solarwinds

eBOOK

Compliance Is Not Enough: Planning a Complete Security Strategy

single point of contact

Table of Contents

Introduction

Following the guidelines established by compliance frameworks like PCI DSS, HIPAA, SOX, FISMA, and GLBA may make some SysAdmins and other IT professionals think they have a handle on security.

In reality, however, following compliance policies is not the same as being truly secure. While compliance rules can help you lay the foundation for keeping software environments as secure as possible, compliance is only a starting point for solid IT security.

To become secure, you need to not only ensure that your team understands and enforces compliance rules, but also that your systems and environments are secured with a suite of tools and best practices that harden your organization against attacks across the board.

This eBook discusses the relationship between compliance and security. It starts by outlining why compliance is important and offers tips for enforcing it in real-world settings. It then explains what compliance has to do with security, and the additional steps that organizations should take (beyond merely meeting compliance requirements) in order to provide for a well-rounded security approach.

Today's Cybersecurity Threatscape

You don't need to be a security engineer to know that we are living in an age of never-ending cyberattacks and data breaches. Reports of major cyberattacks against companies across the full spectrum of industries are now a routine part of the mainstream news cycle, and the frequency of such attacks is rising.

And so is the cost of cyberattacks. In fact, according to Forbes®, the financial consequences of cybercrime will total two trillion dollars by 2019.

Why are cyberattacks increasing in frequency and fallout, despite the huge amount of money that organizations now invest in IT security? There are several reasons:

- **The primary goal of attackers has become financial gain.** Many cyberattacks were once executed for the simple purpose of disrupting operations. However, more and more cyber-criminals are launching attacks for financial gain rather than out of pure malice.
- **New industries have become prime targets.** Certain industries, like financial services, have long been the target of cyberattacks. However, other industries have now been added to that list. For example, attackers are now heavily targeting the healthcare industry. The black market cost of healthcare data is high because it can be used for identity theft and insurance fraud. Plus, healthcare data can be used over a long period. Unlike stolen credit card data, which usually stops being useful as soon as an attack is detected and a compromised card is decommissioned, healthcare data can be exploited for years after a breach.
- **Companies continue to use outdated infrastructure and systems.** The amount of data organizations need to store is increasing—in many cases, at a rate that exceeds their ability to acquire new infrastructure. As a result, sensitive data is being consigned to outdated environments that are often more susceptible to attacks.
- **American companies are prime targets.** A large portion of ransomware attacks (disabling systems or data and demanding payment from victims in order to restore access) that occur in the United States originate from foreign countries. Cyberattackers abroad target the United States because of the high value of the American dollar, making Americans at higher risk for these attacks.

The threats outlined on this list are a reminder that high-frequency and high-stakes cyberattacks are not going to go away anytime soon. 2016 was a brutal year for cyberattacks, and 2017 has already seen its share of attacks. However, don't be fooled into thinking that the worst is over. Cyberthreats continue to loom large across a range of industries, even for organizations that take compliance seriously.

Compliance Policies

In order to understand why compliance alone is not enough to defend against cyberattacks, you have to understand the goals of compliance.

The major compliance frameworks that affect businesses in the United States today include:

- **Payment Card Industry Data Security Standard (PCI DSS)** – A regulatory framework that governs credit card transactions and the management of cardholder data
- **Health Insurance Portability and Accountability Act (HIPAA)** – Rules that affect how organizations create, store, transmit, or otherwise interact with protected health information
- **Sarbanes-Oxley Act (SOX)** – A framework created after the ENRON and WorldCom scandals to help establish corporate accounting policies for publicly traded companies on the New York Stock Exchange, with additional measures to protect sensitive financial information
- **Gramm-Leach-Bliley Act (GLBA)** – A set of rules that establishes controls for the way financial institutions handle personal information

The list above represents the top compliance frameworks that impact businesses in the United States, but this is not an exhaustive list. Depending on your organization's industry and types of operations, you may be subject to additional compliance requirements, too.

