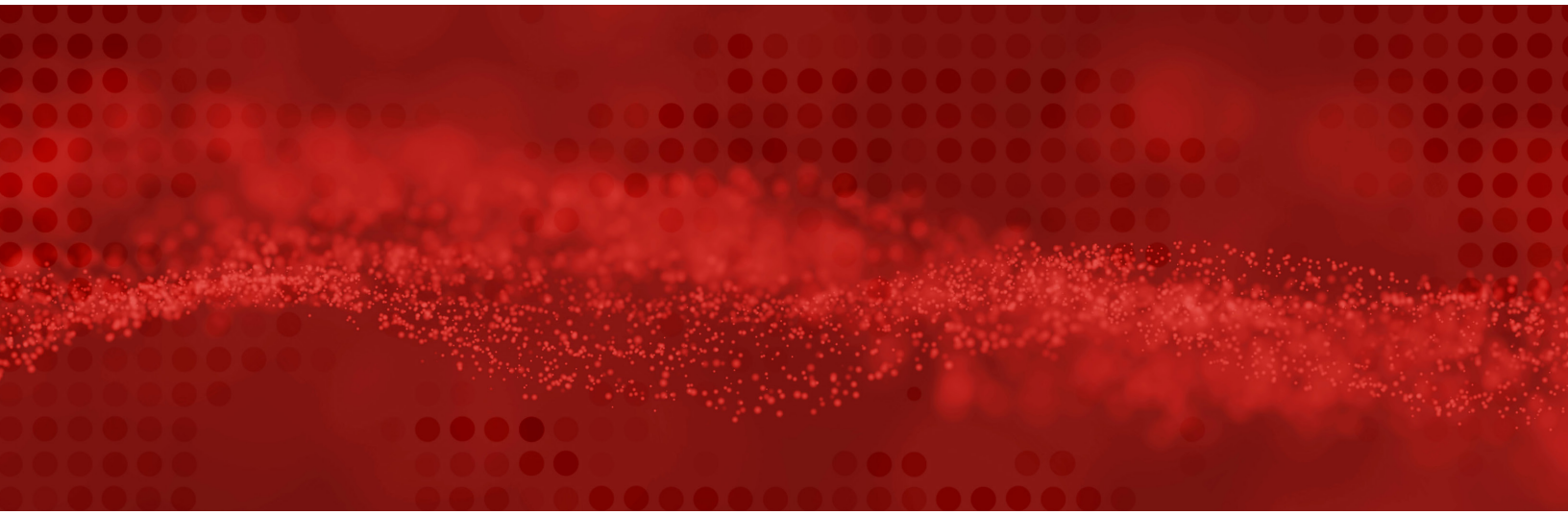
RSA

SOLUTION BRIEF

MITIGATE CYBER ATTACK RISK

CONNECTING SECURITY, RISK MANAGEMENT & BUSINESS TEAMS TO MINIMIZE THE WIDESPREAD IMPACT OF A CYBER ATTACK



DIGITAL TRANSFORMATION CREATES NEW RISKS

As organizations extend technology deeper into their day-to-day business operations, their risk profiles evolve. New digital risks—those unwanted and often unexpected outcomes that stem from digital transformation, digital business processes and the adoption of related technologies—represent a larger portion of potential obstacles to achieving business objectives. While the digital technology creates new business opportunities, it frequently leads to higher levels of cybersecurity, third-party, compliance and business resiliency risk.

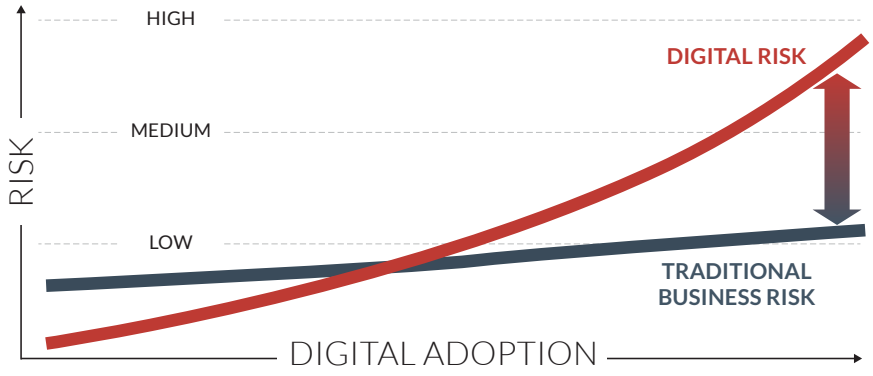


FIGURE 1: Digital risk increasing the overall business risk as organizations embrace digital transformation.

