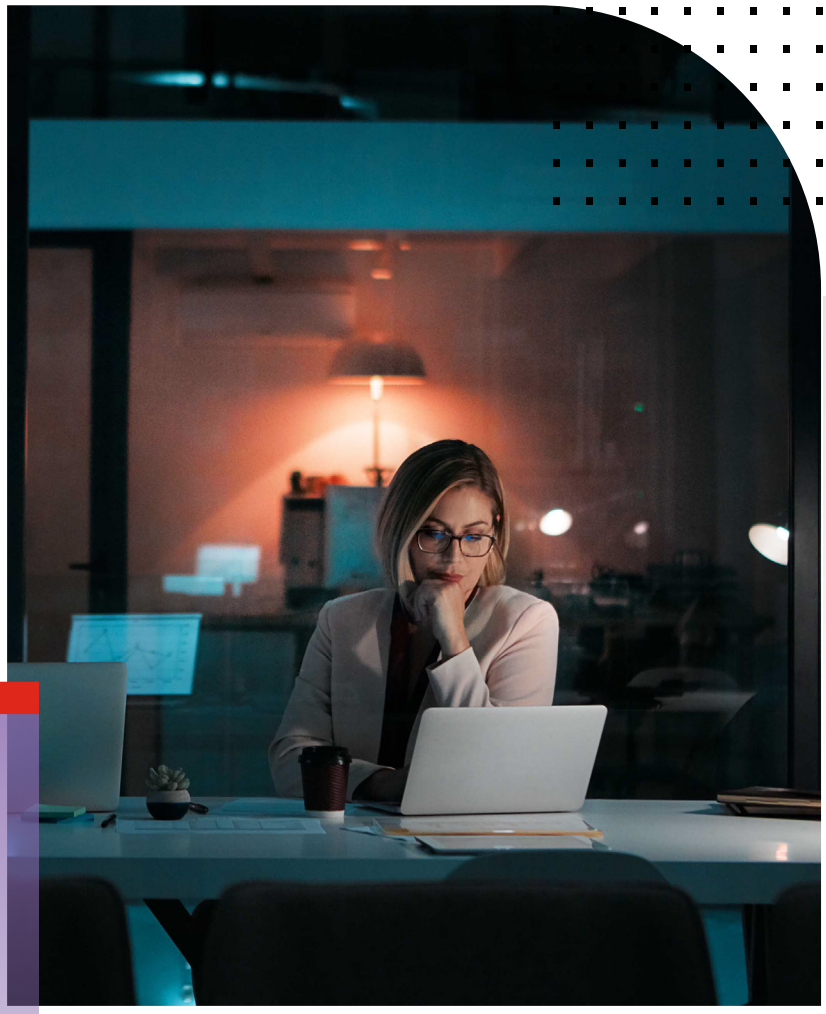
WHITE PAPER

Why Compliance Is a Critical Part of a Cybersecurity Strategy

Using Regulations and Standards To Develop a Proactive Risk Posture



Executive Summary

Compliance can seem like a time- and resource-absorbing headache. Go beyond the frustration, however, and compliance can reveal itself to be a critical security linchpin and business enabler. There certainly isn't disagreement that compliance is an effective means for enhancing protection and tracking and reporting on security measurements that matter. But compliance means different things, and it's difficult to know where to start and what to track. Getting the right security architecture in place is an important starting point. However, it extends beyond there to automating not only compliance tracking and reporting but also notifications of intrusions and/or breaches and their remediation.

Different Types of Compliance

Regulations come in a sea of acronyms. But they can be divided into three general types: Government regulations are often broadly applicable, industry regulations address industry-specific needs, and security standards give all organizations a framework for securing IT infrastructures and data.

There is a dramatic evolution and growth in regulations and security standards, placing increasing pressure on organizations to achieve and demonstrate ongoing compliance with them. For example, the European Union's General Data Protection Regulation (GDPR) creates new security pressures and the need to demonstrate compliance.

When it comes to security standards, the National Institute of Standards and Technology (NIST) standard is gaining rapid adoption for evaluating, tracking, and reporting security status. At the forefront is the adoption by U.S. federal agencies, which were directed to use it via a U.S. Executive Order in May 2017.[1] Private sector entities are following suit, with 30% indicating they were using it in 2015—a number predicted to rise to 50% by 2020.[2]

Why Compliance Matters

"If you think compliance is expensive, try noncompliance," says a former U.S. deputy attorney general.[3] Consequences can include fines, sanctions, loss of reputation, negative business outcomes, or a combination of the above. Consider the business case for compliance:

1. Avoid compliance/regulatory fines

Fines can be substantial. Compliance can reveal itself to be a critical security linchpin.

Government Regulations

European Union General Data Protection Regulation (GDPR) makes any organization that touches the personal data of EU residents accountable for protecting that data.

Sarbanes-Oxley Act (SOX) is intended to improve financial disclosures and prevent accounting fraud. Because financial reporting depends on secure technology, an SOX assessment is an opportunity to identify IT inefficiencies and revisit the breach response plan.

