Business-Driven Risk Management Closes the Gap of Grief

GRC capabilities help translate security risks into business terms

Overview

Evidence is mounting that organizations can reduce the cost of breaches and increase security efficiency by proactively managing risk.

Organizations that hold a legacy perspective of security are at a disadvantage. In response to the latest security threats, these organizations often purchase the latest security gadget or system. For each new threat, there may be a new box. But each box is a security silo. Rather than providing integrated and complete coverage, point solutions create network blind spots, areas where the organization can't monitor user and system activity. So despite these security investments and perhaps even because of them, organizations still find it difficult to put security details in business context in real-time or to respond appropriately when information security vulnerabilities and incidents are identified.

As a result, security leaders are unable to understand and communicate security details as business risk. RSA calls this the "Gap of Grief".

We believe that the solution to the Gap is Business-Driven Security™, an approach to translate security risk into business language that business leaders and Board Members can understand and act upon. Business-Driven risk management in the form of a Governance, Risk and Compliance (GRC) solution plays a major role. In fact, GRC as a concept is at a point of evolution – moving ever closer to the business to truly transform risk management into a strategic enabler. RSA's vision of a Business Risk Management platform takes GRC capabilities into the next generation with the ability to translate any risk into actionable intelligence to improve business decisions. This evolution falls directly in line with Business-Driven Security.

Business Risk Management solutions are about more than security. Security risk is just one piece of operational risk, which is in turn just one piece of enterprise risk. A Business-Driven Risk Management solution provides an accurate, aggregated, and timely view of all enterprise risk – whether that risk is associated with people, processes, technologies, third parties, regulations, or something else – and provides a unified response to any security incident. In other words, it delivers organization-wide visibility, so security and business leaders can work together to proactively prioritize and manage risk.

In addition, Business-Driven Risk Management solutions enable an organization to extract more value from existing security investments by integrating with other systems and using the logs and data they generate.

By understanding and communicating information security in terms of the impact to the overall business, organizations can make better business decisions and more efficiently allocate the human and capital resources that manage information security.

Challenges abound

The world has changed. The attack surface has exploded; no longer do we have a clear, defensible perimeter secured simply by establishing preventative controls. The threat landscape is broader in scope, more sophisticated and targeted and new regulations are emerging around the world.

- **The scope and frequency of attacks continue to grow.**
- **Organizations, executives, and Board Members are increasingly held accountable** for failing to adequately manage information security.
- **Information security regulations are becoming more onerous.** Regulations increasingly focus on the infrastructure on which the information is stored, processed, and transmitted. Fines for compliance failures are growing. In addition, overlapping regulations can differ significantly in their approach to a problem.

The security function is not set up to win

The IT security function, as it exists in many organizations, is not effective.

- Many security teams cannot communicate security risk in a language that business leaders understand.
- This creates a disconnect between security teams and business leaders which leads to poor decisions about how to prioritize human and capital resource investments to protect and manage information risk.
- Many organizations do not fully understand where they have material exposure to information security risk, the significance of the risk, or what is being done to manage it.

Increased interest from business leaders

These days, about 70% of Boards of Directors are asking for increased senior executive involvement in risk oversight, according to a survey by the American Institute of Certified Public Accountants (AICPA). (See 2016 The State of Risk Oversight, AICPA.) For large or public companies, that figure is 88%.

In the event of a breach, CEOs and Board Members want to actively manage risk. They want to connect the breach to a system or asset and they immediately want to understand business impact. A Risk Management solution is invaluable in providing the information the CISO requires for those C- and Board-level conversations.

Board involvement may decrease breach costs

A recent study found that Board involvement reduced breach costs by about $6 for each compromised personal record. (See 2016 Cost of a Data Breach Study: Global Analysis, Ponemon Institute.) With Ponemon reporting global average number of records impacted by a breach at 23,834, this translates to $143,000 in savings per breach. Clearly, organizations that communicate security information in terms of business risk are reaping the benefits.

The study also identified many other Risk Management factors that decrease breach costs, including:

- Data governance improvements.
- Formal incident response planning.
- Business continuity planning.
- Mature compliance practices that reduce regulatory examination time and associated fines.

Yet, only one in four respondents in the 2016 AICPA survey felt that their organization had a complete risk management process, showing that although better methods and tools are available, the companies that use them have a clear advantage over 75% of the competition.

Security questions from business leaders

Business leaders simply want confidence that their security teams have effective control of security risk.

