Digital mayhem and digital insecurity

Why are the costs of data breaches rising despite the substantial increase in security investments?

Certainly some of it can be attributed to the rising costs of responding to breach disclosures, increased threats, and a higher priority placed on cyber-security. However, a big part of the rising cost is that too much emphasis is placed on preventing and spotting attacks, when organizations should also be developing the ability to respond when the inevitable occurs.[1]

It's as if the network perimeter has become the last line of defense — a modern-day *Maginot Line.*

Despite advances in technology and best efforts to stop them, cyber attacks are escalating and attackers are constantly introducing new threat vectors. Under the circumstances, breaches and break-ins are simply inevitable. Your adversaries have nothing but time. They also possess the element of surprise as to the timing, target, and strength of the attack.

Given these factors, the level of complacency that many executives express is concerning. In fact, every day brings news of another company that's been hacked and humbled.

Look closer and you'll typically find that these companies invested heavily in cyber-security solutions. In most cases, they actively invest in firewalls and anti-virus/malware software. However, they tend to under-invest in activities like assessing business risks and prioritizing security spending against those risks, that might more effectively secure their crown jewels — be they customer credit card data or other critical information assets.

It's as if the network perimeter has become the last line of defense — a modern-day *Maginot Line*.

To overcome these extraordinary risks and vulnerabilities, it's critical to apply a new perspective. As opposed to thinking merely in terms of defense and prevention, it's time to place much greater focus on response and resilience in moments of crisis. It's time to prioritize true business risks as opposed to merely seeking technical fixes geared to compliance box-checking.

That's why companies like yours increasingly embrace and implement cyber resilience programs. Read on to learn how you can apply the crucial principles, plans and practices necessary to protect your brand reputation and your information assets.

1 11th Annual Security Survey Whitepaper 2013, CSO Security and Risk, George V. Hulme CSO, October 16, 2013.

75%

organizations reporting losses of more than $10M per incident are up 75% from just two years ago.[2]

Trends and drivers: digital insecurity and the mounting threat to your brand

Companies are enduring more cyber-attacks than ever, according to the *11th Annual Global Information Security Survey*, conducted by PriceWaterhouseCoopers and CSO Online.

Digital security expenses are also escalating. In fact, the average losses per incident are up 23% year-over-year in the number of organizations reporting losses of more than $10 million per incident up 75% from just two years ago.

Despite the mounting attacks and losses, executives remain confident in the robustness of their security initiatives. In the survey, 84% of CEOs and 82% of CIOs contend their cyber-security programs are effective, while 78% of chief information security officers express full confidence in their existing cyber-security programs.

But the survey also strikes a cautionary tone: according to CSO, the number of security incidents detected is rising significantly year-over-year — climbing from 2,989 reported in 2012 to 3,741 in 2013. What's more, 18% of survey participants report that they are unaware of the number of incidents their organizations detected in the last year.

"The bad guys basically go where they want to go and do what they want to do, and they're not being stopped. Maybe for every one organization that's effectively stopping attacks, there are 100 that are being breached," says Eric Cowperthwaite, CISO of Providence Health and Services.[2]

Devastating cyber-security failures have received much attention in the media.

Take the case of Adobe Software. According to an October 2013 article in the New York Times, hackers gained access to credit card and personal information of Adobe's customers, including encrypted passwords. They also stole copies of the source code of some of Adobe's most popular products.[3]

While a costly response was clearly reported in the media, the long-term impact on Adobe's reputation is far from clear. In fact, the number of accounts that may have been impacted has since climbed to nearly 49 million.

2 11th Annual Security Survey Whitepaper 2013, CSO Security and Risk, George V. Hulme CSO, October 16, 2013.
3 "Adobe Announces Security Breach," New York Times, David Kocieniewski, October 3, 2013.

