Risk and Compliance—For Better or Worse?

In today's business environment, many companies are required to comply with multiple industry and government mandates that govern IT security. Being in compliance does not equal being secure. So, what is the relationship among IT security, risk management and regulatory compliance? Can security be improved by shifting from a compliance-driven to risk-based approach?

MARKET DYNAMICS

Compliance with government standards and industry regulations is at the top of a lengthy list of IT security priorities. Unfortunately, the majority of organizations are still using a check-box mentality as part of a compliance-driven approach to security. This method achieves point-in-time compliance certification rather than an improvement of the company's security posture.

The Council of Europe Convention on Cybercrime; emerging legislation in the US, such as the National Institute of Standards and Technology (NIST)'s SP 800-137, the Federal Information Security Management Act (FISMA) of 2002, the Federal Risk and Authorization Management Program (FedRAMP), the Securities and Exchange Commission (SEC) Cyber Guidance, and the formerly proposed Cyber Security Act of 2012; and enforcement of existing regulations by the US Office of the Comptroller of the Currency Regulation Enforcement and the US Federal Trade Commission (FTC) case against the Wyndham Hotel Group are forcing organizations to rethink the check-box approach. The Wyndham Hotel Group believed that its audit reports would recuse it from having to implement appropriate security controls to protect its customers' data. To steer organizations away from using industry regulations or government regulations as an excuse to take shortcuts, more and more compliance mandates demand better risk management. A good example is the Payment Card Industry Data Security Standard (PCI DSS), which in its second revision introduced the concept of risk correlation associated with prioritization of remediation actions and evidence collection.

The bitter truth is that one can schedule an audit, but one cannot schedule a cyberattack. As a result, organizations have to find ways to streamline governance processes, continuously monitor compliance and their security posture, and correlate these activities to business criticality. By doing so, businesses can create a closed-loop process that encompasses the definition, evaluation, remediation and analysis of an organization’s risk posture on an ongoing basis.

SECURITY: THE HOLY GRAIL?

When it comes to determining an organization's security posture, it is a commonly held belief that performing vulnerability management will address any exploits and minimize the risk of a data breach. However, without putting vulnerabilities into the context of the risk associated with them, organizations often misalign their remediation resources. This is not only a waste of money, but more important, it creates a longer window of opportunity for hackers to exploit critical vulnerabilities. At the end of the day, the ultimate goal is to shorten the window attackers have to exploit a software flaw. Therefore, even vulnerability management needs to be supplemented by a holistic, risk-based approach to security, which considers factors such as threats, reachability, the organization's compliance posture and business impact.

Without a threat, the vulnerability cannot be exploited.

Another limitation is reachability—if the threat cannot reach the vulnerability, the associated risk is either reduced or eliminated.

In this context, an organization’s compliance posture plays an essential role, as compensating controls can be leveraged to prevent threats from reaching their target. According to the Verizon 2012 Data Breach Investigations Report, 97 percent of the 855 incidents reported in 2011 were avoidable through simple or intermediate controls. This illustrates the importance of compensating controls in the context of cybersecurity.
Another factor in determining the actual risk posed by a vulnerability is business impact. Vulnerabilities that threaten critical business assets represent a far higher risk than those that are associated with less-critical business assets.

Altogether, an organization’s focus should be on risk and not just security.

To gain insight into their risk posture, organizations must go beyond assessing compliance by taking threats and vulnerabilities as well as business impact into account (see Figure 1). Only a combination of these three factors assures a holistic view of risk. Compliance posture is typically not tied to the business criticality of assets. Instead, compensating controls are applied generically and tested accordingly. Without a clear understanding of the business criticality that an asset represents to an organization, an organization is unable to prioritize remediation efforts. A risk-driven approach addresses both security posture and business impact to increase operational efficiency, improve assessment accuracy, reduce attack surfaces and improve investment decision-making.

In general, there are four different approaches enterprises can use to tackle security (see Figure 2).

The first concept was prevalent in the 1990s and can be best described as a reactive approach, whereby security is seen as a necessary evil. In this approach, silo-based point products are leveraged to monitor the company’s security posture. However, the usage of these tools is primarily of a reactive and tactical nature.

