FIGHTING THE 'GAP OF GRIEF' WITH BUSINESS-DRIVEN SECURITY

The worldwide cybersecurity spend for 2015 topped $75 billion according to research analyst firm, Gartner. Despite this level of spending, we have seen 2000 data breaches, 700 million personal records stolen, and an average financial loss of $3.5M per incident. However, the most shocking statistic is that on average organizations only know that they have been hacked less than 30% of the time.

Unfortunately, even with this significant spend on security, it's still too difficult to put security details into business context fast enough – if it can be done at all. Both security and business leaders struggle to understand to what degree security incidents can impact business continuity, intellectual property, and damage to their reputation, among other things.

The truth is, CEOs and Boards of Directors don't care about whether a breach was caused by the Angler toolkit exploiting a vulnerability in Internet Explorer. What they do care about is overall impact to the business and they need the information fast.

These details of security need to be understood and communicated in the language of business risk. The inability to do so is what we call the "gap of grief." And this gap stands in the way of being able to answer THE critical question when an incident does occur… HOW BAD IS IT?

In most organizations today, we see a distinct Gap between business leaders and security teams, essentially a disconnect with security teams absorbed in trying to determine what a cyber incident is and how fast can they stop it while the business leaders are laser focused on only the impact to the organization.

The Gap is especially poignant when an incident happens and the CEO asks, "How bad is it?"—and the security team is not entirely confident they understand the scope of the threat, or how it will impact the organization. Which, as mentioned above, is really what senior management cares about.

WHAT CAUSES THE GAP? SPOILER ALERT: LACK OF ALIGNMENT / LACK OF CONTEXT.

Let's think about how security strategies have evolved. Over the years, for security exclusion, in other words, to "keep the bad guys out", most organizations layered multiple preventative tools. We started with static, signature-based technology like firewalls, IDS/IPS, and A/V. As threats became more sophisticated, we added next-gen firewalls, sandboxes, and other "advanced threat solutions".

Most organizations did the same thing for security inclusion, or "letting the good guys in". They recognize that identity has been and still is the most consequential threat vector. So they invested in a myriad of disconnected technologies PKIs, multi-factor authentication, provisioning/deprovisioning systems, governance, and life cycle management.

The problem with this layering mentality and the "new threat, new box" strategy is that it is reacting to the threat environment vs. aligning to business processes, growth initiatives, and the organizations risk appetite. All the while creating tremendous complexity that may not even be protecting what matters most to the organization.

This patchwork of point tools is only providing information about their limited view of the environment. Finally, more technology means more alerts, but no priority; every alert is treated the same. Without context, we can't determine if anomalous activity is

malicious or benign, we can't connect a seemingly disparate series of alerts into a single attack campaign, and we can't focus right away on those alerts that may have the biggest impact on the business. Worse, alerts without context or priority means more time to investigate, which requires more advanced analysts, which the industry just doesn't have.

Everyday there are new sources of cyber risk and organizations simply don't have the visibility or the analytics they need across their environment or the contextual intelligence to answer that ever important question – how bad is it? This leaves even mature organizations without a complete understanding of how cyber plays into their enterprise risk posture.

Taken together, it has created a perfect playground for bad actors trying to get in.

Make no mistake, either: closing 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 point of weakness to be exploited. We need only to look at the news headlines to see what happens when the Gap of Grief is not closed. What could be more frustrating then having the alerts you need but not being suss through a sea of less meaningful alerts to find them or failing to connect the alerts to the business impact.

But think about what "bridging the Gap of Grief" really means: it means aligning business initiatives with security from the onset, regularly assessing environments to ensure all critical systems/processes/data are categorized and aligned to security (defeating shadow IT), establishing visibility across systems, using analytics to drive insight, orchestrating response and workflow, and critically gaining the contextual intelligence to translate impact to the business.

And ultimately being able to defeat the attacker before damage to the business or being able to answer the question "how bad is it" with confidence.

So how do we get there?

DEFINING THE MISSION OF BUSINESS-DRIVEN SECURITY

Business-driven security is the concept of creating explicit linkage between what security technology is telling you and what that means in terms of business risk.

FOUR PILLARS OF BUSINESS-DRIVEN SECURITY

A chief security officer who wants to close the Gap of Grief needs to work with the business units to achieve four steps along the way.

Full Visibility. The security team must be able to see what's happening in the enterprise at all times—across business processes, networks, devices, people, and transactions. Only with that 360-degree ability can you identify security risks across the whole business environment. Too many security monitoring strategies today have an overreliance on a single data source, (e.g., logs) that provide an incomplete picture of the organizations attack surface from the endpoint to the cloud.