Frequently-asked CEO questions include:

- Have high priority assets been prioritized for threat detection and response?
- Where is this information handled, stored, processed, transmitted, and archived? How are weaknesses identified, threats detected, and incidents resolved?
- In the absence of controls and risk transfer, what is the likelihood that this important information can be stolen, altered, destroyed, or inaccessible for a period of time? What is the impact to the organization?
- How does our information security risk compare to the organization's other risks?
- Are any of these risks of enough significance to warrant devoting human and capital resources to mitigate and transfer the risk?
- Where significant risks have been identified, are the committed human and capital resources adequate to meet objectives?
- Where technology vulnerabilities and weaknesses have been identified, is the organization prioritizing remediation efforts based on the areas of highest business risk? Who is responsible?
- If an incident occurs, how bad could things get? Can the security team identify which information was breached, by whom, and in what timeframe? What are the potential repercussions?

- How do security risks impact the business? How might security team collaboration with the business improve corporate performance?

If security leaders are unable to clearly and readily answer these questions, business leaders may conclude that investments in technology and people are being spent without understanding the big picture of information security and business risk.

Technical answers, made in the absence of business context, widen the Gap of Grief.

Stuck in the Gap of Grief

The benefit of communicating with business leaders is clear. The questions a security team will be asked are known. and yet, the thought of the CEO walking up the hallway pains many CISOs, in part because business leaders have a skewed perspective of how to prioritize risks.

A recent survey of executives found that 59% are concerned with their organization's ability to stay operational following a data breach involving high-value information assets, such as trade secrets and confidential corporate information. (See The Cybersecurity Risk to Knowledge Assets, Kilpatrick Townsend and Ponemon Institute.) However, 53% indicated their senior management's greater concern is a breach involving credit card information or Social Security numbers. Notice the disconnect? For most leaders, protecting consumers from fraud is a higher priority than protecting the organization from threats that could very well force it to close the doors.

These grim facts demonstrate that security leaders with advanced technical knowledge are having a difficult time discussing in straight-forward business terms how to prioritize information security risks, assess the impact of security on organizational strategies and objectives, justify resource expenditures, and encourage business units to mitigate risk.

Point solutions create blind spots

Organizations sometimes feel the pressure to respond to a narrow set of threats with a point solution. Because organizations are buying, vendors have obliged with a proliferation of such tools. Although they may perform as claimed against select threats, they create blind spots in networks where user or system activity is not fully monitored.

Without full visibility, many organizations simply can't accurately identify their highest risks. Therefore, security leaders can't deliver risk-based recommendations to the business leaders and Board Members that have fiduciary responsibility to manage risk.

A common Business Risk Management framework provides a holistic view

Often, organizations don't understand the benefits of bringing together their patchwork of security, compliance, and governance efforts into a single

Business Risk Management framework that expands governance, risk and compliance activities. Business Risk Management is the next evolution of GRC – a step beyond implementing processes in reaction to compliance requirements towards a metamorphosis of risk management into an enabler of the business.

What exactly is a Business Risk Management platform? It is a set of capabilities that provides a common framework or platform to address three fundamental enterprise needs:

- Governance. The manner in which senior executives direct and control the organization.
- Risk Management. A set of processes used to manage issues that might prevent the organization from meeting its objectives.
- Compliance. An organization's efforts to adhere to laws, regulations, standards, policies, and contracts.

A Risk Management solution enables an organization to catalog all elements and their interrelationships to manage risk and compliance obligations in a way that is not just defensive but also energizes the organization's business objectives. These elements may include strategies and objectives, products and service, policies and procedures, authoritative and regulatory sources, business processes and sub-processes, third parties, and IT infrastructure elements (web services, IT software applications, IT systems, databases, and data stores), risks, and controls. In addition, the solution engages deep into the Lines of Business, which are sometimes referred to as "the first line of defense," to better align risk management processes with business operations.

The increased visibility leads to better business decisions, more efficient allocation of human and capital resources, renewed focus on the organization's mission, and peace of mind.

Business-Driven Risk Management

While no organization can completely eliminate risk, applying Business Driven Security enables organizations to more intelligently direct limited resources to the security risks that have the greatest business impact. This is the core reason for the shift from GRC to Business Risk Management – to factor business impact into decision-making at a much more detailed level.