The impacts from these growing digital risks may be more disruptive than the operational risks that businesses have historically managed. In fact, many organizations are finding that as digital adoption accelerates, digital risk becomes the greatest facet of risk they face, especially growing cyber risks.

AS ORGANIZATIONS EXPAND DIGITAL OPERATIONS, CYBER SECURITY RISKS MULTIPLY

Organizations need to evolve to stay in front of rising cyber threats and their wide-reaching impact across increasingly digitized operations. Attackers continue to advance and use sophisticated techniques to infiltrate organizations which no longer have well defined perimeters.

It's arguably impossible to prevent all cyber attacks. Therefore, organizations must marshal advanced detection capabilities and deploy a coordinated response across security, IT, risk and business stakeholders to minimize the impact of an attack.

At the same time, responsibilities for detecting and responding to security incidents are expanding beyond the security operations center (SOC). Business stakeholders continue to digitize their operations, elevating the risk and potential impact of cyber attacks. Consequently, they must now play a larger role in protecting their assets as well as their bottom lines.

Expanding security and data privacy regulations coupled with increased consumer demand for more corporate transparency around data use and breaches, have also prompted business stakeholders also are now more involved in security and risk management as a matter of corporate governance. Organizations face pressure to respond proactively to security incidents, both to ensure compliance and manage fallout from customers, investors and partners.

Of course, it's arguably impossible to prevent all cyber attacks. Therefore, organizations must marshal advanced detection capabilities and deploy a coordinated response across security, IT, risk and business stakeholders to minimize the impact of an attack.

CYBER ATTACK RESPONSE TAKES MORE THAN A TECHNICAL SOLUTION

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

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

- what occurred
- how bad it was
- what and who were impacted
- what was done to stop it
- how the organization is preventing it from happening again

Increased regulatory and customer pressures are forcing business leaders to be more transparent about attacks and the steps they take to mitigate them in the future. Cross-functional teams now have greater responsibility and shorter timeframes (e.g., 72 hours for European Union's GDPR regulation) for notifying customers, third parties and regulators, even if the impact to the business or customers was negligible. These changes in notification laws have dramatically altered how organizations manage security incidents. In fact, during the first eight

months GDPR took effect, organizations reported 59,000 data breaches and European regulators imposed 91 fines, including a $57 million fine for processing personal data without valid authorization[1].

These new dynamics require security, risk and business teams to plan and coordinate their strategic and technical responses to a cyber attack. Yet the traditional, functionally-siloed approach to cybersecurity prevents security, IT, risk and business stakeholders from collectively understanding the true nature of cyber attack risk, and thus, of coordinating an effective, enterprise-wide response designed to mitigate it.

As digital adoption expands, these groups MUST converge into a combined force to manage cyber attack risk.

BREAK DOWN ORGANIZATIONAL SILOS TO MITIGATE CYBER ATTACK RISK

Build the connective tissue between security, IT, risk and business teams to more effectively detect a cyber incident; understand the full scope, scale and impact of an attack; address the underlying technical cause of an attack to stop it; and proactively engage business teams to handle the customer, legal and regulatory response.

RAPIDLY DETECT INCIDENTS:

To detect an incident, give security and operations teams advanced tools to cut through the clutter to pinpoint the threats that matter most. Organizations can combine pervasive visibility and insights such as logs, packets, netflow, endpoint, user behavior, identity and fraud data from across the digital environment. This data should be enriched, in real-time, with business context and threat intelligence to be able to investigate and identify known and unknown threats.

- Provide your security operations center (SOC) with a security platform that collects data across all environments (cloud, virtual, on-premises) and leverages advanced analytics and business context to help analysts identify and prioritize the most significant threats.
- Connect security analysts with identity and access management controls so they can understand anomalous access activity and limit exposure from an identity-based attack.
- Apply fraud intelligence, risk-based authentication and behavioral analytics to detect and respond in real time to threats in consumer-facing channels.

ASSESS THE INCIDENT:

Help security and risk teams identify the scope and severity of incidents, as well as understand their overall business impact.

- Connect and correlate advanced threat analytics, asset vulnerability, user and entity behavior, access and entitlement insights, and fraud intelligence to support forensic investigations and determine the full scope of an incident.
- Give SOC teams access to organizational and IT asset catalogs with asset criticality information so that they can prioritize incidents based on risk.
- Centralize incident response to speak with one voice as to 'what it is', 'how bad it is' and 'what's being done to address it' to ensure accurate analysis and reporting to business leaders, the C-suite and board to make decisions.

COORDINATE INCIDENT RESPONSE:

Centralize incident management across organizational silos to facilitate a consistent, coordinated and automated response to attacks.

