy protections and the underlying business model should also be evaluated.

There is often a lack of understanding among business leaders today as to the legal and ethical responsibilities they have for securing and maintaining the privacy of employee, customer and partner information. While the IT team plays a key role in keeping a business secure, relying on the IT department alone is not the best answer.

To state the obvious, businesses have a lot of information. That information can be in paper or electronic form. Electronic information can be stored in internal systems, like databases or email, or the information can be in computer or mobile phone applications connected to the web. Examples of these information assets are employee records, customer records, intellectual property, financial records and business plans.

Some information is *personal information* such as names, addresses, social security numbers or drivers licenses. Some information is *sensitive personal information* such as medical or financial records. A company may store *confidential information* such as business plans or intellectual property. There may be information added to existing information for the purpose of marketing and sales that transforms information about an individual in a way that changes the duties a business has to the individual. There are different duties imposed upon a company based on the type of information that is held, collected, used, processed, shared and destroyed. Do you know what those duties are and how your business is actually handling that information?

Businesses have a duty to secure their information assets from damage, loss, modification or unauthorized access in whatever forms the information exists, whether paper or electronic. For some types of information, like employee health information, there is a duty of privacy as well. Therefore, both information security and privacy ought to be included as part of a company's risk management plan.

Information security and *privacy* are related concepts but are not the same thing. These concepts may overlap and may involve the same people but the focus is different.

The objective of information security is to ensure information's confidentiality, integrity, availability and accountability. The focus of information security is to reduce the potential for damage, loss, modification or unauthorized access to systems, facilities or data. Information security includes the technical and physical controls of IT systems, building security, remote users, vendors, third parties and the creation and maintenance of business continuity and disaster recovery plans. Those in your business that might have information security roles include the Chief Security Officer (CSO), the Chief Risk Officer (CRO), the Chief Compliance Officer (CCO), the Head of HR or Legal department, Chief Information Officer (CIO), Head of physical security, Head of Marketing or various other representatives from the company. Small businesses may not include these specific roles but the issues managed by those roles need to be evaluated.

The objective of privacy protections is to ensure an individual receives the following considerations with regard to their protected data: notice, choice and consent and the option to correct misinformation. Privacy protections adhere to the people who give a business their personal information. These protections are concerned with the individual's ability to control the use of that information.

There are state and federal statutes, regulations and common law bases for these privacy protections. For example, federal statute requires a business to maintain the privacy of medical records under the Health Insurance Portability and Accountability Act (HIPAA). There is a duty under the Federal Trade Commission Act and most state laws to avoid "unfair and deceptive trade practices" which can be applied to a company's use of information in its business. There are also four generally accepted common law rights of privacy: intrusion upon seclusion, appropriation of name or likeness, publicity given to private life, and publicity placing a person in false light.

Generally, a US business should take into account the following from a privacy perspective:

Medical Privacy (ex., medical records)
Financial Privacy (ex., using credit reports in hiring)
Marketing Privacy (ex., faxes and digital marketing)
Workplace privacy (ex., such as drug and alcohol testing or employee background checks)
Online Privacy (ex., technologies, privacy notices, collection & use of electronic data, breach notification)
Codes of Conduct (ex., Payment Card Industry Data Security Standard or professional ethical rules)

If that is not enough, there are over 100 countries with some type of privacy protections. The implementation of the European General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) (passed in 2018, to be implemented in 2020) may affect the privacy obligations of certain businesses. For companies subject to the law, the GDPR imposes a number of requirements including notice to "data subjects" (individuals), the individual's right to access their information, to be forgotten, to object, to correct, and to data portability. For companies subject to the CCPA, companies are required to provide notice to "data subjects" (individuals), the individual's right to access data the information, to be forgotten, to data portability, to opt out of sale of information, and to receive services on equal terms. These obligations shift the onus to the business to be more careful with the data it has on an individual rather than being on the individual to protect him or herself.

Given the rollout of the GDPR, the passing of the CCPA major data breaches in 2018 and the further revelations about Facebook's handling of its users' information has given rise to renewed calls for a federal US privacy law.

Why is this discussion important?

Internally, businesses often focus on information security, generally and cyber security, specifically. As mentioned above, this focus is important but it is does not address the whole picture. If the model for the businesses is to use the internet to collect as much information as possible and use what is collected to make sales and direct advertising, the discussion of privacy is even more important.

Senior management relies on technology investments to protect their company but do they consider the repercussions if those technologies fail? Further, technology is not much help if, for instance, an employee sees sensitive information in documents at a copier they are not authorized to view. Additionally, do employees understand the need to protect information from exposure?

