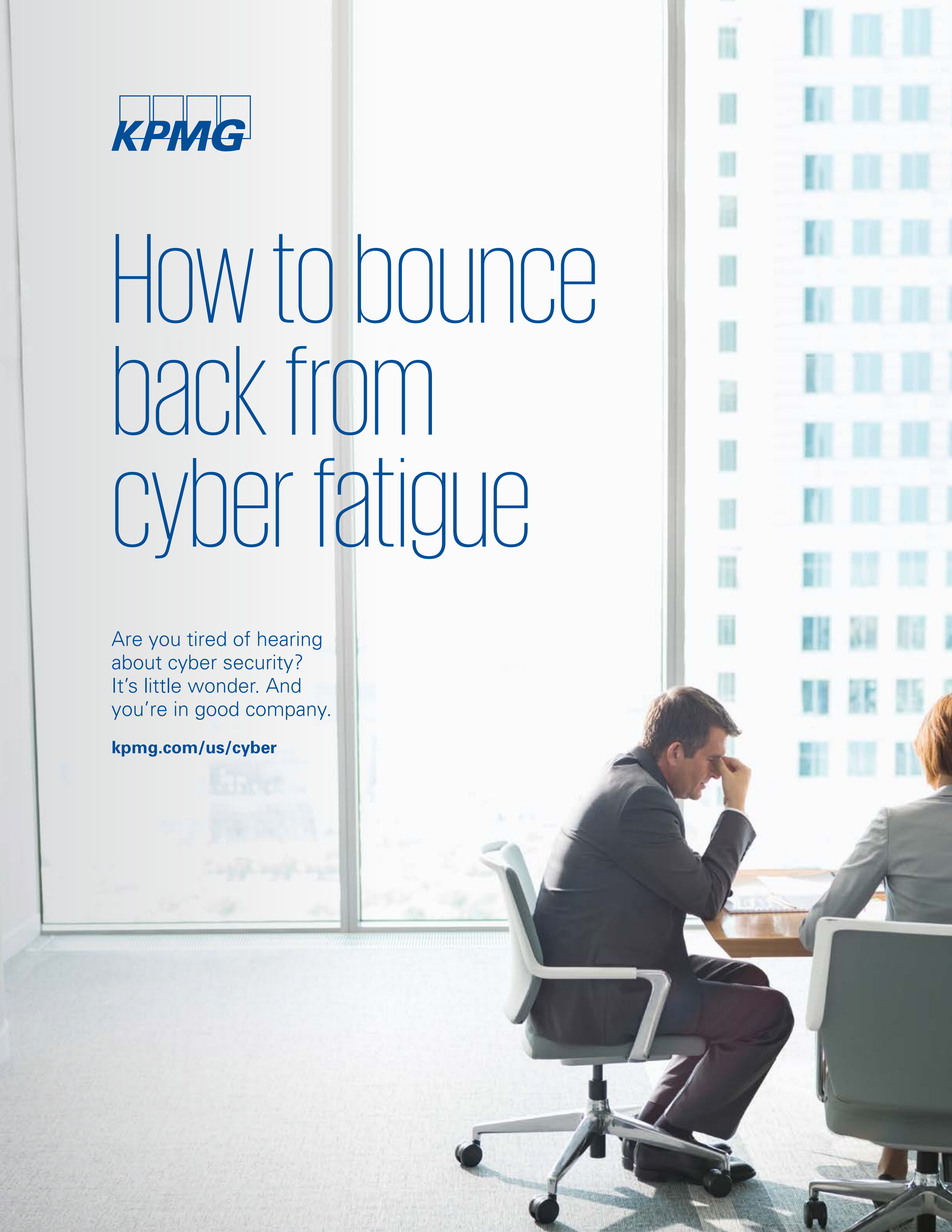
KPMG

How to bounce back from cyber fatigue

Are you tired of hearing about cyber security? It's little wonder. And you're in good company.

kpmg.com/us/cyber



There's a rising chorus of "cyber fatigue" permeating boardrooms, as cyber security is becoming understandably tiresome. This phenomenon arises at a time when avoiding negative PR is paramount for success. As IT professionals concede that a breach is no longer a matter of "if" but "when," it's a given that some decision makers are exhausted as they revisit the same discussion every year, every quarter and every month.