Regulation	Sample Fines	Highlights
GDPR	Launched in May 2018, no fines to date.	Potential fines of up to 20 million euros ($23.3 million) or 4% of world revenues, whichever is higher.
PCI DSS	$5,000 to $100,000 per month for noncompliance, levied by banks and credit card institutions.[4] Plus, $50 to $90 fine per cardholder record breached.[5]	One retailer that lost millions of records faced a potential multibillion-dollar PCI liability.
HIPAA	$49.1 million total, 2015–2017.[6]	29 companies received an average fine of $1.7 million.
FINRA	$332.5 million total, 2015–2017.[7]	10 biggest fines of 2017 averaged $7.7 million per company.

2. Protect brand reputation

Brand success depends on trust, and public trust in online security is already strained. A survey by PwC reveals that 69% of consumers believe companies are susceptible to cyberattacks, and 85% won't engage with a business if they have security concerns about it.[8] More than half (55%) of consumers in another survey indicate they had abandoned online purchases due to privacy concerns.[9]

The marketplace punishes companies that have experienced damaging breaches, long after the breach. A Deloitte study identifies 14 types of impact, including seven with hidden or less visible costs.[10] This latter group includes devaluation of trade names and lost value of customer relationships.

As the basis of its examination, the study examines a $60 billion U.S. health insurer that had 2.8 million protected health information (PHI) records breached when a laptop was stolen from a vendor. The incident's total impact was $1.7 billion, and nearly 75% of that amount resulted from lost contract revenue and lost value of customer relationships in the five years after the breach.

3. Enhance your security posture through compliance

Compliance also forces a fresh, end-to-end review of data governance, and an opportunity to reimagine the value that an organization's data can provide. A close consideration of data and how it is used can enable organizations to define their current risk and proactively ensure they have the right security processes and architecture in place to address those requirements.

Industry Regulations

Federal Information Security Modernization Act (FISMA) protects government information, operations, and assets.

Financial Industry Regulatory Authority (FINRA) protects investor data and market integrity through regulation of broker-dealers.

Health Insurance Portability and Accountability Act (HIPAA) protects patient information.

Payment Card Industry Data Security Standard (PCI DSS) protects credit card data.

In this case, achieving compliance means proactively strengthening your security posture, which is far less expensive than recovering from a breach, ransomware attack, or operational outage. But the reality is that most organizations struggle to demonstrate comprehensive compliance. For example, 56% of organizations say they cannot determine compliance for endpoint devices.[11]

Recommendations for Achieving Compliance

Security leaders seeking to use compliance strategically need to adhere to the following:

1. Engage executive staff and the board

The first step in successful compliance is to engage the executive staff and board of directors.[12] Findings from a recent survey include:

- 77% of respondents feel that boards of directors should put IT security under greater scrutiny.
- 77% of boards of directors demand to know what happened after a security event occurs, and 67% review or increase security budgets, but a post-incident investment is far less efficient.

Tips for engaging senior leadership include:

- Align compliance objectives with business strategy
- Communicate business risks regularly
- Test your incident response plan and have it include executive staff and the board of directors
- Walk through the incident response plan with executive staff and the board of directors
- Benchmark against present state and outside benchmarks—and revisit these periodically
- Look for cybersecurity solutions with automated tracking and reporting. This can facilitate reporting to leaders and help offset security skills shortages.

2. Focus on a positive security posture

Compliant doesn't mean secure: Some recent major data breaches occurred at organizations rated PCI compliant just weeks or months before the breach.[13] Rather, security is one of the primary goals of compliance, and certain security principles are proving especially valuable. The Ponemon Institute notes that the average organization can reduce the cost of a breach by $1.55 million by fully deploying security automation.[14]

Another global survey reveals that organizations that follow six cybersecurity principles had not suffered a damaging attack in the past two years, while organizations that had been less likely to follow the principles had experienced 16 damaging attacks in that period.[15] The six principles include:

1. Integrate systems to create a unified security architecture
2. Share threat intelligence across the organization
3. Ensure safeguards work on all parts of the network
4. Use built-in compliance controls
5. Have end-to-end security visibility
6. Have automated more than half of security practices

Combine and Conquer: The Principles of NOC-SOC Integration

When a breach attack occurs, an important part of cybersecurity compliance is having the ability to track and quickly mitigate it, plus report on the details. A key step in being able to do this more efficiently is to consolidate a view of operations and security by integrating the functions of the network operations center (NOC) and security operations center (SOC). A NOC and SOC can be found in many large organizations.

This integration can be done without forklift upgrades or organizational restructuring. Solutions exist that can align the work of NOC and SOC teams in a way that can enable attack detection, response, and recovery in minutes rather than days or weeks. This is particularly important considering that 68% of breaches aren't discovered for months.[16] The alignment of NOC and SOC teams also harnesses the cross-team skill sets, improving resource usage. And the solutions that align NOC and SOC can enhance proof of compliance, providing for repeatable tests based on security best practices that result in a cumulative, companywide security rating score.[17] This enables security leaders to assess their current risk posture against their organization's risk tolerance/appetite in real time, and institute measures—often using automation—that bring security-related issues back into compliance.