While the specific requirements of compliance policies vary from framework to framework, an underlying objective of IT security in compliance policies relates to what is known as the CIA Triad. In this case, "CIA" stands for:

- **Confidentiality.** This means keeping data private and available only to authorized users.
- **Integrity.** To be compliant, data needs to be consistently protected at all stages of the data management cycle, from the time the data is generated, through the analytics process, and up to its deletion, when the data retention period ends.
- **Availability.** Data must always be available to the parties that need to access it and have authorization to do so. Highly available data is more difficult to secure than data that is locked away, but if data is not available, it may as well not exist.

The CIA Triad, which is used by the National Institute of Standards and Technology (NIST), serves as a reference framework for specific compliance regimes like HIPAA and PCI DSS. The Triad applies to company data (meaning information about the operations of an organization), as well as to user data (data about a company's users or customers). In order to be effective, compliance policies must apply not only to data on devices inside a company, but also on devices employees take outside the company. This also includes data that is transferred over any type of network.

Security and Compliance Best Practices

To adhere to the CIA Triad, organizations should adopt best practices within the following realms.

SECURITY

Keep documentation secure

Documentation contains secrets that attackers could use to gain unauthorized access to systems or data. You don't want to give away security secrets by providing attackers easy access to your documentation. So, be sure to protect documentation as much as data. Only legitimate parties should have access to your documentation.

Secure log data

Even if logs don't always contain protected or sensitive data, they are a crucial source of information that can aid in an attack. Securing log data is therefore vital.

Don't neglect physical security

To enforce compliance policies, physical access to hardware and data needs to be restricted just as much as digital access.

DILIGENCE

Report and document everything your organization does

Documentation is key for implementing compliance best practices and demonstrating a commitment to compliance.

Keep retention policies in mind

Don't discard logs or other data too soon. Most compliance policies specify a minimum (and, in some cases, maximum) required retention time period during which data has to be maintained before it can be deleted.

Ensure that your business conducts security awareness training

Security awareness training involves training your employees and, if appropriate, your users, in security best practices. Such training not only helps to keep all parties informed about security best practices, but also demonstrates your company's commitment to compliance.

Validate and monitor your compliance controls

To gain an objective and accurate assessment of your compliance follow-through, ask independent parties to verify your compliance operations. Outside compliance validation and monitoring helps ensure that the compliance controls you establish are actually enforced. External validation is especially important because some compliance frameworks offer no official certification programs. As a result, it is up to organizations to ensure that they are following best practices.

COMPREHENSIVENESS

Don't rely on a single tool

No one tool or process can keep you compliant and secure. You need to develop a holistic set of compliance tools and processes tailored to your organization.

Don't treat compliance as a bare-minimum requirement

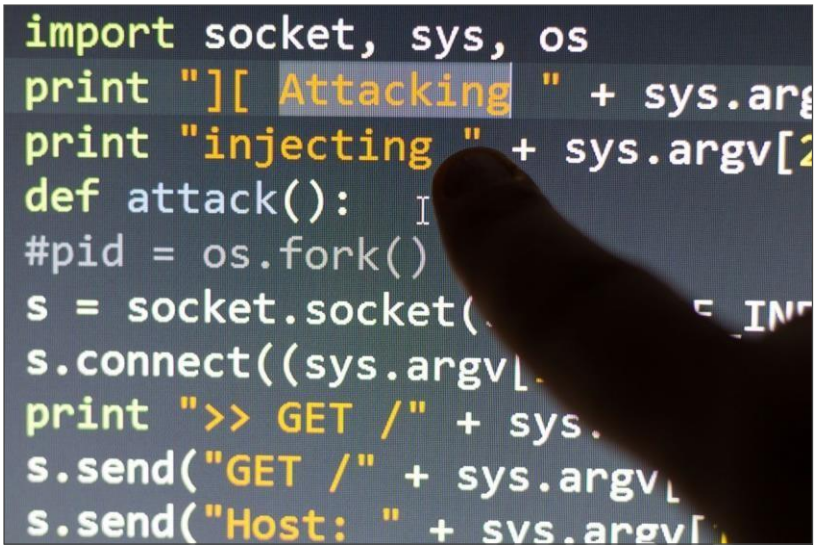
If you think of compliance as something that you do simply to satisfy auditors, you're thinking about it in the wrong way. Instead, use compliance requirements as an opportunity to build the right defenses to secure your data, systems, and network. After all, the costs of being non-compliant extend far beyond simply being reprimanded by auditors or paying fines or penalties.

