RSA

A 4-STEP APPROACH TO

MITIGATING BUSINESS RISKS

FROM CYBER ATTACKS

Connecting Security, Risk and Business Teams to Mitigate Widespread Risks from Cyber Attack

Organizations continue to invest in security technologies to help them prevent cyber attacks. However, the evolving threat landscape—combined with the rate of change and scope and scale of digital environments—are causing many organizations to struggle to keep up with the growing risk of a cyber attack. The reality is, no matter how hard we try, we live in a world where prevention of cyber attacks appears nearly impossible. Therefore, to mitigate this risk, organizations must be quick to detect security incidents and prepared to deploy a truly cross-functional, enterprise-wide response.

THERE'S MORE TO RESPONSE THAN JUST CONTAINING THE ATTACK

Traditionally, the security team represents the front line in detecting cyber attacks and implementing technical responses to contain and remediate threats. This technical response is essential to protecting an organization and its assets. However, for many organizations, this is where their response stops.

While an incident may show up in an executive brief, the rest of the organization may not have visibility into:

In light of increased regulatory and customer pressures, organizations must be more transparent regarding attacks and the steps they take to mitigate future events. Cross-functional teams now have greater responsibility and shorter timeframes (e.g., 72 hours for GDPR) for notifying customers, third parties and regulators about security incidents, even if the impact to the business or customers was negligible.

This new dynamic requires security, risk management and business teams to work in lock step to respond to attacks and manage their fallout.

A 4-STEP APPROACH TO MITIGATE BUSINESS RISK FROM A CYBER ATTACK

Even with prevention measures in place, it is nearly impossible to get to 100% prevention of all cyber attacks. These four steps can help organizations implement a coordinated response from security, IT, risk management and business stakeholders.

STEP 1: PLAN FOR ATTACKS

STEP 2: DETECT SECURITY THREATS

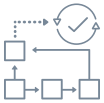
STEP 3: ASSESS THE IMPACT

STEP 4: RESPOND TO THE RISK

STEP 1:
PLAN FOR ATTACKS

Develop policies based on your organization's established risk tolerance and document workflows for centrally managing investigations and remediation, as well as coordinate a business response. This provides a repeatable process for triaging incidents cross-functionally with coordinated, well-defined plans that reduce effort and complexity.

PLAN FOR ATTACKS:



Create workflows to manage investigations and correlate indicators of compromise (IOCs) across the enterprise.

Establish a central organizational and IT asset catalog and taxonomy so teams involved are all on the same page.

Document incident response processes across critical business functions including compliance, public and investor relations, internal communications and the office of the general counsel so that everyone involved in these functions understands their roles and responsibilities.

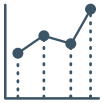
Test incident response workflows across your enterprise regularly for efficiency and effectiveness.

STEP 2: DETECT SECURITY THREATS

Cut through the clutter of alerts and empower your security team to detect known and unknown cyber threats with a security platform that provides visibility across all environments. Combine insights across security, IT and business silos to streamline forensic investigations and help analysts quickly identify the full scope of an attack.

DETECT THREATS:

VISIBILITY
Across logs, network, endpoint and hosts, Netflow



DEEP ADVANCED ANALYTICS
Including user and entity behavior analytics (UEBA)

BUSINESS CONTEXT
Including contextual intelligence and asset criticality

INCIDENT MANAGEMENT
Including orchestration and automation

ACTIONABLE INSIGHTS
Access and entitlement intelligence, fraud intelligence, threat intelligence, known vulnerabilities

STEP 3:
ASSESS THE IMPACT

Security teams typically focus on identifying the scope and technical severity of an incident, but many times lack the ability to quickly assess the business impact of the incident. By giving security teams business and risk context, they can prioritize and orchestrate the appropriate response based on potential business impact.

ASSESS THE IMPACT:

Provide incident responders with information about the importance of different corporate assets so that they better understand business impact and can prioritize accordingly.

Integrate business impact analysis into investigations to understand the up- and down-stream implications.

Conduct a cyber risk quantification to understand the dollar impact of cyber attacks on critical assets.

Incorporate known vulnerability data into investigations to quickly understand which assets are more vulnerable, thereby helping analysts prioritize remediation efforts.

STEP 4:
RESPOND TO THE RISK

Centralize incident management across functional silos both inside and outside of the SOC to ensure consistent, coordinated and—whenever possible—automated response. This centralization gives stakeholders a singular view of the risk an attack poses to the business and what's being done to address it.

	TECHNICAL RESPONSE	BUSINESS RESPONSE
INCIDENT: Rapid, Organized Response	Detect and declare incident Identify impacted areas Clear, process-oriented escalations Automation and orchestration to reduce dwell time and contain the threat	Incident declared, automatically invokes organizational response workflows Ensure business processes are resilient Engage cross-functional teams based on established workflows • Compliance • Legal • Communications • PR/IR
POST-INCIDENT: Address Vulnerability Gaps	Forensic analysis Locate assets, applications and protocols leveraged for data exfiltration Make security changes	Understand need for new controls or process changes (root cause for systemic issues) Communicate priority and direction to ensure most valuable assets are protected Closed-loop process to ensure change management

RSA HELPS YOU MITIGATE BUSINESS RISKS FROM A CYBER ATTACK

RSA provides an end-to-end solution that combines holistic threat detection with coordinated, cross-functional response. It connects security, risk and business stakeholders and gives them advanced capabilities for measuring and mitigating the business impact of a cyber attack. With RSA, you get hands-on advisory services to help you assess and mature your organization's ability to detect and respond to a cyber attack.

HOW WE HELP

RSA CYBER INCIDENT RISK FRAMEWORK

- Engagement
- Assessment
- Benchmark Report
- Cyber Practice Program

RSA RISK & CYBERSECURITY ADVISORY PRACTICE

EVOLVED SIEM/ ADVANCED THREAT DETECTION & RESPONSE

- Security Platform
- Logs & Packets
- Endpoint
- UEBA
- Orchestration & Automation
- Declare Incident Automation with **RSA Archer Suite***

RSA NETWITNESS® PLATFORM

INTEGRATED RISK MANAGEMENT

- Cyber Incident & Breach Response
- Vulnerability Program Management
- Business Impact Analysis
- Dashboards & Reporting
- Cyber Risk Quantification
- Extend Business Context to Security Analyst via Context Hub in **RSA NetWitness Platform***

RSA ARCHER® SUITE

SECURE, RISK-BASED ACCESS & AUTHENTICATION

- Risk-Based Authentication
- Authentication Anomaly Detection
- Identity, Governance & Lifecycle Management
- Access Policy Violation Detection
- Threat Aware Authentication – interoperability with **RSA NetWitness Platform***

RSA SECURID® SUITE

OMNI-CHANNEL FRAUD PREVENTION

- Omni-Channel Fraud Detection
- Advanced Adaptive Authentication
- Real Time Risk Assessment
- Fraud Intelligence

RSA FRAUD & RISK INTELLIGENCE SUITE

* Interoperability between products

Are you prepared to mitigate the business risks from cyber attacks? Take our online assessment to see how you stack up: **riskassessment.rsa.com**

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

RSA®

© 2019 Dell Inc. or its subsidiaries. All Rights Reserved. RSA and the RSA logo are trademarks of Dell Inc. or its subsidiaries in the United States and other countries. All other trademarks are the property of their respective owners. RSA believes the information in this document is accurate. The information is subject to change without notice. Published in the USA, 4/19 eBook H17602 W213684