The high cost of cyber fatigue

Over the past several years, some of the world's largest firms and brands incurred cyber breaches that compromised data from hundreds of millions of consumers. It's an endlessly expanding roster of high-profile security failures, a cascade of vulnerabilities that have heightened the insecurities of IT professionals, who in turn have bombarded the sensibilities of boardroom executives. Their collective plea:

"We've got to do more. We've got to spend more to do more."

There's also Target's security failure that brought to bear an onslaught of corporate introspection and second-guessing. Boardroom executives across the country, when pressed yet again by IT professionals to spend more to do more, let out a collective wail:

"What's the use?!"

It's a common reaction. Not in reference to the devastating impact, but as a result of media saturation. On any given day, the headlines are replete with stories about companies, irrespective of size or technological capabilities, that have suffered security breaches. The cumulative effect has begun eroding boardroom vigilance despite the potential effect on brand confidence and income.

Stop playing the game

Moreover, let's not forget compliance. Subsequent to each headline-grabbing breach comes a barrage of finger pointing, with companies asserting compliance and regulators claiming missteps. Months later, in many cases, penalties are assessed, with companies indeed discovering procedural lapses. At the same time, regulators then enhance existing compliance standards, a tacit admission that the status quo has become insufficient to evolving hacking tactics. The game goes on, requiring ever-increasing compliance costs. Corporate executives want to know:

"Is there an end in sight?"

When looking at the costs of data breaches as an indication—we say, not for a long while.

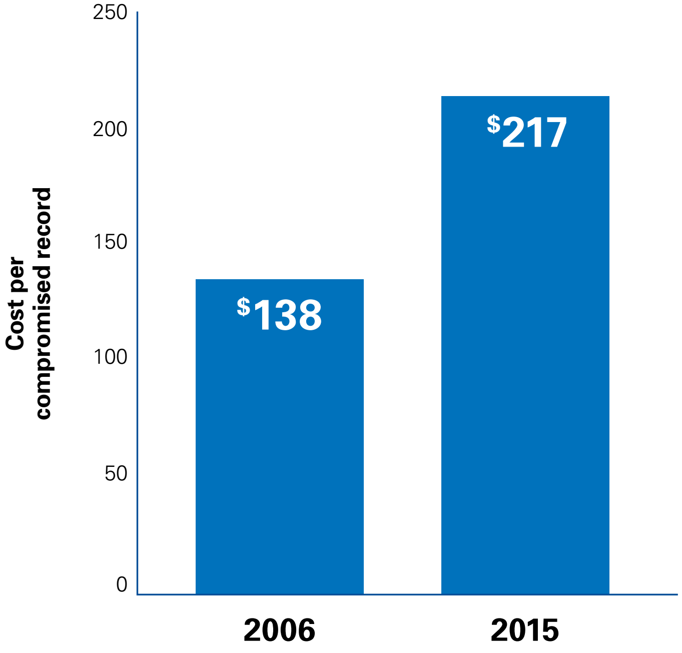
Are you experiencing symptoms?

A few indicators that your organization may be experiencing cyber fatigue would include:

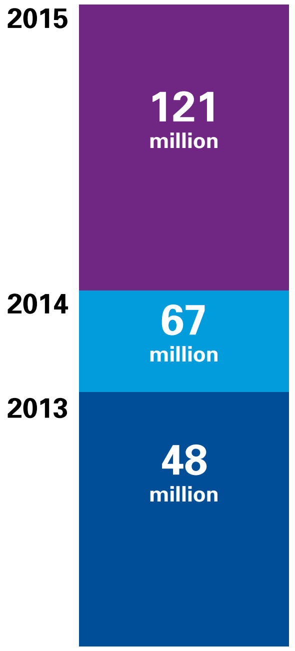
1. Double-digit, compound annual growth rate (CAGR) in cyber budgets over the last five years
2. Ever-increasing depth and breadth of executive and board briefings on cyber issues
3. Continual net addition of cyber-related technologies — with few, if any, being retired.