Security Standards

National Institute of Standards and Technology (NIST)

Cybersecurity Framework contains standards, guidelines, and best practices to help organizations review their cybersecurity and prioritize what should be improved.

Another important set of cybersecurity standards has a more global following:

ISO/IEC 27001 was developed by the International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) and serves as a management framework to enable organizations to identify, analyze, and address information risks.

ISO/IEC 62443 is a series of standards that provide a flexible framework to address and mitigate security vulnerabilities in industrial automation and control systems (IACs).

For those who are interested, deeper comparisons of NIST and ISO 27001 are available.[18,19]

Automate Critical Reporting and Notification

As risk management becomes a critical business issue for organizations, security leaders must track and report cybersecurity measurements that align with the organizational objectives. These reports aren't simply for the security organization but for the executive suite and even boards of directors.

Manual aggregation and interpretation of compliance indicators across disparate security systems incur significant time that security organizations simply cannot expend. Even if a security leader has an infinite resource budget, it is almost impossible to recruit and retain all of the cybersecurity talent required in the face of an acute cybersecurity skills shortage.[20] Here, automated tracking and reporting of compliance with industry and governmental regulations and security standards free a security team to focus on strategic initiatives rather than tactics. It also enables security leaders to proactively manage compliance, which most assuredly improves an organization's risk posture.

But the value of automation of reporting and notifications extends beyond enabling a security team to stretch limited resources. It also helps ensure regulatory compliance. Take GDPR as an example. In the event that critical assets and data are breached, security organizations must send a notification within 72 hours or face substantial fines, in addition to the potential brand impact. With the right controls in place and the ability to shrink intrusion-to-detection windows, organizations can automate breach notifications and even automate the remediation process. In addition to minimizing the impact of a breach, this also helps ensure compliance with the 72-hour notice stipulation.[21]

The Real Goals of Compliance

Compliance is not an end-all solution when it comes to cybersecurity. But regulations and standards provide valuable indicators as to what security factors should be measured—namely, those that are important. In the case of security standards such as NIST, organizations can codify security benchmarks and best practices and then measure their risk posture against those—proactively making improvements in areas needing remediation.

Achieving compliance is extremely difficult for a security organization lacking a cohesive architectural approach due to the acquisition of point security products that are not integrated. A critical starting point for a successful compliance strategy is the development of a security fabric that encompasses the entire attack surface while integrating all of the security elements. It also means that certain security processes are automated, eliminating time-consuming manual tasks and speeding detection, prevention, and remediation activities. These automated functions need to include compliance tracking, reporting, and notifications. Compliance that lacks these attributes becomes reactive, heightening the risk posture of an organization.

[1] Presidential Executive Order, "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure," Whitehouse.gov, May 11, 2017.

[2] "Cybersecurity Framework," NIST.gov, accessed September 16, 2018.

[3] Doug Cornelius, "Compliance Week 2009," Compliance Building, June 4, 2009.

[4] Mike Mariano, "PCI Non Compliance Fines & Consequences," I.S. Partners, April 26, 2019.

[5] "Will You Be Penalized For PCI Non-Compliance?," Dynamic Edge, Inc., January 11, 2017.

[6] "HIPAA Fines Listed by Year," Compliancy Group, accessed September 17, 2018.

[7] "Biggest Finra penalties of 2017," InvestmentNews, accessed September 16, 2018.

[8] "Consumer Intelligence Series: Protect.me," PwC, accessed September 16, 2018.

[9] "Over half of consumers have decided against an online purchase due to privacy concerns: KPMG International," KPMG, December 7, 2016.

[10] "Beneath the surface of a cyberattack," Deloitte, accessed September 16, 2018.

[11] "The Cost of Insecure Endpoints," Ponemon Institute, June 2017.

[12] Patrice Perche, "Cybersecurity Needs to be Seen as a Strategic Issue, Not Just an IT Investment," Fortinet, October 9, 2017.

[13] Christian Moldes, "Compliant but not Secure: Why PCI-Certified Companies Are Being Breached," CSIAC.org, May 9, 2018.

[14] Larry Ponemon, "Calculating the Cost of a Data Breach in 2018, the Age of AI and the IoT," SecurityIntelligence, July 11, 2018.

[15] "Fortinet 2018 Security Implications of Digital Transformation Report," Fortinet, July 25, 2018.

[16] "2018 Data Breach Investigations Report," Verizon, March 2018.

[17] "Bridging the NOC-SOC Divide: Understanding the Key Architectural Requirements for Integration," Fortinet, August 23, 2018.

[18] Dejan Kosutic, "Which one to go with—Cybersecurity Framework or ISO 27001?" Advisera, February 24, 2014.

[19] "Which framework is right for my business? NIST Cybersecurity Framework vs ISO 27002 vs NIST 800-53 vs Secure Controls Framework," Compliance Forge, accessed May 20, 2021.

[20] Jon Oltsik, "Research suggests cybersecurity skills shortage is getting worse," CSO, January 11, 2018.

[21] "Fabric-Ready Partner Spotlight Q&A—CSPi," Fortinet, June 8, 2018.

May 22, 2021 8:09 AM

123456-0-0-EN