KnowBe4
Human error. Conquered.

WHITEPAPER

Improving Legal Compliance Through Security Awareness Training

Improving Legal Compliance Through Security Awareness Training

By
Michael R. Overly, Esq., CISA, CISSP, CIPP, ISSMP, CRISC*

KnowBe4

whitepaper

Introduction

Complying with the ever-growing morass of data privacy, security laws and regulations can be a daunting task for any organization. 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. Reconciling all of these legal obligations can be, at best, a full time job and, at worst, the subject of fines, penalties, and lawsuits. Liability can range into the millions of dollars.

The threat from outside hackers is substantial, spear phishing and Advanced Persistent Threats are increasing with double digits every year. Moreover, according to the FBI, the incidence of "insider" misappropriation or compromise of confidential information has never been higher. By better addressing information security with their personnel, including through appropriate awareness training, businesses can mitigate both these threats.

This white paper seeks to provide a "big picture" understanding of legal and regulatory compliance obligations and then to apply that understanding to the specific issue of mitigating the security threat posed by an organization's own employees which are the weak link in IT security.

Finding Common Threads in Compliance Laws and Regulations

The sheer number and variety of privacy and security laws and regulations can be daunting, if not overwhelming. In some instances, it may be almost impossible for even a large, sophisticated organization to identify all applicable laws, reconcile inconsistencies, and then implement a compliance program. 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, organizations can more easily understand their baseline compliance obligations.

In reviewing the many laws and regulations applicable to privacy and data security, three common threads can be seen. 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 organizations like CERT at Carnegie Mellon and the International Standards Organization ("ISO"). Embracing these common threads in designing and implementing an information security program will greatly increase a business' ability to achieve overall compliance with the laws, regulations, and other requirements (e.g., PCI DSS, industry standards, etc.) applicable to it.

PCI Security Standards Council™
PARTICIPATING ORGANIZATION

Confidentiality, Integrity, and Availability ("CIA"). Anyone involved in information security should be familiar with the acronym "CIA," which stands for Confidentiality, Integrity, and Availability. For data to be truly secure, each of these three elements must be satisfied. "Confidentiality" means the data is protected from unauthorized access and disclosure.

"Integrity" means the data can be relied upon as accurate and that it has not been subject to unauthorized 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.

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.

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 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, as discussed in the next paragraph, 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 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. 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, the level of effort and expenditure by the business to address that risk must increase. To better understand this concept, the following are excerpts from two laws that incorporate "scaling":

First Example from the Massachusetts Data Security Law: 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 program; (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 from the HIPAA Security Rule: Security efforts should take into account:

(i) The size, complexity, and capabilities of the business.
(ii) The business' 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 section, these concepts are discussed in the context of mitigating the threat of employees being the weak link in IT security through the implementation of appropriate training.

KnowBe4

whitepaper

Applying the Common Threads to Personnel Training

Security awareness training for employees is one of the most effective means of reducing the potential for costly errors in handling sensitive information and protecting company information systems. Training can be conducted through a number of means and certain approaches are more effective than others:

- **The Do-Nothing Approach:** The organization conducts no security awareness training and relies on automated systems to protect against phishing and malware.
- **The Breakroom Approach**: Employees are gathered during lunches or meetings and are told what to look out for in emails, web surfing, etc.
- **The Monthly Security Video Approach:** Employees are shown short videos that explain how to keep the organization safe and secure.
- **The Phishing Test Approach:** Certain employees are pre-selected and sent simulated phishing attacks, IT determines whether they fell prey to the attack, and those employees get remedial training.
- **The Human Firewall Approach:** Everyone in the organization is tested, the percentage of employees who are prone to phishing attacks is determined, and then everyone is trained on major attack vectors. Simulated phishing attacks are sent to all employees on a regular basis.

Awareness training can ensure personnel have a solid understanding of their employer's security practices and policies. In contrast, an uninformed employee is susceptible to malware, phishing attacks, and other forms of social engineering. They can do substantial harm to an organization's systems and place its data at risk.

In a CyberSecurity Watch Survey, conducted jointly by the U.S. Secret Service, the CERT Insider Threat Center, CSO Magazine, and Deloitte, found that where the perpetrator of an electronic crime could be identified, 21% were committed by insiders. The survey also revealed that 46% of the respondents thought that damage caused by insider attacks was more severe than damage from outsider attacks. To satisfy the requirements of the Payment Card Industry Data Security Standard (the "PCI DSS"), businesses must conduct security awareness training on hire and at least annually thereafter. The security awareness program must provide "multiple methods of communicating awareness and educating employees (can include: posters, letters, memos, web based training, meetings, promotions and simulated phishing attacks)."