- Prepare for attacks proactively before they occur. Create policies based on your organization's established risk tolerance; document workflows to centrally manage investigations and remediation; and define incident response processes across critical business functions including compliance, public and investor relations, internal communications and the office of the general counsel.
- Automate and orchestrate workflows from incident declaration to closed-loop remediation to streamline triage and response.
- Post event, centrally manage the action register to close vulnerabilities, change policies and procedures, and train employees to ensure follow-through and mitigate future risk.

THE RSA ADVANTAGE

There are many point solutions across the market today to address security and risk issues. However, organizations need an integrated approach to manage emerging digital risks. RSA delivers market-leading security, integrated risk management, identity and fraud technologies in addition to battle-tested advisory services from the RSA® Risk & Cyber Security Advisory Practice. Connecting key capabilities, shared business context and threat insights allows organizations to break down the functional silos that prevent them from rapidly detecting and responding to cyber attack risks.

RSA
RISK & CYBERSECURITY
ADVISORY PRACTICE

RSA® RISK FRAMEWORK FOR CYBER INCIDENT RISK

Improve your organization's cyber risk readiness with the RSA Risk Framework for Cyber Incident Risk. It's aligned to the NIST Cybersecurity Framework and designed to represent the perspective of your CEO and board.

RSA
NETWITNESS®
PLATFORM

RSA NETWITNESS® PLATFORM

Advance your security team's threat detection and response game with the UEBA and SOAR capabilities in our evolved SIEM and get instant visibility into threats across your digital enterprise. ***Declare an incident and automatically kick-off workflows to rapidly respond to an incident across business, risk and security teams at the push a button with interoperability with RSA Archer Suite.***

RSA
ARCHER®
SUITE

RSA ARCHER® SUITE

Minimize the impact of security incidents with the RSA Archer Suite. Coordinate cyber incident and breach response across the organization, from the SOC to the boardroom. Establish policies and workflows to centrally manage investigations; document enterprise-wide incident response procedures; and more. ***Interoperability with RSA NetWitness Platform allows you to automatically share business critical context with security analysts to help them prioritize threats based on business impact.***

RSA SECURID® SUITE

Reduce your risk of identity-based attacks and insider threats with modern, mobile multi-factor authentication; real-time detection of suspicious access and entitlements; and automated, risk-based identity governance controls. ***Interoperability between RSA SecurID Access and RSA NetWitness Platform means you can enable threat aware authentication, using threat intelligence from the SOC to automatically enforce step-up authentication based on risk.***

RSA® FRAUD & RISK INTELLIGENCE SUITE

Detect and respond to fraud threats in your consumer-facing digital channels with a combination of actionable fraud intelligence, real-time behavioral analytics and risk-based adaptive authentication. To enrich threat detection and investigations, leverage insight into cybercrime activities on the dark web targeting your organization and customers (e.g. stolen credentials, phishing attacks).