Remember that compliance needs are always changing

Not only are compliance policies themselves occasionally updated, but your technology—the IT infrastructure that underpins your business or the devices you support—will also expand and evolve over time. You must therefore perform constant compliance checkups to ensure that you are following best practices. In other words, make a commitment to continuous compliance.

Make compliance the center of everything you do

The best way to enhance compliance is to place compliance at the forefront of your operations. Don't treat compliance as an afterthought. After all, you don't want to set up a rack of new servers without first thinking about compliance considerations, only later to discover that your new infrastructure is not compliant and needs to be reconfigured.



The Costs of Non-Compliance

Regulatory fines tend to be the first consequence that comes to mind when decision-makers think about failing to be compliant, but there are many more costs of non-compliance. Some examples include:

- **Fines.** Many are unaware of the true cost of regulatory fines, which can amount to millions of dollars.
- **Criminal penalties.** Individuals or organizations found responsible for willful compliance failures can be subject to criminal penalties that include not just fines, but jail time.
- **Data loss.** Data fuels your business, and losing it to theft or compromise can have huge consequences for your ability to continue operating.
- **Lawsuits.** Organizations that suffer compliance failures may face expensive lawsuits from groups or individuals affected.
- **Brand damage.** A company's name in the news for a compliance failure is never a good thing in the eyes of consumers. The damage to your company's reputation and brand can take years to overcome.
- **Loss of customer loyalty.** For the same reasons, customers may choose to stop supporting a company when they learn that it has failed to take compliance seriously.

The costs of non-compliance thus extend far beyond the direct regulatory fees. The fallout of compliance mistakes may last for years and cost many times more than regulatory fines alone.

A TOOLSET FOR IN-DEPTH DEFENSE

To defend against compliance violations, you need a set of tools that will not only aid your efforts to meet and exceed compliance regulations, but also help make your business more secure. You need in-depth defense.

This toolset should consist of the following types of products, which are explicitly cited in several compliance frameworks. Two examples are PCI DSS v3.2 requirement 6.2 and 10.6, which cite the need for patch management and the review of log data and security events on a continual basis. These products cover a wide array of threat vectors targeting your business and data:

- **SIEM solutions.** A Security Information and Event Management (SIEM) solution uses logs and other data sources to detect network anomalies that could indicate serious security threats. SIEM solutions allow security and other IT professionals to retroactively review log data to identify attack patterns and build rules to respond to these threats in real time, stopping them in their tracks. Primary among SIEM solution capabilities is the ability to produce compliance reports to substantiate the controls a business has in place to meet strict guidelines.
- **Patch management solutions.** Unpatched servers and workstations are increasingly targeted by attackers, so keeping the software that runs on these machines up to date is essential for minimizing security vulnerabilities. Patch management tools' ability to conduct network scans for out-of-date software make them ideal for running a tight ship when it comes to security, while also providing operational efficiencies for software application management purposes.
- **Network change and configuration management (NCCM) tools.** Networking devices, such as firewalls, form a frontline defense against intruders to a network, which can make these devices a target for attack. Tampering with config files or the opening of ports on such devices can be cause for concern. NCCM solutions help protect against these concerns and provide a safe means of comparing, updating, and backing up config files recovered from false moves, or avoiding them altogether.

