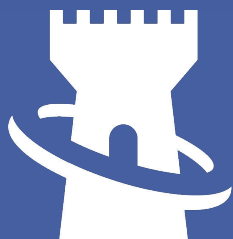


Beyond Compliance: Making Security a Business Strategy



SECURE HALO

SECURING THE ENTERPRISE

Are You Just Checking the Box?

Corporations of all sizes are awash in regulatory requirements, including a growing number related to data security and third-party cyber risk. The protection of consumer data, investor information and systems, and credit card transactions is not only of paramount importance to customers, and therefore regulators, but is critical to ensuring that the integrity of business infrastructure remains intact.

With continuously evolving attack vectors and pervasive breaches, regulatory and enforcement agencies have introduced increasingly stringent criteria. Regulators now look for evidence of a more robust approach to data security, including risk assessments, vulnerability management, improved policies and procedures, employee training, and incident response plans, as well as assessment and monitoring of third-party vendors connected to your business network.

Achieving compliance and bolstering cybersecurity are both priority issues for organizations, but they're not always executed in a coordinated way, or given the resources necessary to achieve both. "Check the Box" security is commonly utilized by organizations that choose to economize their security efforts by meeting only the minimums mandated by federal and state regulations. This is often the case at small- and mid-sized businesses, where budgets are lower and executives and board members may not have backgrounds in technology or online security.

Secure Halo™ regulatory and security experts encourage all businesses to aim higher, recognizing that compliance is merely a baseline. To move beyond checking the box, organizations must move from a compliance mindset to an enterprise risk approach.

REGULATIONS

- DFARS
- HIPAA
- Sarbanes-Oxley
- PCI-DSS
- FISMA
- GDPR

REGULATORS

- DoD
- OCR
- EU
- FFIEC
- SEC
- NY DFS



Does Compliance = Security?

While compliance is a necessity, it should not be the end goal because hackers know too well that a compliant organization is not necessarily a secure one.

Meeting just the minimum requirements will not protect organizations from a breach, which could have detrimental effects on reputation and generate escalating costs for incident response and litigation. A review of compliance and security shows how they differ:

Compliance

- Meets a baseline set of requirements or standards dictated by an external governing body
- Applies same requirements to all organizations, regardless of its size or of quantity and type of data in its possession
- Requirements are updated infrequently, and are therefore not responsive to changes in the threat landscape
- Represents controls in place at the time compliance is achieved

Security

- Is undertaken to protect customer data, maintain business reputation, and reduce risk
- Applies controls across people, technology, and processes in a customized and strategic fashion
- Responds to continuously evolving threats and, in a more mature cyber enterprise, gets ahead of threats with layered security, strong governance, educated leadership, and cultivation of a cybersecurity culture
- Is viewed as a strategic component of enterprise risk management, and is tied directly to business goals and outcomes

Both Compliance and Security are Necessary

A “Check the Box” approach provides a false sense of security because it reflects only a prescriptive set of security measures in place at the time of the evaluation and does not align those controls with the actual risks, vulnerabilities, and business needs of the organization. However, when considered in conjunction with strategic security, compliance requirements can provide a standardized framework around which to build a security program.

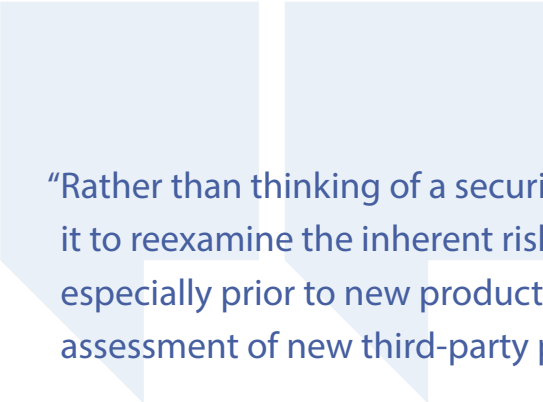
When Compliant Companies are Breached

Target was PCI-DSS compliant. A third-party breach cost the retail giant \$18.5 million.

Heartland Payment Systems Inc. was PCI-DSS compliant. A breach exposed 130 million credit and debit cards.

Neiman Marcus said its security measures exceeded PCI-DSS standards. A breach exposed 1.1 million payment cards.

A failure of compliance requirements, implementation, or evaluation?



“Rather than thinking of a security assessment as a once-a year checklist, use it to reexamine the inherent risk profile and maturity level of your enterprise, especially prior to new products, services, or initiatives. That should include assessment of new third-party providers or merger and acquisition efforts.”

– Nick Streaker, Vice President, Technology, Secure Halo™

What Are Regulators Looking For?

There are daily reports of hackers attacking the defenses of organizations both large and small, including looking for easy entry points such as untrained employees who are susceptible to social engineering, and third parties connected to a company's systems.

