RSA

WHITE PAPER

SECURITY & RISK: TACKLING DIGITAL RISK TOGETHER

SECURITY & RISK: THE CASE FOR COLLABORATION

In the era of digital transformation, every organization faces this critical question: Are you going to let digital risk hold you back, or are you going to manage it and move forward?

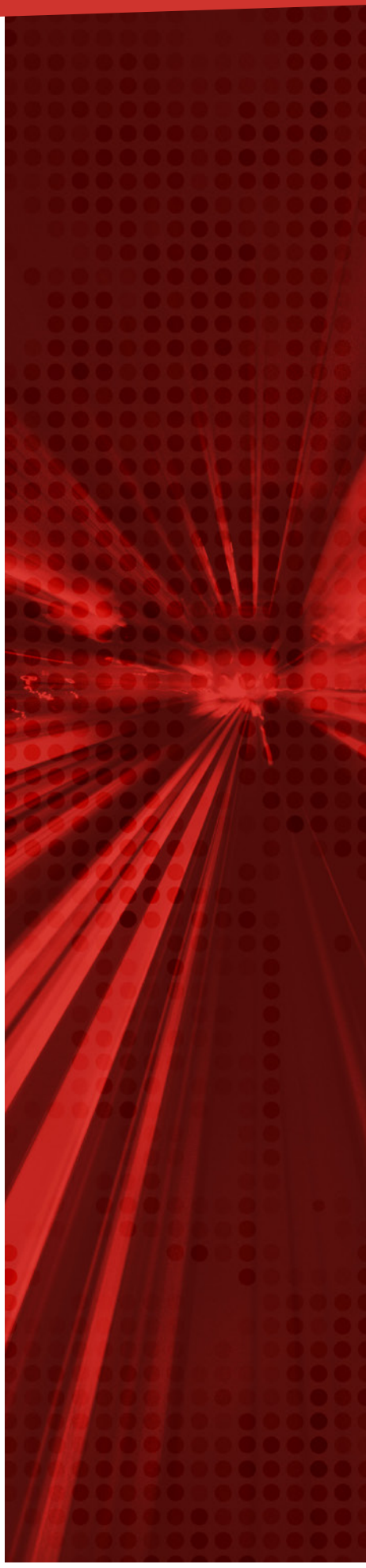
Managing the risk that comes with adopting more digital technologies is crucial to successfully applying those technologies to achieve business goals. It's a tough challenge that requires security and risk management teams reaching across traditional divisions to work truly in tandem, often for the first time.

In most organizations, there has historically been a distinct division between security and risk management—understandable in the days when security events had consequences mainly for IT, rather than for the business as a whole. But that division is no longer tenable when security risks are business risks, which is increasingly the case as more organizations undergo digital transformation.

We still see the security vs. risk division in play every day, when those who are responsible for managing business risk tend to focus on the potential of digital transformation to advance the business—while those who are responsible for security are more likely to first think of its potential to jeopardize security. Who is right?

The answer, of course, is both. Organizations need to manage risk so they can move forward, and they need to manage risk so they can stay safe.

And if that's the answer, then the question is how to manage digital risk so the organization can pursue opportunity and remain secure. Only with both sides working on the same side can the organization achieve this goal. How do we get there? Let's look at where security and risk teams are now, and see where they can go next—together.



YOU SAY SECURITY, I SAY OPPORTUNITY

Security and risk teams tend to develop their own ideas of what "good" looks like. Given the silos in which they have traditionally operated, it's understandable that this often happens independently, most likely without the benefit of understanding the other's objectives, requirements or capabilities. Consider these examples.

IMPACT OF NEW TECHNOLOGIES

SECURITY PERSPECTIVE

Adding more SaaS applications, expanding further into IoT, expanding the supply chain—these and other digital initiatives result in more points of vulnerability to secure. And the faster change happens, the harder it is for the security team to keep up.

RISK MANAGEMENT PERSPECTIVE

Taking on digital initiatives means being able to offer more innovative products and services, and deliver better experiences—which means being able to win and keep customers, instead of losing them to more innovative competitors.