Once the frequency of data breaches increased and consumer interests were threatened, industry standards and government regulations were introduced and forced a compliance-driven approach to security. Here the objective is to achieve point-in-time compliance certification, whereby the tactical reactive approach is supplemented with layered security controls. Since many regulations and industry standards lack the notion of continuous monitoring, many enterprises using this approach adopt a check-box mentality and implement minimum requirements to pass the annual certification audits.

The rising tide of insider and advanced persistent threats, mounting regulatory pressure...
and the impact of big security data on an organization’s operational efficiency have led many progressive organizations to adopt either a risk-based or business-oriented approach to security. A risk-based approach to security assumes a prevention mentality, taking a proactive approach by interconnecting otherwise silo-based security and IT tools and continuously monitoring and assessing the data.

A business-oriented approach extends the risk-based approach by connecting into enterprise risk processes, taking input across financial, operational and IT risk factors. The ultimate goal is increased operational efficiency and effective business decision making.

ELEMENTS OF RISK-BASED SECURITY

In general, there are three major elements of a risk-based approach to security: continuous compliance, continuous (security) monitoring, and closed-loop, risk-based remediation.

Continuous compliance includes the reconciliation of assets and automation of data classification, alignment of technical controls, automation of compliance testing, deployment of assessment surveys and automation of data consolidation. When conducting continuous compliance, organizations can reduce overlap by leveraging a common control framework, increase accuracy in data collection and data analysis, and reduce redundant as well as manual, labor-intensive efforts by up to 75 percent.

Applying continuous (security) monitoring implies an increased frequency of data assessments (e.g., on a weekly basis) and requires security data automation (see figure 3) by aggregating and normalizing data from a variety of sources such as security information and event management (SIEM), asset management, threat feeds and vulnerability scanners. In turn, organizations can reduce costs by unifying solutions, streamlining processes, creating situational awareness to expose exploits and threats in a timely manner, and gathering historic trend data, which can assist in predictive security.

Last, closed-loop, risk-based remediation leverages subject matter experts within business units to define a risk catalog and risk tolerance (see figure 4). At the same time, a closed-loop, risk-based remediation process entails asset classification to define business criticality, continuous scoring to enable risk-based prioritization, and closed-loop tracking and measurement. By establishing a continuous review loop of existing assets, people, processes, potential risk and possible threats, organizations can dramatically increase operational efficiency, while improving collaboration among business, security and IT operations. This enables security efforts to be measured and made tangible (e.g., time to resolution, investment in security operations personnel, purchases of additional security tools).

BENEFITS OF RISK-BASED SECURITY

By leveraging a risk-based approach to security, progressive organizations can reduce risk, reduce costs, improve response readiness and increase risk-posture visibility. A good example is Fiserv, a company that serves the financial services industry with a broad spectrum of payment and account processing solutions such as transaction processing, electronic bill payment and presentment, business process outsourcing, and document distribution services. Fiserv uses a risk-based approach to security and dynamically aggregates and correlates financial, operational and IT key risk indicators (KRIs) from multiple and diverse controls to detect system vulnerabilities so identified risk can be effectively mitigated. This approach has resulted in a reduction of the time it takes to produce risk profiles from six to three months, resulting in efficiency savings.
of up to US $500,000. Furthermore, Fiserv was able to save US $1 million in overhead expenses by automating risk assessment efforts while at the same time shortening the policy control process from four to two months, saving an additional US $200,000. In addition, Fiserv achieved increased credibility with its board, management and regulators.

**CONCLUSION**

Cyberattacks can occur any time—so a solely compliance-driven approach to security is no longer effective. Instead, a risk-based approach to security as recommended by NIST in SP 800-137 (among others) is the best approach.

When applying a risk-based approach to security, organizations must automate many otherwise manual, labor-intensive tasks. This, in turn, results in tremendous time and cost savings, reduced risk, improved response readiness, and increased risk-posture visibility.

---

3 Agiliance, “Managing Security Risk for NERC/FERC Compliance,” Case Study Results, 2010
4 *CSO Magazine*, “GRC’s ROI: Fiserv Gets a Handle on Governance, Risk and Compliance,” April 2012

---

![Figure 4—Closed-loop, Risk-based Remediation](source: Agiliance Inc. Reprinted with permission.)