"When it was first revealed, Adobe apologized and offered free yearlong credit monitoring to affected customers," *TechNewsWorld* reported. "Adobe initially indicated it was unaware of any immediate threat to customers, but due to the loss of the source code, it is possible that hackers might be able to uncover and exploit weaknesses in Adobe's products."[4]

Or consider the experience of Sony. When it lost the personal information of PlayStation users several years back, the economic and reputational impact was devastating. The attack occurred between April 17 and April 19, 2011, forcing Sony to turn off the PlayStation Network on April 20. On May 4, Sony confirmed that personally identifiable information from each of the 77 million accounts appeared to have been stolen. During the week, Sony sent a letter to the US House of Representatives, answering questions and concerns about the event. In the letter Sony announced it would be providing Identity Theft insurance policies in the amount of $1 million per user of the network.

And, finally, look at the blow to Global Payments. This leader in credit card processing experienced a breach in its credit card entry systems. As a result of the breach, the company lost thousands of card numbers. Visa, meanwhile, temporarily revoked its ability to take their credit cards. Subsequently, it was forced to pay a penalty to customers in the tens of millions of dollars.

Recognizing the escalating threat associated with such events, the World Economic Forum has made Cyber Resilience a top concern to be studied and debated. The topic has even been a key theme at the organization's annual confab for government and corporate leaders in Davos, Switzerland.

The challenge clearly seems to be growing in scope and magnitude. In *Risk and Responsibility in a Hyper-connected World: Pathways to Global Cyber Resilience*, WEF argues that increasing connectivity has created increasing vulnerability. "The ability to provide a trusted environment for individuals and businesses to interact online is a critical enabler for innovation and growth," it states. "Digital transformation makes the protection and resilience of our shared digital environments a critical enabler for the economic growth of companies and countries."[5]

4 "Adobe Hack Victim Count Skyrockets to 38M," TechNewsWorld, Erika Morphy, October 31, 2013.

5 Risk and Responsibility in a Hyperconnected World — Pathways to Global Cyber Resilience, World Economic Forum, June 2012.

By assessing cyber security in a myopic, constrained, and excessively technical fashion, they remain deeply vulnerable to hackers and cyber criminals. They defend the perimeter while allowing the crown jewels to go largely unprotected.

Breakdown: checklist complacency and unforeseen consequences

Such trends and patterns create a series of issues that must be treated with deep seriousness by executive leaders. Companies now face a growing array of digital security threats — and many remain deeply vulnerable. What's their greatest source of unaddressed vulnerability?

Insufficient and incomplete understanding of business risk. Many companies are prone to something we call *Checklist Complacency.* They adopt security software that meets an array of standard criteria, yet continue to maintain an incomplete understanding of the real business risks they face.

In the absence of full risk assessment and prioritization, all risks are treated equally — and all assets remain equally vulnerable. Many organizations purchase point solutions to address one-off security issues (usually due to compliance demands) as opposed to taking an expansive look at the connections between their top business risks and digital security needs. By assessing cyber security in a myopic, constrained, and excessively technical fashion, they remain deeply vulnerable to hackers and cyber criminals. They defend the perimeter while allowing the crown jewels to go largely unprotected.

The inability to fully align security postures with business risks has two major implications:

Reputational risk. Companies face immense threats to their brands when security breaches occur — whether the issue is compromised customer information, system downtime in a high-transaction environment, or some other high profile issue.

Hard earned trust and confidence can be rapidly (perhaps irretrievably) lost. Cyber security failures happen in full view of the public and can lead to substantial damage in terms of public perceptions. In fact, high profile organizations are likely to get a great deal of unwanted press coverage in the case of an undefended cyber attack.

The bottom line is that the reputational threats are real. As the cases of Adobe, Sony and Global Payments demonstrate, corporate reputations can suffer tremendously when cyber risks are not effectively anticipated and managed.