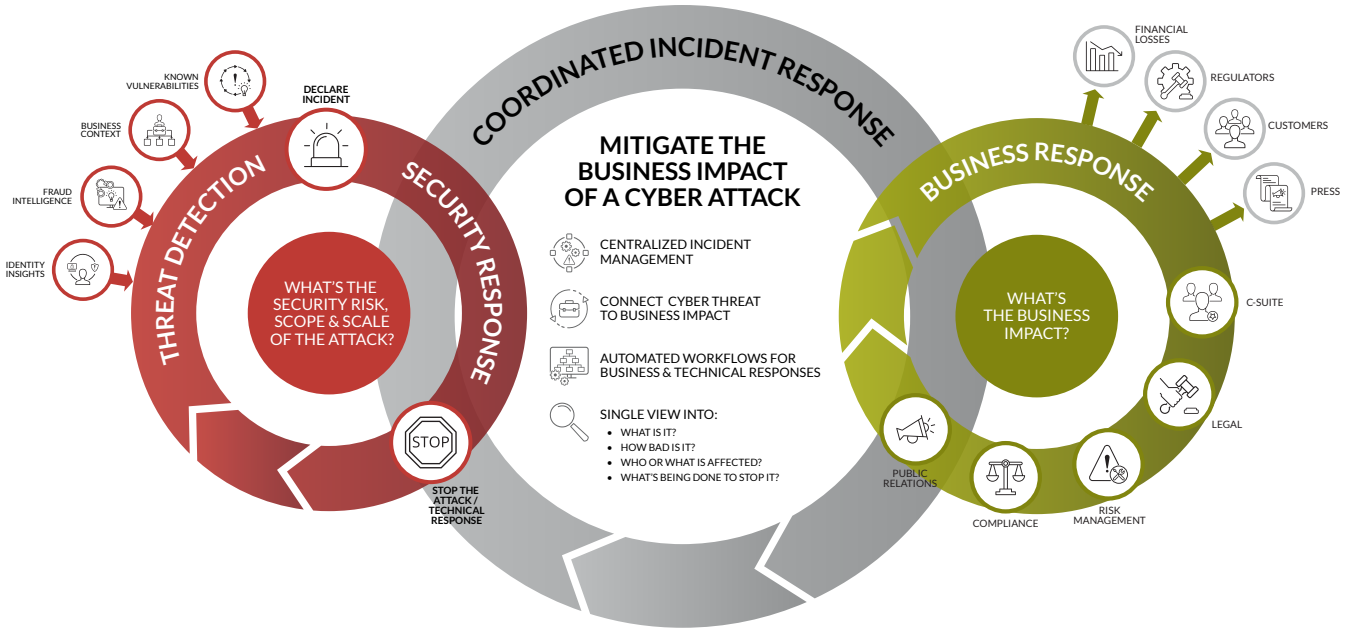


FIGURE 2: RSA helps organizations coordinate the technical and business responses to minimize the overall impact of the cyber attack.

ASSESS YOUR ABILITY TO RESPOND TO AN ATTACK

Our solution for mitigating cyber attack risk goes well beyond technical tools. Our holistic approach starts with an assessment of your current capabilities and processes for detecting and responding to cyber threat and culminates with a roadmap for improving your organization's security and response posture.

The RSA Risk Framework for Cyber Incident Risk can help you:

- Assess your organization's current cyber risk readiness with an approach that crosses traditional functional boundaries.
- Use a maturity model that supports the perspective of the CEO and board members.
- Align your security strategy with industry standard frameworks such as NIST Cyber Security Framework (CSF) 1.1 and NIST SP 800-61 Rev. 2, Computer Security Incident Handling Guide (CSRC).

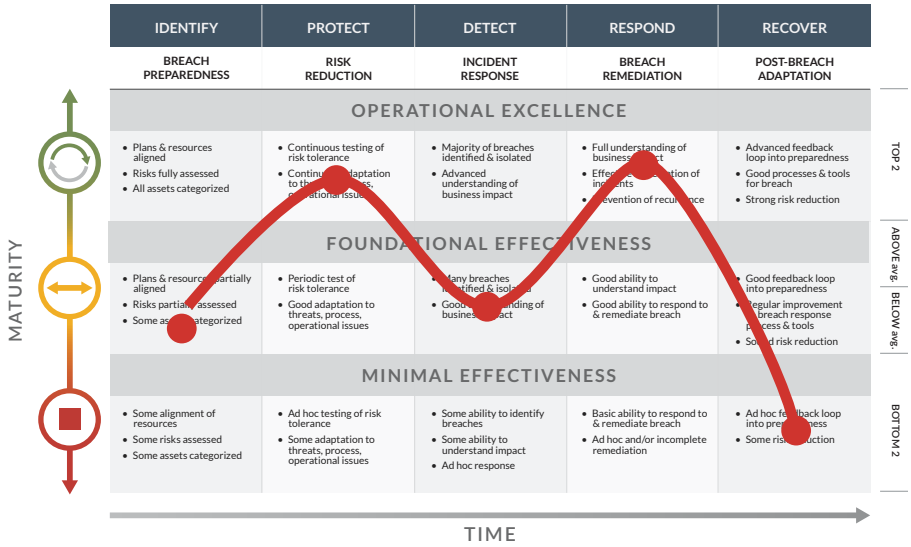


FIGURE 3: The RSA Risk Framework for Cyber Incident Risk helps organizations assess maturity of their cybersecurity programs and provides a roadmap for optimal improvement.

CONCLUSION

Cyber attack risks are more prominent and widespread in today's digital environment. Organizations struggle to respond to the evolving threat landscape—a challenge compounded by visibility and process gaps created by functional silos. This results in uncoordinated responses to cyber incidents that magnify financial, operational, reputational and compliance risks for businesses. To mitigate those risks, RSA provides a holistic solution that breaks down silos and provides organizations with the technology, processes and insights to face cyber attacks with confidence.

ABOUT RSA

RSA® Business-Driven Security™ solutions provide organizations with a unified approach to managing digital risk that hinges on integrated visibility, automated insights and coordinated actions. With solutions for rapid detection and response, user access control, consumer fraud protection and integrated risk management, RSA customers can thrive and continuously adapt to transformational change. For more information, visit rsa.com.

1. https://www.darkreading.com/attacks-breaches/over-59k-data-breaches-reported-in-eu-under-gdpr/d/d-id/1333798