RSA

SECURITY AND RISK MANAGEMENT COLLABORATION

A Guide to Working Together to Mitigate Cyber Attack Risk

CYBER ATTACK RISK IS BUSINESS RISK

There's more to responding than just stopping the attack. In this e-book, we'll explore areas where security and risk management leaders can collaborate to mitigate cyber attack risk.

Today's digitally connected operations present complex challenges for organizations that want to accelerate innovation and drive business objectives while ensuring they are managing their increasing digital risk. Organizations must bring together security and risk management leaders and teams to reduce the business impacts of cyber attacks. But this has traditionally been a challenge, because these two business functions typically have very different objectives and perspectives.

For example:

CISO OBJECTIVES

- Set and execute IT strategy
- Strengthen security posture and defense
- Control costs while reducing risk to acceptable levels
- Enable business, speed, innovation and productivity
- Maintain data privacy and drive IT compliance
- Drive IT compliance (PCI, SOX, etc.)

"It's my job to ensure our business teams' 'need for speed' doesn't put the company at undue risk. I know they need to work fast. But they need to know what's really at stake. Our reputation isn't something I can fix once it's broken."

CRO OBJECTIVES

- Set and execute risk management strategy
- Control costs while managing risk at acceptable levels
- Run the enterprise risk management program throughout the company
- Lead the enterprise risk committee and report to the CEO and board of directors

"It's my job to know about, understand and facilitate the management of all of the big risks across the enterprise, including those that threaten the organization's strategies and objectives or may be introduced through new products and services, business processes, combinations and reorganizations."

In today's digitally transformed world, bringing security and risk management together to combat cyber attack risk is critical to protecting the organization's assets, financial bottom line and reputation. Both silos in the organization play important roles in the threat detection and cross-functional response required to minimize overall business impact. Security and risk leaders should consider how their teams can work with each other to manage cyber attack risk across five domains: **breach preparedness, risk reduction, incident response, breach remediation and post-breach adaptation**.

BREACH PREPAREDNESS

Breach preparedness is the foundational component for managing cyber attack risk in any organization

Breach preparedness is the foundational component for managing cyber attack risk in any organization. It is impossible to be 100 percent secure; therefore, having technical and organizational action plans, a common language and well-defined processes is critical, so that when an incident does occur, the SOC team can contain it quickly and other areas of the organization that are impacted can be ready to execute their response plans.

Here are some key areas where security and risk management leaders can collaborate on breach readiness:

Establish a baseline and understand where you are today to manage cyber attack risk, and complete a gap analysis of current state posture to desired levels of cyber maturity based on industry best practices (such as NIST Cyber Security Framework 1.1).

Establish acceptable risk tolerance and describe it in business terms that can be understood across both parts of the organization as well as up the chain to the executive team.

Develop workflows and playbooks for response (both technical inside the SOC and business actions) as well as incident notification across the silos.

Assess risks and categorize assets based on criticality to the business and connect that data with the security team.

Connect tools to share information and allow for real-time data exchange between security and integrated risk management platforms.

RISK REDUCTION

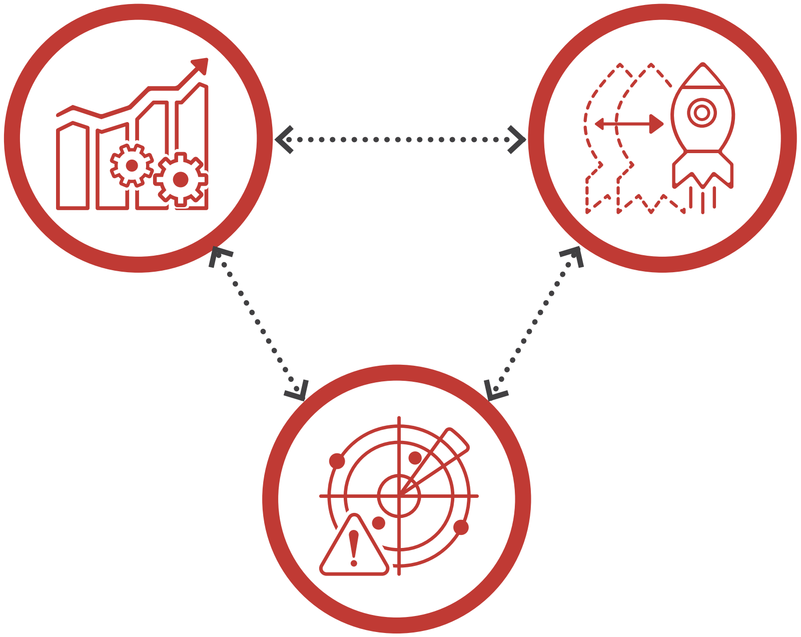
Organizations must continue to invest in protection capabilities to prevent attacks from occurring

Protecting assets, addressing and prioritizing known vulnerabilities and threats, and implementing tools, policies and processes to reduce threats will allow organizations to improve their security risk posture. And while it may not be possible to get to 100 percent attack prevention, organizations must continue to invest in protection capabilities to prevent attacks from occurring.