Financial risk. When downtime occurs or customers flee, companies are destined to take a financial hit. All hands are on deck when damaging events occur and attention shifts

Ironically, board level pressures to reduce costs can actually exacerbate the risks and vulnerabilities that lead to such consequences when those risks are not properly identified and prioritized.

to security, damage control, and regulatory compliance. But the primary motivation is survival. In fact, the damage can ripple through the entire value chain, disrupting supply and demand chains as well as shareholder value.

Ironically, board level pressures to reduce costs can actually exacerbate the risks and vulnerabilities that lead to such consequences when those risks are not properly identified and prioritized. In fact, unmanaged risks and their potential consequences are far less visible than the profits made possible by minimizing cyber-security investments.

"From the board's perspective, investing in cyber-security is usually not high on the agenda of stockholder meetings," according to the report from the World Economic Forum. "The investment may be significant and, unless the company has a way to market its security capabilities, there is no immediate upside to the investment. The true value of cyber security, then, is hidden in the effects this 'unrewarded risk' may have on an organization."[6]

Why are current perspectives on cyber risk so confined and incomplete? One issue is that the consequences of cyber attacks are often hard to translate into the language of business decision makers (it transcends "security" alone). Security professionals are challenged to frame the issue of cyber risk in business terms. In fact, they often lack a framework to enable them to meet this objective because:

- Conventional frameworks typically don't connect technical solutions with high level policy concerns (around growth, shareholder value, and regulatory compliance).
- Conventional frameworks often don't provide a scorecard (beyond simple security models, e.g., ISO). You typically can't build meaningful KPIs that go beyond measuring areas of unclear relevance to the business (for example, what does it mean — in business terms — that there were x number of cyber attacks?)
- Conventional frameworks generally defy quantification in terms of business risk. After all, factors such as brand value are largely intangible.

At present, most organizations cannot intelligently prioritize business risks as they pertain to security. To do so would require them to start with the consequences of a cyber-attack (as opposed to the threat associated with an attack). **You must consider first what you want to protect and then work backwards to determine the most effective strategy for protecting the asset.**

Too often, organizations focus on compliance over effectiveness. They manage regulatory risks, but they don't protect the enterprise. Existing frameworks and checklists simply don't address critical risks in a prioritized fashion.

What's more, organizations often behave as if attackers can be thwarted with firewalls and other forms of first-line security. In fact, there's an extraordinary and excessive amount of attention placed on preventing attacks as opposed to responding to them in an agile fashion when inevitably occur. As a result, current perspectives leave organizations dangerously (and unwittingly) vulnerable.

6 Risk and Responsibility in a Hyperconnected World — Pathways to Global Cyber Resilience, World Economic Forum, June 2012.

If you look at security programs in large organizations, they probably spend 70 to 80 percent of their budget on preventative measures.[7]

Breakthrough: absorbing attacks with cyber resilience

To truly protect your organization and ensure you are fully prepared for cyber-attacks, you'll have to embrace and implement a Cyber Resilience Program (CRP).

This involves a shift in thinking and investment. Whereas current cyber-security policies tend to revolve around preventive and defensive measures (covering firewalls, anti-virus/malware detection, and end-point security), resilience requires far more focus on an agile and rapid response. It's about rigorously aligning security resources with perceived business risks to protect your assets and brand.

While cyber-mitigation strategies can reduce operational risk, the threat cannot be eliminated entirely: defenses will be breached. The ability to respond to and recover from these breaches — *Cyber Resilience* — is fundamental to risk management strategy.

Indeed, your organization will most likely encounter a cyber-attack or security breach. The question is whether you can absorb them effectively to minimize operational impact. This requires you to implement a Cyber Resilience Plan that encompasses and addresses several key factors:

1. **Business impact analysis** — identifying gaps and assessing the impact if certain events occur — prioritizing business assets and understanding the business consequences of an event.
2. **Overarching security policy** — a security foundation (sometimes with multiple tiers) that addresses business objectives and is codified and derived from experience.
3. **Comprehensive testing regime** — once the security policy is defined, ensuring adherence to that policy and applying ongoing tests, measures, and modifications (based on risk tolerance).
4. **Managed security tool implementation** — making strategic investments by building and executing a "completeness map" that links business issues to necessary tools, services, and capabilities.
5. **Cyber recovery plan** — creating response procedures, communications plans, and impact analysis processes to quickly recover and gain advantage from a cyber incident.