Data breach costs are rising

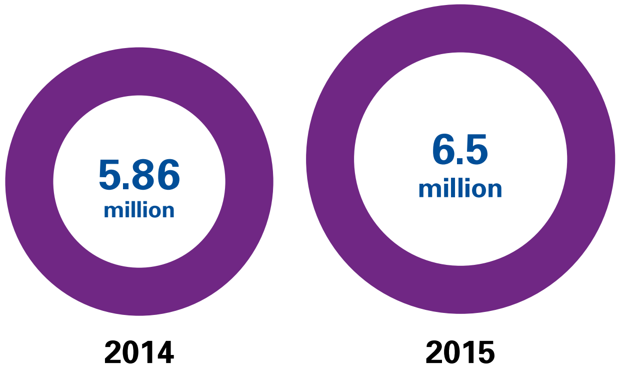
Data breach costs continue to rise-up 57% over the past decade[1]



The number of compromised consumer records continues to grow[2]



Across all companies the average total cost rose 11%



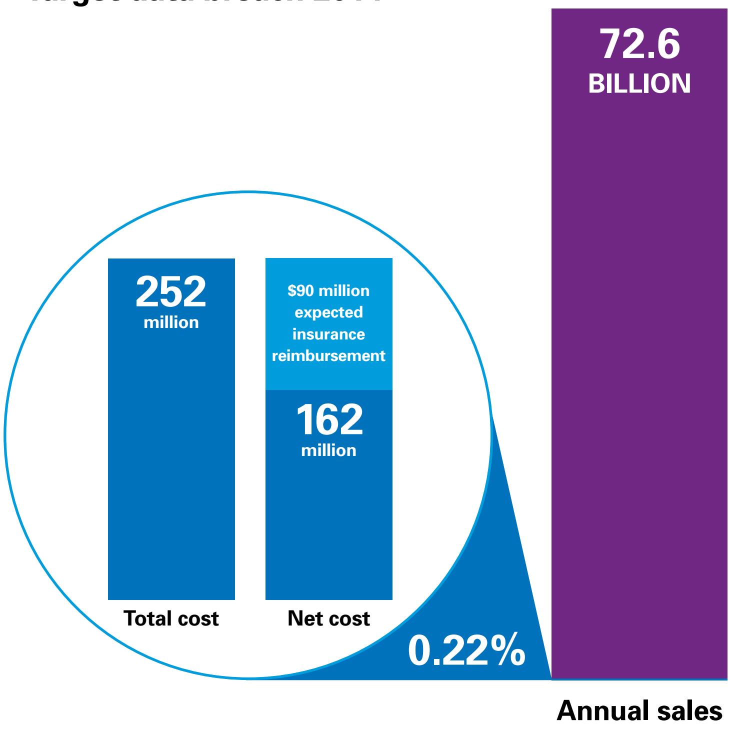
When one examines the case of Target and others, the financial impact deserves additional context. The loss represents less than one-quarter of one percent (0.22%). And that's before taking into account tax deductions commensurate with the breach.

It's a bottom-line metric that is causing corporate board members, when pressed by their CIO to buttress cyber security measures, to shift their response from the reflexive, "How much?" to the more judicious, "Why?"

Boards have been hearing about the need to spend more in order to do more for several years — at least dating to the Target breach — and they want to know:

[1] Ponemon Institute 2015 Cost of Data Breach Study: United States
[2] SecurityWeek.com - Data Breaches Numbers
[3] Target 2014 Annual Report
[4] Experian.com 2015 Data Breach Industry Forecast

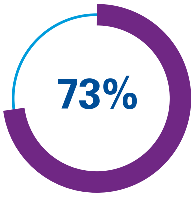
Target data breach 2014[3]



"How much should we continue to invest in this?"