Rapid Insight. Faster time-to-insight, through better analytics and detection capabilities is paramount in the modern business environment of external business partners, cloud computing, personal devices, and the like; where plenty of unusual behavior will be harmless—and plenty will not. The "time to insight" for security teams is collapsing to zero. The more time you need to interpret an event, the greater your risk can be.

Efficient, Comprehensive Response. Today, security teams take the findings from their security tools and remediate in a highly manual way that doesn't scale. The most effective way to turn insights into action is to orchestrate and automate response. When you spot a user acting suspiciously, you can enable the control plane of identity to go into action–stepping up authentication to ensure that you are confident this user is legitimate.

Business Context. The security team can't rely only on seeing what is happening on its network and among its system users; they must be able to interpret those events quickly and understand the criticality of the systems and or processes affected. This contextual intelligence facilitates faster and better decisions. If you're an analyst, understanding business context (such as the criticality of an asset) can help you determine how urgently you should escalate incidents.

Each of these four pillars must work together to effectively close the Gap of Grief. They are predicated on the security team having a keen knowledge of how the business works—of what "normal" looks like for your enterprise and what is most important. If security stays on its side of the Gap and moves ahead with its own program, you risk disconnecting the business units. If the business units stay on their side and move ahead with their plans, they can introduce new security risks you won't discover until after the attack happens.

Disregarding business-driven security—that is, not closing the Gap of Grief—simply leaves each side to breed more misunderstanding of how the other works, and more risk. At some point an adverse event *will* happen, and then both sides will be forced to unite. Except you'll be standing in front of the CEO, the board, a regulator, customers, or the public, all of them wanting to know how you "let this happen." And you will feel the grief then, too.

WHAT 'CLOSING THE GAP' MEANS

Tools alone aren't enough. Next generation security strategy requires connecting security risk and business risk that is contextual and specific to each individual organization, and it requires a whole new way of thinking.

So how can you get started? There are 6 key steps to creating a Business-Driven Security strategy:

1. Prioritize assets / processes and understand their vulnerabilities

2. Quantify business risk and impact if those assets/processes were compromised

3. Build a strategy to defend those assets with clear cost/benefit relationships outlined; make sure your strategy is holistic (people, process, technology)

4. Determine gaps between what you have in place today and your ideal state

5. Take a phased approach to addressing the gaps, but start today; prioritize according to impact on risk posture

6. Constantly inspect your environment and re-evaluate threats and vulnerabilities to tune your strategy; have a response plan in place

On a practical level, closing the Gap of Grief means much more collaboration between the security team and "the business." Exactly who qualifies as "the business" will differ from time to time, but we can sketch out a few givens: a few relationships or routines that must exist, if you want to implement business-driven security well.

First, the chief information security officer must be part of the strategic team that sets and reviews business objectives, initiatives, and priorities. Then you can align your security strategies to business operations from inception. You can determine which business systems and assets are most critical, and prioritize remediation plans and processes that will help you protect what matters most.

Many times that strategic discussion will mean talking with business operations leaders. Sometimes it will mean talking with the compliance officer, and often with the CEO or CFO to discuss cost-benefit questions. The result should be a clear sense of your security posture and what security infrastructure you will need, given the business initiatives of the organization.

Second, business-driven security must also be driven by a clear sense of exclusion *and* inclusion. To create efficiencies in business, many external organizations and contractors now need to interact with your network, and employees have to use cloud services and/or personal devices. *Identity management* forms the foundation of good security. That builds on our first point above; security teams will need to work with business units to understand how a "normal" identity behaves (even if that identity is only an IoT device) and how to assess the risk of anomalous behavior.

Business-driven security requires more beyond those basic steps, of course. We could (and will) say much more about all the nuances of how such an approach works. For now, suffice to say that today's approach of siloed solutions—call it business-agnostic security—has not kept pace with modern IT. It isn't in synch with how the business operates. That's why the Gap of Grief becomes more painful every year.

The Gap can be closed, and business-driven security is the way to close it. Then the security team can finally be a full partner with business operations and senior leaders at your enterprise, which is exactly where security belongs.

ABOUT RSA

RSA helps leading organizations around the world take command of their security posture by partnering to build and implement business-driven security strategies. With RSA's award-winning cybersecurity solutions, organizations can effectively detect and respond to advanced attacks; manage user identities and access; and reduce business risk, fraud and cybercrime. For more information, go to www.rsa.com.