Senior Managers need to be aware of the privacy obligations the company has to its employees, customers, partners, and regulators. Has the business looked at whether the business practices take privacy obligations into consideration? For example in 2018 there were several FTC investigations over allegations that companies falsely claimed they were in the process of certifying compliance under the EU-U.S. Privacy Shield framework. This framework ensures companies transferring data from EU countries to the US are complying with the GDPR. In a product case a mobile phone manufacturer allowed a third-party service provider "to collect detailed personal information about consumers, such as text message contents and real-time location information, without their knowledge or consent despite promises by the company that it would keep such information secure and private." (FTC Press Release April 30, 2018). A service company marketing themselves as a talent agency failed to protect the privacy of children under 13. In the company's privacy policy it said it did not knowingly collect personal information on children under 13 and that those accounts needed to be created by a legal guardian "yet the site did not place any restrictions on users who indicated they were under age 13 and did not take steps to verify whether a profile was being created by a legal guardian." These examples illustrate the various ways that businesses misused customers' information or had statements that contradicted their duties to secure the privacy of that information.

When the systems, processes or people management has in place fail, the business is vulnerable to a number of losses including business interruption, contingent business interruption if a partner has a network security issue, reputation damage, and third party litigation for mishandling the information. Talk to anyone who has had to handle a breach, whether electronic or paper, and they can tell the toll it takes on staff and the losses they sustained.

What other questions should you ask?

The answer varies by business segment, size of business and available resources. At the very least, senior leadership must ensure the business knows what privacy laws they are subject to, What type of information is covered by the law and whether the business is in compliance with the law. Other considerations include the following:

Does the company have a data governance strategy to protect information?
Does the company have a privacy team established?
Has the company done a Data Protection Impact Assessment (DPIA)?
Has the company done a Privacy Impact Assessment (PIA)?
Does the company have an incident response plan?
Has the company trained its employees about the importance of data security and privacy?
Does the company have any policies and procedures with regard to data security and privacy?
Does the company have a privacy notice online?
Are the business practices actually aligned with the privacy notice?

There are a number of resources to help a business assess the gaps in their information security and privacy obligations. There are experts (lawyers, accountants, privacy professionals, IT consultants) and software solutions (see Advisen's Cyber Guide 2018). Once there is a good understanding of the gaps, leadership should determine whether to assume the risk of financial loss or transfer it by way of insurance.

If you don't believe these problems can happen to your company consider the following scenario:

An employee clicks on a phishing email which launches malware on to the company's network. The data on the company's network is locked and encrypted by the malware and the hackers make an extortion demand in exchange for the encryption key to unlock the information. Meanwhile, the system is not available to your employees, customers and partners. The fact that the system is unavailable means many things. To begin with, there is a loss of income and employee productivity while the systems are being restored. There is usually a need for forensic experts to come in and evaluate what happened and for privacy counsel to be engaged to determine whether the incident is a breach that triggers notification to effected individuals. There is the loss if the ransom is paid. Hackers may require that ransom be paid in bitcoin, which may be difficult for a company to procure. There is the strain on the company's team to deal with the event. There is a public relations and reputation loss if news of the breach reaches the public. If there was no backup of the data or the data was compromised, there is a cost to restore the data. If the company is publicly traded there may be a hit to the stock price. This company may also be located in a state that requires regulators be notified when a breach occurs. The state regulator sets up an investigation into the event, tying up employee time and exposing the company to fines and penalties.

Do you have the money and the expertise to handle this event?

How Does Insurance Respond To These Issues?

Businesses, in conjunction with their insurance agents/brokers, must consider cyber liability and data breach insurance as part of their risk management strategy. When evaluating insurance coverage, companies need to evaluate whether there is adequate coverage in the event of damage, loss, modification or unauthorized access of information AND whether there is coverage in the event of a breach of privacy. The industry has addressed many of these issues in standalone cyber coverage and cyber endorsements.

Common first party insurance includes coverage for business interruption loss, contingent business interruption from a partner's business interruption, cyber extortion costs, data restoration costs, reputational harm, and breach response costs. Common third party coverage includes insurance for regulatory fines and penalties, liability arising from a breach of information security and privacy and liability arising from practices associated with a company's website. In addition to the first and third party coverage, the market is also responding to losses arising out of criminal activity such as fraudulent instruction and social engineering.

Business owners and management have many things to worry about. There is a storm brewing over how businesses handle data. Ask the right questions and don't be caught off guard.