These known vulnerabilities have led federal regulators to require more stringent security controls both within organizations and among the vendors that provide core support. Regulators expect banks, for example, to establish risk tolerance, to conduct ongoing monitoring and independent reviews, and to have active board involvement throughout the vendor risk management process.

Regulation continues to evolve in the healthcare industry, where the Office for Civil Rights (OCR) HIPAA Security Rule established a minimum security standard for protecting electronic Protected Health Information (ePHI). The rule enforces administrative and physical safeguards, organizational standards, and appropriate policies and procedures

The Department of Defense (DoD) has recognized threats to its supply chain by requiring all government contractors (primes and subs) to comply with NIST 800-171 rules to protect Controlled Unclassified Information (CUI). Any contractor that wants to keep doing business with DoD must demonstrate compliance at a minimum.

What Are Steps to a 'Beyond Compliance' Approach?

All business leaders must consider the bottom line when making decisions about where to focus resources of time and money. While it's difficult to clearly measure return on investment when bolstering cybersecurity, in today's connected world, the management of cyber risk should not only be viewed as a means to achieve compliance, but be embraced as an integral part of business strategy. This may be a shift in mindset for boards and executives who have previously viewed cybersecurity as an issue to be handled by the IT or compliance department.

Shift to a Risk Management Approach

All organizations should include cyber risk within their enterprise-wide risk management program. The National Institute of Standards and Technology (NIST) describes the most sophisticated cybersecurity approach as an Integrated Risk Management program where, "the relationship between cybersecurity risk and organizational objectives is clearly understood and considered" and "senior executives monitor cybersecurity risk in the same context as financial risk and other organizational risks."

In its April 2018 update to the "Framework for Improving Critical Infrastructure Cybersecurity," NIST says that viewing cybersecurity as an enterprise risk enables a bank to decide how it will handle risk - mitigate, transfer, avoid, or accept - depending on its potential impact to the delivery of critical services. This then, allows executives to make informed business decisions about cybersecurity expenditures.

A proactive risk management style improves the way companies can avoid or manage existing and emergent risks, and provides the tools necessary to quickly adapt to a crisis. This model prepares a "before" and "after" calculation for plausible risk events by taking steps to:

- Assess the strengths and potential gaps of existing programs
- Model the impact of risk events
- Set up a strategic cybersecurity program to address risks
- Partner with an experienced and objective third party to assess and then execute a plan

Regulation



Risk



Reputation



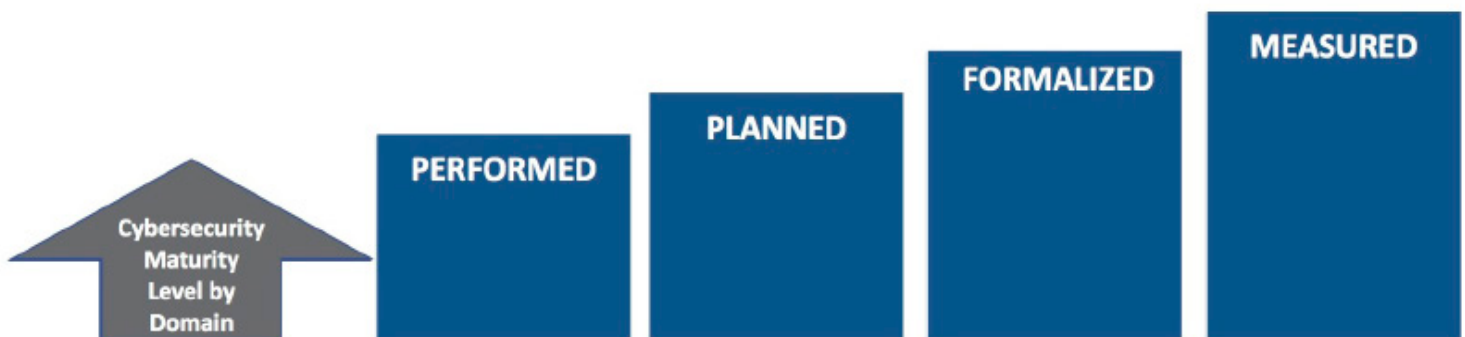
Create a Strategic Cybersecurity Program

Among the many goals that companies of all sizes consider on a daily basis are protecting consumer information, maintaining reputation and resilience, and meeting state and federal regulations to enable uninterrupted business operation. Though complex, the multiple regulatory guidelines serve a similar purpose: to foster effective practices that will protect the nation's financial infrastructure and individual privacy.

Achieving compliance is a business requirement but it can serve as a foundation to reach a more mature level of enterprise security. In its years providing enterprise security assessments and cybersecurity consulting to federal agencies and critical infrastructure, Secure Halo™ has found that those organizations that invest in complementary cybersecurity efforts that harmonize technology, processes, and people have better Cyber Risk Profile (CRP) scores and have more built-in resilience to confront a cyber attack or breach.