COMPLEXITY OF OPERATIONS

SECURITY PERSPECTIVE

Responding to new kinds of security risks, staying ahead of cyber threats when new ones are popping up all the time, being proactive when the business is constantly launching new digital initiatives—that's what the security team's job is like today. Risk managers just have to worry about one thing.

RISK MANAGEMENT PERSPECTIVE

Forging relationships with new partners to be more competitive, dealing with regulatory challenges around data privacy, demonstrating the effectiveness of business development strategies to the board—that's what the risk management team is up against. Security just has to worry about one thing.

WHERE TO INVEST RESOURCES

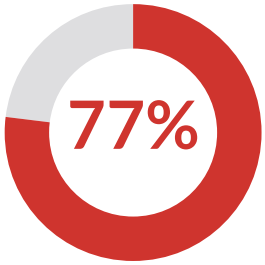
SECURITY PERSPECTIVE

Expecting the security team to keep pace with digitally driven changes, but not investing in the tools and people they need, makes it impossible for security to do everything necessary to keep the business safe.

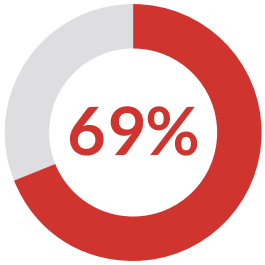
RISK MANAGEMENT PERSPECTIVE

Making decisions about investing resources is about maximizing positive business impact while minimizing risk. How can we justify more security investment unless we can project a return that meets that standard?

Those aren't the only ways in which security and risk teams see things differently, but they're good examples. And many organizations are acutely aware of the problem. Consider that in a recent RSA survey of security and risk professionals:

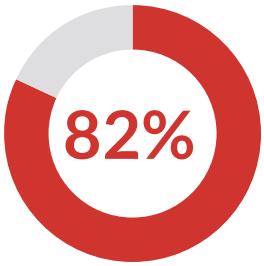


said the **relationship** between **business risk and IT security** can be **difficult to coordinate**



said they believe the use of **different tools and languages** makes **communications** between security and risk personnel **challenging**

Perhaps even more important, though—and more promising for the prospect of narrowing the distance between the two—is the recognition of their interdependence:



said their organization **considers security** a **business risk** rather than just an IT risk

IT TAKES TWO
TO ANSWER THE TOUGH QUESTIONS

Without an understanding of the business risks of a security breach or a fraud attempt, how can an organization possibly plan to advance and protect the business? When network sensors start firing, alerts start pouring in and cases start accumulating, siloed risk and security teams will likely be focused on their own responsibilities and assets.

Security and fraud operations do their best to identify threat vectors and apply mitigation, while starting to collect evidence for the ensuring investigation. But have their response plans taken into account critical uptime that needs to be preserved? Are standard operating procedures for incident communications informed by compliance requirements? Security teams that aren't able to budget and plan for these complexities are not going to be able to account for them in the midst of an attack.

Before long, people at the top start to ask their own questions:

CFO:
What is the exposure to loss?

GENERAL COUNSEL:
Was IP or other sensitive data taken?

CRO:
What are the regulatory compliance implications?

CIO:
Are our security investments meeting efficacy expectations?

CEO:
What about the impact to our brand?

BOARD OF DIRECTORS:
What is the overall business impact?

And you'll also hear things like:

"What have we done to address the problem?"

"How fast can we fix it?"

"How are we measuring it?"

"Are we improving?"

"How do we compare to peers in our industry?"

Security alone cannot answer these questions definitively; nor can the business. The questions require informed and well-considered responses that incorporate multiple perspectives. Even without the myriad new threats and challenges that appear every day, security and risk management functions that aren't in sync can leave organizations without a complete understanding of their overall digital risk posture.

MANAGING DIGITAL RISK TOGETHER

The digital transformation imperative, and the digital risk it brings, are paving the way for a convergence of risk and security today. Some organizations are developing security strategies in a broader business context, seeking to inform security with specific information about business objectives and values. Organizations looking to adopt such an approach should consider a few key recommendations:

The CISO should be part of the strategic team that sets business objectives, initiatives and priorities. It's the only way to ensure alignment of security strategy and business priorities from the start—the only way to ensure security strategy has a business context.