Key aspects of any awareness training program should include the following:

- Train on an ongoing basis. Avoid limiting training to when an employee is first hired or assigned to a new role in the organization.
- Train creatively, not just in a non-interactive class-room setting.
- Look for means to introduce interactivity into the training process.
- Have a means of measuring progress.

The three common threads discussed in Section 2 can be readily applied to security awareness training:

CIA: Training can be used to ensure every employee has an appreciation for the basics of information security, including the concepts of Confidentiality, Integrity, and Availability of sensitive data. In particular, employees must be trained to understand that their actions, even if unintentional, can severely compromise these foundational requirements of information security. Examples of how employees fall victim to malware, phishing, and other forms of social engineering should be emphasized. In fact, the Federal Financial Institutions Examination Council ("FFIEC") has recommended that financial institutions ensure training "address social engineering and the policies and procedures that protect against social engineering attacks."

Acting Reasonably/Taking Appropriate Measures: While security experts may differ in their approach to addressing various security issues, all would be in agreement that a key element of any reasonable and appropriate security program is security awareness training. From standards organizations like ISO and CERT to industry standards like the PCI DSS to governmental entities like the FFIEC, it is clear that implementing a security awareness program is both reasonable and appropriate. Put another way, the failure to have such a program would likely be unreasonable and inappropriate given the risks involved.

Scaling Security Measures to Reflect Severity of Threat: The final "common thread" running through security and privacy laws is to ensure the measures used to address a particular threat are properly scaled. Several factors must be balanced: the likelihood and severity of the threat, the practicality of the measure, and the costs of implementing the measure. Looking at the first factor, the insider threat, as discussed above, is substantial. The likelihood of occurrence is high. The second factor relates to practicality of the measure. Awareness training is well understood and defined. There is nothing so profoundly novel about training that it would be considered impracticable. The final factor is cost. As noted above, training can be conducted using a number of approaches (e.g., classroom, posters, e-mail, and technology). Cost should, generally, not be a significant factor. This is particularly so with some technology solutions. In fact, technology solutions can satisfy a number of key criteria for effective training: training progress can be documented and measured, the solutions can be interactive (increasing the probability the employee will actually learn and retain the lessons), they can be creative, and, in many cases, can be easily implemented in a cost effective manner through reinforcement of the training using email or simulated phishing attacks.

Conclusion

Identifying and understanding the wide range of information security and privacy laws and regulations can be a complex task. There are, however, certain common concepts or "threads" that run through most of these laws and regulations. Gaining an appreciation of those common threads can provide businesses with a far better big-picture understanding of their compliance obligations and to apply that understanding to achieving better overall protection for their organizations. In this white paper, we have applied the common threads to mitigate the threat of both insiders and attacks coming from the outside by focusing on security awareness training.

---

* 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, e-mail, 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 Ling-by-Line (Aspatore Press 2004).

Disclaimer: Laws change frequently and rapidly. They are also subject to differing interpretations. It is up to the reader to review the current state of the law with a qualified attorney and other professionals before relying on it. Neither the author nor the publisher make any guarantees or warranties regarding the outcome of the uses to which this white paper is put. This white paper is provided with the understanding that the author and publisher are not engaged in rendering legal or professional services to the reader.

Additional Resources

Free Phishing Security Test
Find out what percentage of your users are Phish-prone.

Free Email Exposure Check
Find out which of your users emails are exposed before the bad guys do.

Free Domain Spoof Test
Find out if hackers can spoof an email adress of your own domain.

Free Phish Alert Button
Your emloyees now have a safe way to report phishing attacks with one click!

Ransomware Simulator
Find out how vulnerable your network is against ransomware attacks.

Ransomware Hostage Rescue Manual
Get the most complete Ransomware Manual packed with actionable info that you need to have to prevent infections, and what to do when you are hit with ransomware.

To learn more about our additional resources, please visit www.KnowBe4.com/resources

About KnowBe4

KnowBe4 is the world's most popular integrated Security Awareness Training and Simulated Phishing platform. Realizing that the human element of security was being seriously neglected, KnowBe4 was created to help organizations manage the problem of social engineering through a comprehensive new-school awareness training approach.

This method integrates baseline testing using real-world mock attacks, engaging interactive training, continuous assessment through simulated phishing, and vishing attacks and enterprise-strength reporting, to build a more resilient organization with security top of mind.

Thousands of organizations use KnowBe4's platform across all industries, including highly regulated fields such as finance, healthcare, energy, government and insurance to mobilized their end users as a first line of defense.

For more information, please visit www.KnowBe4.com

KnowBe4
Human error. Conquered.

KnowBe4, Inc. | 33 N Garden Ave, Suite 1200, Clearwater, FL 33755 | Tel: 855-KNOWBE4 (566-9234) | www.KnowBe4.com | Email: Sales@KnowBe4.com