BRIDGING THE GAP OF GRIEF
WITH BUSINESS-DRIVEN SECURITY
CONTENTS

Executive Summary.........................................................................................................................1
Introduction: The Gap of Grief................................................................................................... 3
Modernization, Malice & Mandates............................................................................................ 5
Bridging the Gap with Business-Driven Security................................................................. 7
Conclusion..........................................................................................................................................9
EXECUTIVE SUMMARY

“W”orldwide spending on information security products and services will reach $86.4 billion in 2017, an increase of 7 percent over 2016, with spending expected to grow to $93 billion in 2018, according to the latest forecast from Gartner, Inc.”¹ Despite this level of spending, in the same period, we have seen nearly 2,000 data breaches² and nearly 2 billion personal records reported stolen.³ Security technology alone cannot solve our security problems.

In most organizations today, there is a disconnection between security and fraud teams and their business counterparts. More than 80 percent of board members in a recent survey believed IT and security executives needed to improve the way they report to the board.⁴ Because the lack of understanding and coordination can cause all parties real anxiety and discomfort, RSA has dubbed it “the Gap of Grief.”

This gap isn’t new, but it is without a doubt growing more treacherous for organizations every day. Businesses need to simultaneously quicken the pace of digital transformation, anticipate the growing resourcefulness of malicious actors and respond to unprecedented regulatory expansion (both in quantity and scope). The pressure is so great from these forces—modernization, malice and mandates—that it is spurring a convergence of security and business, with the aim of developing and implementing a more coordinated approach to security strategy.

To embrace this convergence, and bridge the Gap of Grief, it is more important than ever to put security details into business context quickly. A thoughtfully designed formula of visibility, insight, response and context—what RSA calls “Business-Driven Security”—must underpin any security or business effort. Only then can organizations understand to what degree incidents affect things like business continuity, end-user experience, intellectual property and brand reputation.

Getting it right means being able to accurately and quickly answer the most critical question corporate leaders care about in the wake of an event:

“WHAT IS THE IMPACT TO THE BUSINESS?”
“SECURITY TECHNOLOGY ALONE CANNOT SOLVE OUR SECURITY PROBLEMS.”
INTRODUCTION: THE GAP OF GRIEF

The Gap of Grief, another name for the familiar problem of siloed security and business functions, resulting in poor visibility and communication, is all too common in today’s tech-fueled, highly competitive business environment. More than 80 percent of respondents to a Dell survey believed security teams can better enable digital transformation initiatives if they are included early in the project.5 Throughout the lifecycle of any business, this divide can inhibit even the best security strategies.

Security teams and business functions all tend to develop their own idea of what “good” looks like. This often happens independently, most likely without the benefits of understanding the others’ objectives, requirements or capabilities. Even before an incident occurs, the Gap of Grief can affect budgeting, planning and preparedness. Without a contextual understanding of the business risks of a security breach or fraud attempt, how can you spend and plan and practice to secure what matters most?

When network sensors start firing, alerts start coming in and cases start accumulating, these groups are often focused on their own responsibilities and assets.

Security and fraud teams do their best to identify threat vectors and apply mitigation, while starting to collect evidence for the ensuing investigation. This is where the Gap of Grief can really show itself.

Have 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 who 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.

“EVEN BEFORE AN INCIDENT OCCURS, THE GAP OF GRIEF CAN AFFECT BUDGETING, PLANNING & PREPAREDNESS.”
And you’ll also hear people ask things like:

- “What have we done to address the problem?”
- “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. These kinds of questions require informed and well-considered responses, incorporating a diversity of sources and analysis.

Even without the myriad new threats and challenges that appear every day, the Gap of Grief can leave mature organizations without a complete understanding of how cybersecurity affects their overall digital risk posture.
MODERNIZATION, MALICE & MANDATES

A number of forces can make the Gap of Grief more treacherous for organizations. The demands of interoperability and availability, along with consumers’ and organizations’ appetites for modernization and innovation, can present constant challenges. The stealth, persistence and resourcefulness of malicious actors only seems to be increasing. On top of that, new and more stringent mandates continue to raise the bar for compliance and digital risk strategies.

Modernization: Quickening Pace of Digital Transformation

Modernization is about the digital, IT and workforce transformations that are in motion across businesses and the public sector. These transformations leverage multi-cloud environments, cloud apps, and Internet of Things (IoT) and mobile technologies, which expand consumer-facing channels but often sit outside the traditional secure perimeter. Too often, teams lack the skills, tools and processes to deploy, manage and protect their assets within these highly distributed environments and in light of the growing sophistication of cyber threats. Technology unlocks opportunities, but can expand attack surface and significantly affect the ways in which consumers interact and transact.

Malice: Increasingly Hazardous Threat Landscape

Never before have malicious actors had so many tools, techniques and procedures at their quick and easy disposal. Increasingly stealthy and virulent malware, costly account takeovers, site-killing distributed denial of service (DDoS) attacks, and persistent ransomware exploiting zero-day vulnerabilities are just a short list of what enterprise security and fraud teams are up against. All of this and more is being made readily available in thriving, anonymous underground markets. Adversaries are also getting creative, and seem to be finding ways to access whatever new digital assets their victims deploy, including consumer devices and apps. Making matters worse, it is easier than ever for attackers to orchestrate sophisticated campaigns, targeting a specific organization or employee, persisting until successful, and digging in for the long haul.