The following are areas of collaboration between security and risk management leaders to reduce risk:

Align and prioritize prevention investments, resources and policy change management based on asset and business criticality.

Practice simulated breach detection and response scenarios to identify gaps in processes and continually optimize.



Conduct regular risk assessments across target areas to continue to adapt to reduce risk.

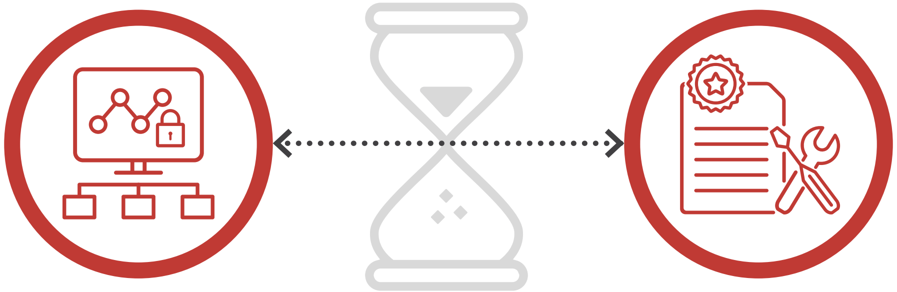
INCIDENT RESPONSE

Timing is critical

Detecting an attack as fast as possible and initiating the right response activities based on the level of risk the attack poses: These are the most critical actions to take to keep a small incident from escalating into a major breach.

For security and risk management leaders, visibility and context are critical elements of collaboration to ensure that each function is able to quickly deploy the right level of response. The ability to connect data across functions helps the security analyst be more effective at identifying the threat.

Timing is critical. For one thing, there are regulatory constraints on reporting an incident; European data privacy regulations, for example, require that a breach be reported to regulators within 72 hours after discovery. Gaining clear visibility into what exactly happened, who was affected, and what has been or will be done to contain it is also critical.



Threat detection capabilities enriched with advanced analytics and broader data sets make it possible to connect the dots across the environment to identify the threat before it can cause harm.

Security operations analysts should have access to asset criticality data right within their tools in order to quickly understand the potential impact upon detection.

BREACH REMEDIATION

A breach is not just a technical problem, but also a business problem

A breach is not just a technical problem, but also a business problem that requires a well-coordinated and planned response.

Key collaboration points for security and risk management in the remediation phase include the following:

Use automated incident notification from the SOC to risk management to enable risk managers to assess the incident, identify the business impacts and engage the appropriate resources to execute the response (and/or crisis management) plan.

Manage a single line of communications upstream to the C-suite and board, as well as downstream to internal departments and customer-facing channels, based on defined workflows.

Document what occurred and understand the vulnerabilities that were exposed, and develop an action plan to remediate.

POST-BREACH ADAPTATION

Take stock of the event, learn from it and continue to improve the effort to reduce overall risk

Just because the organization has remediated the breach doesn't mean that the case is closed. Organizations must have processes and procedures in place to ensure the breach does not happen again. This means establishing a feedback loop on the incident itself and how the response was orchestrated, and then taking those learnings and putting them into practice to reduce the risk of reoccurrence.

Collaboration between security and risk management leaders is paramount in this area to take stock of the event, learn from it and continue to improve the effort to reduce overall risk.

Use closed-loop vulnerability management to ensure that the actions in the plan were addressed to an acceptable tolerance level.

Look retrospectively into each phase of the breach response and report out to stakeholders and C-level leaders to identify areas for improvement across the organization.

Update policies to address failures.

Develop and deploy education and training to raise awareness across the organization of best practices to follow to reduce risk.

Helping organizations minimize the business impacts from cyber attacks and reduce their overall digital risk is the overarching goal of RSA. With our portfolio of solutions, we are helping security and risk management leaders understand their current capabilities, efficiently detect and contain threats, and coordinate the cross-functional response to minimize the negative financial, reputational and customer-relationship impacts of a breach.

DIGITAL RISK IS EVERYONE'S BUSINESS
HELPING YOU MANAGE IT IS OURS

RSA offers business-driven security solutions that provide organizations with a unified approach to managing digital risk that hinges on integrated visibility, automated insights and coordinated actions. RSA solutions are designed to effectively detect and respond to advanced attacks; manage user access control; and reduce business 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.

Find out how to thrive in a dynamic, high-risk digital world at rsa.com