- **Device management.** The ability to detect the location of devices, open and close ports, and manage network switches is crucial for detecting and reacting quickly to security threats that originate on particular devices. This can easily happen today, especially when users are accustomed to connecting and disconnecting their own devices from enterprise networks.
- **Secure file transfer.** Without the proper levels of encryption, or the proper underlying infrastructure to support data's safe passage from one individual or machine to another, machines become easy pickings for hackers. Using secure FTP protocols and ensuring that no data is stored in the DMZ is essential for avoiding issues and helping to ensure that data in transit remains safe.

Again, no one tool can provide complete security. If it could, breaches would likely not be as common as they are. Instead, organizations must develop a complete toolchain of security solutions that provide the foundation for both compliance and security.

Summary: Compliance ≠ Security

Compliance is a good starting point for security. However, being compliant does not automatically equate to being secure.

Compliance frameworks don't address every possible security gap or vulnerability that can exist within an organization. Full coverage would be impossible because threats and vulnerabilities adapt much more quickly than compliance policies can be updated. As a result, an organization may be perfectly compliant with regulatory requirements, yet still suffer a major cybersecurity breach.

That's why it is essential to go above and beyond basic compliance. Compliance certainly matters and should be taken seriously. However, organizations that are fully committed to keeping data secure, protecting their users and reputation, and avoiding the financial and operational pain of breaches must do more than simply meet compliance requirements. They must deploy an end-to-end lineup of security and compliance solutions that can harden every part of their infrastructure and software against attack.

The SolarWinds® Security Portfolio

SIEM: Log & Event Manager

A SIEM that makes it easy to use logs for security, compliance, and troubleshooting.

TRY IT FREE

Patch Manager

Intuitive patch management software for quickly addressing software vulnerabilities.

TRY IT FREE

Network Configuration Manager

Automated network configuration and compliance management.

TRY IT FREE

User Device Tracker

Locate users and devices on your network with User Device Tracker.

TRY IT FREE

Serv-U® Managed File Transfer Server

Enhance security and control over file transfers in and outside your organization.

TRY IT FREE

ABOUT THE AUTHORS

Destiny Bertucci, Head Geek, SolarWinds

Destiny is a Head Geek™ at SolarWinds, and a Cisco® Certified Network Associate (CCNA), CIW Masters, INFOSEC, MCITP SQL, and SolarWinds Certified Professional®. Her 15 years of network management experience spans healthcare and application engineering, including over nine years as SolarWinds Senior Application Engineer.

Jamie Hynds, Senior Product Manager, SolarWinds

Jamie draws on years of experience serving in a variety of roles, such as Sales Engineer for SolarWinds Core IT Products, and IT Auditor/Security Consultant for Deloitte®, among others. In each role, he has assisted businesses in the adoption of technologies to enhance security, meet regulatory IT compliance, and pass audits for a broad array of compliance frameworks.

Josh Berman, Product Marketing Manager

Josh leads the messaging and strategic marketing direction for over 10 products from the SolarWinds Security and Tools Portfolios. His introduction to the IT space came in the five years he spent working for an Austin-based colocation, managed hosting, and private cloud provider that assisted businesses in healthcare, financial services, education and other various industries with high security needs and sensitive data.

ADDITIONAL RESOURCES

Security Kung Fu Webcast Series

Master the art of Security Kung Fu and tune in to our webcast series to learn tips that will help you combat threats to your network. Choose from four sessions: SIEM Solutions, Firewall Logs, Active Directory® Changes, and Security vs. Compliance.

Having a plan of action is the first step in being compliant. Always having a 24/7 remote security team available gives you peace of mind knowing there is someone ready to respond to a network breach. Single Point of Contact provides various managed security services to small and large businesses. Being compliant means you have the best possible security protocols in place, and we want to help you get there and maintain those practices. Be sure to contact us to see how we can help in this area of your business.

single point of contact