Working with security leaders, business executives and Board Members can ensure that risk management is consistent with the organization's risk appetite, adheres to strategies, and meets objectives.

A Business-Driven Business Risk Management solution can enable organizations to:

- Identify critical assets, where each resides, its level of criticality, and how it should be prioritized.
- Assess the level of information risk.
- Understand where to apply limited resources to control information risk, to ensure that organizations are not over- or under-controlling risks.

- Monitor and manage the information risk on an on-going basis.
- Respond to new threats and incidents as thoughtfully and quickly as possible.

RSA's approach to Business Risk Management

The RSA Archer® Suite empowers organizations to manage multiple dimensions of risk on one configurable, integrated software platform. With RSA Archer solutions, organizations can efficiently implement risk management processes using industry standards and best practices, to significantly improve their business risk management maturity.

RSA's approach to Business Risk Management goes beyond event and incident management to establish a risk management foundation. The RSA Archer Suite provides organizations with access to a holistic view of security and business risks so attention can be directed to analysis and strategic problem solving. By improving the quality of information, organizations are improving the quality of their decisions.

The RSA Archer Suite serves as an aggregation point to consolidate governance, risk, and compliance information of any type. It allows technical and non-technical users to automate processes, streamline workflow, tailor the user interface, and report in real-time.

The RSA Archer Suite integrates with a range of other security technologies including point solutions and RSA's other Business-Driven Security Suites.

By leveraging information from existing security systems, the RSA Archer Suite helps organizations get a better return on their existing investments in security technology.

Conclusion

Business-Driven Security is an approach to information security risk management that focuses on communicating security details such as risk and incident response in terms that can be understood by an organization's top business leaders.

The RSA Archer Suite is specifically built to support Business-Driven Security. It powers conversations between security and business leaders by providing excellent dashboard views, actionable metrics, and better control.

With the RSA Archer Suite, security risk is depicted in a manner that can be compared with the organization's other risks, regardless of their type or source. This visibility into risks allows security leaders to answer questions from business leaders about security risk, priorities, and incident response. The improved visibility also allows compliance teams to address questions about the organization's compliance posture.

By understanding information security risk, compliance risk, and business risk within a single framework, CISOs, C-Suite executives, and Board Members can make better business decisions and ensure that the organization's objectives are met.

In a new spirit of collaboration, all parties can play a more proactive role in protecting what matters most to the organization.

Business-Driven security solutions from RSA

RSA is a leader in advanced cybersecurity solutions delivering Business Driven SecurityTM so organizations of all sizes can take command of their evolving security posture in this uncertain, high-risk world.

Our solutions and services uniquely link business context with security incidents so organizations can reduce risk and be sure they are protecting what matters most.

More specifically, RSA is the ONLY company that enables the three most critical elements of a sound security strategy: rapid detection and response, control at the user access level, and business risk management. No other company does this.

The **RSA Archer® Suite** empowers organizations to manage multiple dimensions of risk with solutions built on industry standards and best practices on one configurable, integrated software platform.

The **RSA® Fraud & Risk Intelligence Suite** is a centralized fraud prevention platform that uniquely blends continuous monitoring, risk-based authentication and fraud intelligence to deliver rapid insight into cybercrime attacks. Leveraging data from your business and other anti-fraud tools, the RSA Fraud & Risk Intelligence Suite enables organizations to greatly improve detection and response to fraud incidents across digital channels without impacting the customer experience.

The **RSA SecurID® Suite** enables organizations of all sizes to accelerate their business while minimizing identity risk and delivering convenient and secure access to the modern workforce. The RSA SecurID Suite leverages risk analytics and context-based awareness to ensure the right individuals have the right access, from anywhere and any device.

The **RSA NetWitness® Platform** is a threat detection and response platform that allows security teams to detect and understand the full scope of a compromise by leveraging logs, packets, endpoints, and threat intelligence. By aligning business context to security risks, RSA NetWitness Platform provides the most advanced technology to analyze, prioritize, and investigate threats making security analysts more effective and efficient.

About RSA

RSA, a leader in cybersecurity and risk management solutions, provides organizations with technology to address challenges across security, risk management and fraud prevention in the digital era. RSA solutions are designed to effectively detect and respond to advanced attacks; manage user access control; and reduce operational risk, fraud and cybercrime. RSA protects millions of users around the world and helps more than 90 percent of the Fortune 500 companies thrive and continuously adapt to transformational change. For more information, go to **rsa.com**.

RSA