By addressing all these factors in a rigorous and disciplined fashion, your business will:

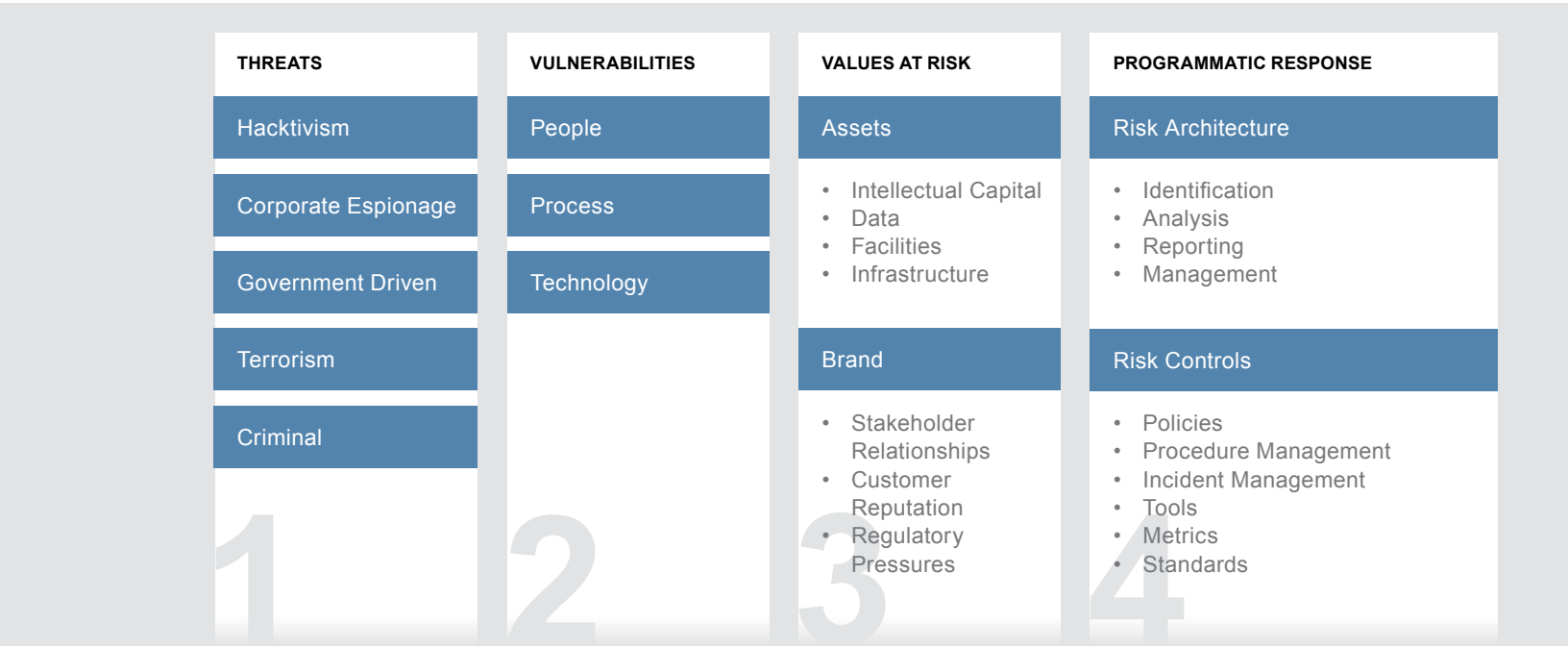
- **Intelligently deploy limited resources to protect critical assets from cyber threats.**
- **Standardize program processes to increase consistency and repeatability for security efforts across the organization.**
- **Ensure cyber-related spending is aligned with high priority business concerns for maximized ROI and targeted risk reduction.**