Mandates: Industry and Government Forcing the Issue

Not only do U.S. organizations have to continue to manage legacy mandates like HIPAA and Gramm-Leach-Bliley, they now need to anticipate the requirements to a number of proposed and pending new directives, along with subtler shifts to regulation in general. The proposed U.S. Cybersecurity Disclosure Act of 2017 would create a legal mandate for companies to disclose whether and how their board of directors includes any members with cybersecurity expertise, as defined by the National Institute for Standards and Technology (NIST). Much of the focus around the European Union’s General Data Protection Regulation (GDPR) has been on the weight of the regulatory burden it imposes and the size of the penalties it exacts for failing to comply with its specified data protection principles. The European Banking Authority’s Revised Directive on Payment Services (PSD2) serves as the legal foundation for a groundbreaking cross-EU payments market.
One often overlooked aspect of new regulations, is the "risk assessment" requirements that many have introduced. The GDPR, new cybersecurity regulations from the New York Department of Financial Services (NYDFS) and other legislation all include specific language around implementing appropriate risk assessment processes.

“A NUMBER OF FORCES CAN MAKE THE GAP OF GRIEF MORE TREACHEROUS FOR ORGANIZATIONS.”
BRIDGING THE GAP WITH BUSINESS-DRIVEN SECURITY

The combined pressures of modernization, malice and mandates are spurring a new way of thinking about security strategy, marked by a convergence of security and business risk in the enterprise. Some organizations are starting to develop security strategies in collaboration with the broader IT, fraud, risk and business functions, seeking to inform security with relevant, contextual and specific information about what the business values most. Organizations looking to adopt such a “Business-Driven Security” approach should consider a few critical elements.

To ensure security strategy has the context of business risk at its heart, the CISO must become part of the strategic team that sets and reviews business objectives, initiatives and priorities. Only then, and with real championship, can organizations start to align security strategy to the organization’s priorities from inception.

Business-driven security teams must have a fundamental understanding of risk. Security and business leaders alike are continually trying to make good decisions that accelerate the business while identifying and manage digital risks to that business. Risk is the language of business.

Assessing risk requires a level of awareness that is both broad and deep enough to sufficiently cover an organization’s critical assets, and even account for those that may not be covered. Specifically, security teams could benefit from a deeper understanding of identity as an undeniably effective attack vector; according to Verizon, 81 percent of hacking-related breaches leverage stolen or weak passwords.7

Understanding risk and identity, both enterprise and consumer, gives security operations teams a better understanding of business context, which can improve prevention, detection and remediation efforts. Without the benefit of business context, these critical functions may find it difficult to make the right decisions, follow the right leads and communicate all of the relevant details while being inundated with alerts in the midst of an attack.

THE FOUR PILLARS OF BUSINESS-DRIVEN SECURITY

The four pillars of Business-Driven Security are critical focus areas that can help security teams better understand what “normal” looks like for their business, where there may be issues, and what is ultimately most important. These essential elements must all function together to support the convergence of security and business risk, and effectively bridge the Gap of Grief.
“BUSINESS-DRIVEN SECURITY TEAMS MUST HAVE A FUNDAMENTAL UNDERSTANDING OF RISK.”

FULL VISIBILITY:
The security team must be able to see across all digital channels, both internal- and consumer-facing, at all times—across business processes, networks, devices, people (including consumers) and transactions. Only with visibility from the endpoint to the cloud, with detailed analytics, can organizations identify and correlate security and business risks across the whole environment.

RAPID INSIGHT:
Faster insight, through better analytics, is paramount. The modern business environment is a cacophony of data from external business partners, cloud computing, personal devices and the like, where most unusual behavior will be harmless—but some not. The “time to insight” for security teams is collapsing to zero. The more time needed to interpret an event, the greater the risk.

COMPREHENSIVE RESPONSE:
Today, security teams take the findings from their security tools and remediate in a way that, in most cases, doesn’t scale. The most effective way to turn insights into action is to orchestrate and automate response. For example, when security spots a user acting suspiciously through a deviation to the analytic baseline, they can enable the identity control plane to take action—stepping up authentication to ensure confidence that the user is legitimate.

BUSINESS CONTEXT:
Security and fraud teams can’t rely solely on what they see happening on their own network and in consumer-facing channels; they must be able to interpret events quickly and understand the criticality of the systems and processes affected. Contextual intelligence, including from intel-sharing partnerships and associations, facilitates faster and better decisions for all involved. For security teams, understanding business context (such as the criticality of an asset) can help prioritize work and determine urgency when managing cases or incidents.

Disregarding the Gap of Grief and the inclusive strategy needed to bridge it, can leave security and business teams in isolation; unaware of how the others work, what they need and how they can contribute to organizational success. At some point, an event will occur, and all sides will be forced to work together. By that time, however, they may be standing in front of the CEO, the board, a regulator, customers or the public.
CONCLUSION

Make no mistake: addressing the Gap of Grief isn’t an idea to be argued or debated—it is an urgent necessity that must be achieved. Attacks are proliferating too quickly. Attackers are growing stealthier by the day. Business processes are growing more dependent on a disaggregated IT infrastructure, with each new system or identity becoming another exploitable point of weakness. We need only to look at the news headlines to see what happens when the Gap of Grief is not bridged.

Business-Driven Security is a way of breaking the silos of security and business risk, and aligning business initiatives with security from the onset. It means regularly assessing environments to ensure all critical internal- and consumer-facing systems, processes and data are categorized and aligned to security priorities, practices and controls. It also means managing identity throughout the user lifecycle, and enabling authorized access to all business systems.

In the end, organizations who embrace a Business-Driven Security approach enable themselves to establish visibility across systems, use analytics to drive insight, orchestrate response and gain the contextual intelligence to put security details into business context.

Taken together, this ultimately means having an accurate and contextual answer when someone eventually asks, “What is the impact to the business?”