Security teams, from top to bottom, must have a fundamental understanding of business risk. Working closely together, risk management and security leaders can pursue decisions that accelerate the business while identifying and managing digital risks to that business.

Security operations center (SOC) teams need to have business context for preventing, detecting and remediating threats. For example, is a threat targeting essential tech infrastructure, or just the server that hosts the cafeteria menu? Without the benefit of context, they may find it difficult to set priorities, make effective decisions, follow the right leads and communicate the relevant details—all while being inundated with alerts in the midst of an attack.

THE THREE PILLARS OF BUSINESS-DRIVEN SECURITY

When organizations align risk and security, they ensure the visibility, insight and action required to manage digital risk effectively.

VISIBILITY

The security team must be able to see across digital channels, both internal and customer-facing, at all times—across business processes, networks, devices, people and transactions. Only with visibility from the endpoint to the cloud, with detailed analytics, is it possible to identify and correlate security and business risks across the entire environment.

INSIGHT

Faster insight, through better analytics, is critical. In today's digitally driven business environment, there is an unstoppable avalanche of data from a variety of sources: third-party business partners, cloud computing, a dynamic workforce that's both mobile and remote, a growing threat landscape and more. The more time SOC teams need to interpret an event, the greater the risk.

ACTION

The most effective way security teams can turn insights into action is to orchestrate and automate responses to events. For example, when the SOC team spots suspicious user activity through a deviation in the analytic baseline, they can enable the identity control plane to take action—stepping up authentication to ensure the user is legitimate.

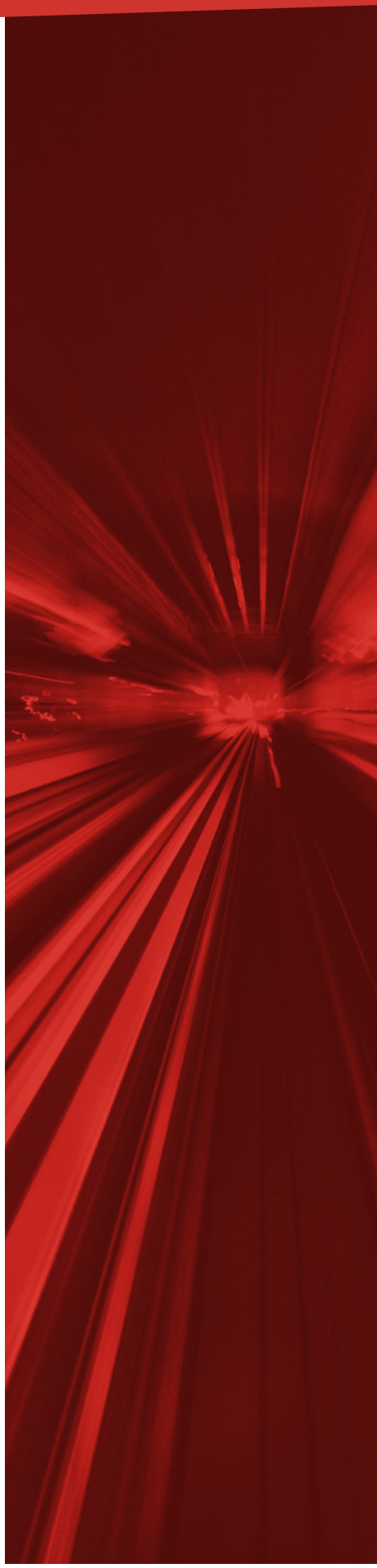
THE TIME TO ACT IS NOW

Organizations that don't pursue an inclusive, collaborative relationship between security and risk management risk paying a high price. At some point, a security event will occur that is devastating to the business, and the two sides will have to work together—if not by choice, then by circumstance. They would do better to act sooner, to protect their standing in the industry, keep their customers and explore today's unprecedented opportunities to pursue a bright digital future.

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