To achieve these results, organizations will have to shift their investments toward resilient and responsive approaches to cyber-risk management. Companies tend to be "too heavy-handed when it comes to investing in preventative controls," says Jay Leek, CISO at private equity firm The Blackstone Group. "We have not invested enough in what I call... 'response' controls. I believe that we need to focus more on how well we can identify and respond to attacks. If you look at security programs in large organizations, they probably spend 70 to 80 percent of their budget on preventative measures."[7]

7 11th Annual Security Survey Whitepaper 2013, CSO Security and Risk, George V. Hulme CSO, October 16, 2013.

A cyber-risk management framework

In *Risk and Responsibility in a Hyper-connected World*, the World Economic Forum provides a useful framework for cyber-risk management that acts as a foundation for Cyber Resilience initiatives:[8]



Identify threats. The risk framework categorizes threats into five major categories: hacktivism, criminal, government-driven, terrorism and corporate espionage. The framework intends to identify the major existing threats in order to define the most adequate and efficient approach to addressing the range of risks they present.

Identify vulnerabilities. A cyber attack usually achieves its objectives through the exploitation of one or more vulnerabilities in technology, process or human action. Cyber vulnerability may also be the result of exploitation of poor practices, such as inadequate patching of known vulnerabilities, or insecure data transmission and storage. Therefore, cyber threat education and awareness...are crucial elements for improving cyber resilience.

Determine the values at risk. Cyber threats have a wide range of potential impacts for governments, companies and individuals: denial of service, data exposure, disinformation, reputation damage and loss of trust. These damages may be summarized into two broad categories: assets and reputation.

Consider available responses to attacks. A first category of responses follows a traditional approach. This entails the adoption of policies and regulations to respond to the current cyber paradigm. A second category of responses promotes a community-based approach. This entails, for instance, the sharing of information, mutual aid or coordinated action so that every stakeholder can mitigate cyber risk and contribute to a safer cyber environment. A third category of response follows a systemic approach. This includes a new model for insuring organizations against breaches on their data held within the cloud.

8 Risk and Responsibility in a Hyperconnected World — Pathways to Global Cyber Resilience, World Economic Forum, June 2012.

Getting there from here

But enterprises also will need a plan for rolling out Cyber Resilience initiatives. Here are four proven implementation steps in rolling out a CRP:

Step One:
Define risks and determine risk appetite. In this stage, you want to define your risk categories, risk profile, risk capacity and risk appetite. By leveraging existing ERM and operational risk frameworks, you can determine your risk appetite for different cyber threats. It gets you beyond focusing on inputs and, instead, turns your attention to outcomes. This is critical because many organizations tend to over- or under-estimate their liabilities, failing to clarify the link between potential consequences and necessary investments.

Step Two:
Assess and manage risks. Here, you identify information assets that are key to the business, identify threats to those assets (including the people, process and technology that are connected to or have access to those assets), identify controls and introduce controls. You then monitor those controls continuously.

Step Three:
Define measurements. In this stage, you clarify the representative metrics that must be monitored (e.g., configuration quality, control effectiveness, security program progress) and targets to be met.

Step Four:
Measure progress and communicate results. Noting that 100% security is unaffordable, the investment should be focused on managing, mitigating, and covering risk through a balanced and sensible approach.

This approach provides a governance structure enabling you to not only defend your company from risks, but responsively act when inevitable breaches do occur. After all, you are operating in a dynamic and volatile marketplace. New and unanticipated threats are constantly emerging. By shifting from a blanket defense to a security posture based on prioritization, agility and adaptability, you enhance risk management and strengthen your overall security.

