Security Standards (Part 1)

BY DANE ASHWORTH AND VICTOR COPELAND

*Dane Ashworth has been with TimeShareWare for 20 years and currently serves as director of consulting, while also overseeing TimeShareWare's ASP operations. Dane specializes in solving business problems with technology and is a member of ARDA's Technology Committee (email: **dane@timeshareware.com**). Victor P. Copeland is an attorney with Ballard Spahr LLP, whose national practice includes representing branded resort, hospitality, and timeshare companies in all aspects of their business. Copeland serves on ARDA's Meetings and Technology Committees, and his e-mail is **CopelandV@ballardspahr.com**.*

This article is part one in a multi-part series. Part one introduces the concept of security standards, why they are important and how to determine which standards should apply to your business. Follow-up articles will dig deeper into specific security standards relevant to the vacation ownership industry.

Types of Security Standards

Security standards typically fall into three basic categories:

1. **Legal**. These are standards set forth in statutes, regulations and other laws enforced by governments. Some regulatory standards have specific data security requirements. For example, the Sarbanes-Oxley Act (SOX) is a federal statute that applies to how public companies protect financial data. Similarly, the GLBA Safeguards Rule issued by the Federal Trade Commission (FTC) is an administrative regulation which applies to businesses engaged in interstate commerce that provide financial services and requires development of an information security plan. Other regulatory standards come from consumer protection laws that do not include specific data security requirements but instead prohibit unfair, deceptive, and abusive acts and practices. However, regulators like the FTC have applied these more general laws in enforcement actions related to an organization's data security practices.

2. **Contractual**. These are standards adopted and enforced by private organizations such as industry groups, rather than by governments. Examples include the Payment Card Industry Data Security Standard (PCI DSS), which applies to merchants and other entities involved in payment card processing by contractual agreement for any business that accepts credit card payments.

3. **Best Practices.** These are data security practices which are used to *implement and comply with* more general regulatory and contractual security standards. Data encryption in transit is an example of a best practice security standard. While a business might not be specifically required by regulation or by contract to encrypt data in transit, doing so is a generally accepted best practice. Complying with regulatory and contractual security standards often requires adherence to many different best practice security standards.

Importance of Standards

Security standards are important because they provide a "roadmap" for how to protect data and a "measuring stick" to evaluate the effectiveness of data security controls. At its most basic, a "standard" is a level of quality or attainment. Adherence to the security standards described above helps demonstrate a specific level of quality in the areas of privacy and data security. These standards also provide generally accepted level of performance.

As such, compliance with security standards reduces the chances of a security breach. Failing to comply with security standards creates exposure for your organization in many different ways, including potential law enforcement actions by the FTC and state attorneys general to enforce regulatory standards, penalties and indemnification obligations under contracts with third parties, and class actions by consumers.

Determining Applicable Security Standards

Determining which security standards apply begins with an evaluation of how your organization conducts business and an audit of potential security risks. Companies processing credit cards, performing transactions over the Internet, developing software, or utilizing cloud hosting providers will need to consider several security standards. Conducting business in certain states or countries, or having a distributed operation across locations with remote workers, may subject your organization to still other security standards. Each of these scenarios requires different security standards to be applied in order to maintain compliance and reduce risk.

A good starting point to learn more about security standards and their application can be found from major vendors in the areas described above. In addition, the U.S. Department of Commerce's National Institute of Standards and Technology (NIST) has a section dedicated to cybersecurity, including a comprehensive Cybersecurity Framework, which can be thought of as a collection of best practices for organizations of all sizes and types to manage cybersecurity-related risk.

Helpful information is also available directly from regulators and bodies that maintain security standards. For example, the FTC has free resources available online to help businesses of any size meet their legal obligations with respect to data security. Similarly, resources about contractual standards are made available through the self-regulating bodies which manage these standards, such as the PCI Security Standards Council's *PCI DSS Quick Reference Guide* available on its website.

Applying Security Standards

Applying security standards requires a right-sizing approach where the standards are tailored to your organization — including its size and complexity, the nature and scope of its activities, and the sensitivity of the personal information it handles. Best practices with specific, measurable, and verifiable requirements are the most straightforward to implement.

In contrast, security standards with general requirements that are open to interpretation can be more difficult to implement. In that instance, consideration of the level of risk and exposure, along with the reasonableness of the interpretation, can help right-size the implementation of the security standard for your particular organization. When making this evaluation, your organization should also consider the Return-on-Investment (ROI) to weigh the relative costs of compliance, both in terms of financial costs and operational impacts, against the likelihood and severity of the risks.

Sometimes these decisions are easy, and other times they can be "close calls" that are complex and difficult. Do not hesitate to have your Chief Information Officer coordinate with outside technology consultants and legal counsel to navigate these issues. Focusing on these matters early—before they become an issue—can save time, money, and headaches further down the road.

Validating Compliance with Security Standards

Once implemented, security standards should be audited or certified. Implementation of general best practice security standards can be internally audited and confirmed for compliance.

In some cases, these standards may be audited as part of a broader and more formal audit or certification if done for SOX, PCI, or other security standards. Specific standards such as PCI may have obligations for a level of certification necessary based on several factors such as company size, number of transactions, or other similar factors. Some organizations may be able to self-attest compliance levels, while others may need to hire a Qualified Security Assessor (QSA) for a formal report and certification.

Regardless of the certification or audit levels applicable to your organization, consideration should be given to hiring an independent third party. Receiving validation from an independent third party is another way your organization can demonstrate compliance and reduce risk.

Conclusion

Security standards—legal and contractual standards as well as best practices—are central to your organization's privacy and data security operations. They are both a "shield" for how to protect sensitive personal information, and a "sword" that can be used against your organization if it fails to do so. Understanding which standards apply to your organization is the critical first step.

Thoughtful and right-sized implementation of these standards, coupled with regular audits and certification, will position your organization to meet its legal and contractual obligations without breaking the bank or hindering operations. ■

This article is the first of many editorial contributions from the members of the ARDA Technology Committee, which is chaired by Suzzi Albrycht Morrison. The goal is to create a collection of "Technology Bytes," different types of content aimed for audiences at various professional levels. This collection will be both on-line and print items, as well as Webinars, conference sessions, etc.

Look for more from this team in 2018!