"When assessing the highly-regulated utility sector, we've noticed that the most mature organizations approach compliance with intent," says Jerry Bujno, Cyber Risk Assurance Advisor at Secure Halo™.

"The compliance requirements enable IT and risk managers to secure budget to create an information security program. Done correctly, this includes going beyond data security technology solutions to include cross-departmental input, and a focus on governance, insider threats, and third-party exposures."



For a better return on cybersecurity spending and to move beyond compliance, Secure Halo™ recommends the following steps as part of a strategic cybersecurity program:

Critical Asset Inventory: To know what to protect, you need to know what you have that is most important. This can be done through the simple act of defining and categorizing cyber assets based on their degree of sensitivity, their association to other critical assets, and understanding the value its loss could have on current and future earnings as well as reputation. Examples of assets include customer privacy information, IT hardware and software, people, intellectual assets and competitive processes, infrastructure, and outsourced services.

Cybersecurity Risk Assessment: Once you have an idea of what critical assets exist, an objective and holistic cybersecurity risk assessment should be performed in order to create a blueprint for a successful risk management plan. Such an assessment can identify trends, patterns, and areas of elevated risk to those assets across the holistic enterprise, as well as provide valuable insight into current strengths and weaknesses of existing controls and how they are postured relative to threat.

Development of Risk Management Plan: After a holistic cybersecurity risk assessment has been performed, (which should include review of risks such as insider threat, third party and supply chain, social engineering) a risk management plan founded on proactive and preventative security can be developed and executed.

A successful risk management plan will:

- Create prioritized security initiatives focusing on the implementation of improvements for top vulnerabilities identified.
- Ensure the proper investment and deployment of controls that are designed to prevent, detect, correct, and recover from digital threats.
- Understand that a sustained commitment to security and effective risk management will be predicated on security culture, which requires not just executive-level buy-in, but support from the greater organization so that policies and procedures are not just created but also enforced, and thereby matured.

Pay Attention to Third-Party Cyber Risks

Organizations and enterprises continue to grapple with growing demands to better manage cyber risks created by third-party vendors. The knowledge that hackers search for easy entry points such as third parties connected to operation systems, has led federal regulators to highlight the necessity for a strong vendor risk management system that includes monitoring, board involvement, and independent reviews.


According to Will Durkee, director of Security Solutions for Secure Halo™, solving the concept of third-party risk isn't a one-size-fits-all solution. Rather these solutions are driven by business relationships and regulatory forces, as each solution will be different based upon the industry or company itself. However, there are steps that every organization should take when working with third-party companies, which include:

- Assess the criticality of dependency on vendors, third parties, and business partners. Which are critical to your ability to do business and how much access do they have to your network and assets?
- Understand the specific risk/regulatory scenarios that might arise (GDPR, HIPAA, NY-DFS) specific to your sector.
- Do a baseline assessment on critical third parties and identify outliers whose security controls don't meet your own organization's standards.
- Decide whether to accept, mitigate or transfer discovered risks.
- Translate those decisions into contractual agreements with third parties.
- Follow up to ensure mitigation measures are being implemented.



LEADERSHIP QUESTIONS

WHAT EVERY CEO OR BOARD MEMBER
SHOULD ASK ABOUT CYBERSECURITY



Do my organization's policies go beyond compliance required by the regulatory bodies?

What parameters are in place to track third-party vendors?

Does the organization have a process for protecting our most valuable assets?

How often do leaders and key stakeholders meet to review important security concerns?

Is the Executive Board informed about the current level and business impact of cyber risks on the organization?

How often does my organization detect anomalies, and how effective are we at defending against those threats?

How comprehensive is the incident response plan?

How Secure Halo™ Can Help

Regulators recognize the burdens of regulatory compliance, but will take action when they deem that an organization has actively chosen not to comply with requirements or improve its security posture. Though business actions are often driven by compliance, achieving more mature security and the resilience it generates is a long-term investment in the business.

Secure Halo™'s decade of experience providing cybersecurity assessments and consulting to the U.S. government, critical infrastructure, Fortune 500 companies, and global underwriters puts it in a unique position to deliver mission-critical, economical solutions for community banks.

The Secure Halo™ security assessment offers a greater understanding of internal and external cyber risk by assessing security controls not just in IT, but across six domains: Data Security, Insider Threat, Internal Business Operations, External Business Operations, Mobility, and Physical Security. This provides a clear view of enterprise security posture.

Secure Halo™ provides an efficient, non-invasive, and cost-effective way to measure and align security controls used by third-party vendors or suppliers. Businesses can identify specific weaknesses, inform vendors, set contractual cybersecurity standards, and more efficiently meet compliance requirements.

Secure Halo™ assessments are mapped to NIST and international standards to improve cyber posture, mitigate vendor risk, and qualify for cyber insurance. The methodology behind the assessments has twice received Department of Homeland Security SAFETY Act designation.

Contact Will Durkee to learn more about how Secure Halo™ can help:

301-304-1700
wdurkee@securehalo.com