Case Study: Implementing a Cyber Resilience Program

One Sungard Availability Services client had previously struggled to keep up with tracking threats to its IT environment. Its approach was to use conventional tools to protect the network perimeter including firewalls and anti-virus/malware software.

Despite the tremendous investment in security tools (point solutions), the company's security gaps were exploited — and the company experienced a breach in an area that hadn't been identified in prior assessments. In this case, a hacker gained control of user accounts — exposing an enormous amount of organizational data. Fortunately, the organization was able to address the issue before it went public.

But the company wasn't going to put itself in the same position again. In an effort to address its risks, the company developed a Cyber Resilience model that included a tiered approach for evaluating the consequences of web application vulnerabilities.

The organization performed the following actions:

- **Defined risk by tiering its applications to determine which consequences were more important than others.**
- **Assessed risk by developing a cyber resilience review process that would identity weaknesses in the applications.**
- **Managed risk through prioritizing the resolution of the weaknesses based on ongoing risk-based reviews and changing context and environment.**
- **Measured risk by calculating the downstream consequences of the weaknesses and created a risk rating to measure them.**
- **Tracked progress by re-measuring in preselected intervals, establishing an organizationally-accepted risk factor and a clear metric to measure progress and improvement.**

This approach enabled the organization to shift its security posture from being a reactive (with limited methods to measure security risk) to being adaptive and responsive — constantly driving towards consequence-based Cyber Resilience.

What's clear is that this is not a path to walk alone.
You want an independent perspective and an ability to draw on best practices in the risk management field. To begin exploring your opportunities in terms of Cyber Resilience, you'll want an advisor and partner you can rely on. Here are some proven criteria you can use to identify a strategic partner:

- **Deep experience in resilience and recovery.** Look for a partner that can credibly demonstrate deep experience built over years helping companies like yours respond and recover in times of crisis.
- **Expertise to extend your team and back you up.** You want a partner who can act as an extension of your existing security and IT team — one that brings deep expertise and will be available when you need guidance and support.
- **Proven process and methodologies.** You can't scale up a security strategy without a defined and rigorous process. Expect your partner to have advanced processes in terms of addressing both cyber-security and cyber-resilience.
- **Insight and guidance on appropriate tools, technologies, systems.** You'll need to invest intelligently in tools, capabilities, and solutions that addressed your prioritized business risks. Expect your partner to have a deep understanding of potential options.

With a trusted partner, you'll be in a strong position to create an executable strategy and plan that enhances your security posture. **But expect independence. Any prospective partner that forces inflexible solutions (including proprietary software or hardware schemes) on you is not acting in your best interest.** Your partner should provide reliable and unbiased guidance to earn your trust and reduce your risk.

Digital mayhem and digital insecurity

Conclusion

Addressing cyber threats through resilience and responsiveness

The potential impact on your business from cyber attacks can be devastating. While many other executives may exhibit misplaced confidence in their security solutions, it's critical to understand that your organization's financials and brand reputation may be vulnerable.

Most organizations today have attempted to tackle the cyber threat with a conventional defensive model. They've adopted tools and point solutions that meet specific requirements, demonstrating Checklist Complacency in the process.

What they have not done is align their security investments with their true business risks. In the absence of thorough assessment and prioritization, they remain deeply exposed to disastrous events — much like the high profile failures we've cited in this paper.

To address these issues, you'll need to think in terms of resilience and responsiveness, agility and adaptivity. You'll need a Cyber Resilience Program that strengthens your security posture. You'll need a risk management framework that offers a comprehensive alternative to defense-driven approaches.

Finally, you'll need a trusted and proven partner — one that understands resilience, extends the capabilities of your team, brings process-driven rigor, and provides reliable insight on the tools and capabilities you'll need to truly secure your enterprise.

Additional reading

Managing Operational Risk in the 21st Century

Lack of Operational Resilience Will Undermine Enterprise Competitiveness: A Strategy for Availability