Still others whose cyber fatigue has proved overwhelming are considering simply insuring the risk. At least the option presents some "finality."

There's a better way. While the majority — 73 percent[4] — of firms acknowledge that they are likely to experience a data breach, that's not an excuse for neglect, or worse, abandonment.



Align to business priorities, not tech architecture

An effective solution is not predicated on choosing either insurance or prevention, but adopting a plan that assesses the totality of a firm's cyber risk and allocates resources accordingly while adhering closely to business priorities.

Such an operational model requires a customized determination of a firm's risk tolerance and an evaluation of its true cost of cyber security.

Doing so requires answering some fundamental questions:

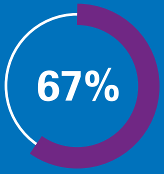
- Do you understand your risk tolerance?
- Are your programs and business model aligned with today's risk landscape in light of your risk tolerance?
- And are they future-ready, capable of evolving as the threat landscape changes?

A holistic approach to cyber security manages risk smarter and more efficiently by enabling companies to balance risk acceptance, mitigation and transfer (insurance), and in the process help maximize protection of corporate brand and reputation. Here's a holistic approach that we recommend in five steps.

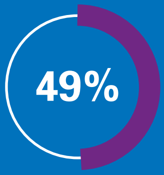
What consumers are saying

According to KPMG's 2016 *Consumer Loss Barometer: Cyber Industry Survey*[5], not all consumers are deterred by the notion of the inevitable breaches they face, whether while doing personal banking, using their mobile phone, or shopping:

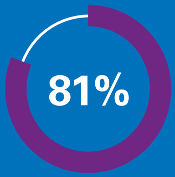
- **Banking:** In the event that a customer's personal bank disclosed a data loss from a cyber breach and then remediated the problem, two thirds (67%) of banking customers say the time and effort needed to switch banking providers is a significant contributor to their willingness to stay.



- **Mobile:** In the event a breach reveals a carrier is sharing data/ encryption technologies with the U.S. government about half (49%) would not switch carriers.



- **Retail:** In the event a big box retailer is hacked, compromising personal information, but soon thereafter addresses the security flaws, eight out of 10 surveyed (81%) would still feel comfortable shopping at that store.



From this and other research in our survey, your organization can first better determine what its customer impact would likely be in the event of a cyber incident. Next, you can obtain a rough "order of magnitude" of how much risk can be tolerated, based on:

- An evaluation of how consumers behave based on loss and the follow-up
- A comparison to the cost of current cyber program
- Consideration of overlaps in technology
- A review across the suppliers of the ecosystem

The next step would be to refine that risk tolerance picture into precise portfolio activities to help execute a broader cyber risk management program.

Remember to treat it like any other business risk — it depends on your appetite and needs to have the right approach and discipline to help stay protected.

[5] 2016 *Consumer Loss Barometer: Cyber Industry Survey*, KPMG LLP, surveying 750 U.S. consumers. This report is based on two separate surveys: one for businesses and another for consumers. The surveys were authored by KPMG and fielded by Forbes Insights.

5 ways to combat cyber fatigue

Our approach is industry-agnostic and incorporates a systematic, risk-based process. Such an emphasis steers attention from the never-ending appeal for resources and redirects it to an objective assessment that reflects a company's business strategies and innovation, risk tolerance, and unique cyber security costs. The five-pronged approach to combat cyber fatigue includes the following:

Let's take a closer look.

1. Make measured investments in cyber capabilities based on risk
2. Regularly measure the effectiveness of your security investments
3. Develop/align the right cyber risk management model
4. Continually update your model to reflect emerging threats
5. Build/promote risk-aligned security organization

5 ways to combat cyber fatigue

1 Make measured investments in cyber capabilities based on risk

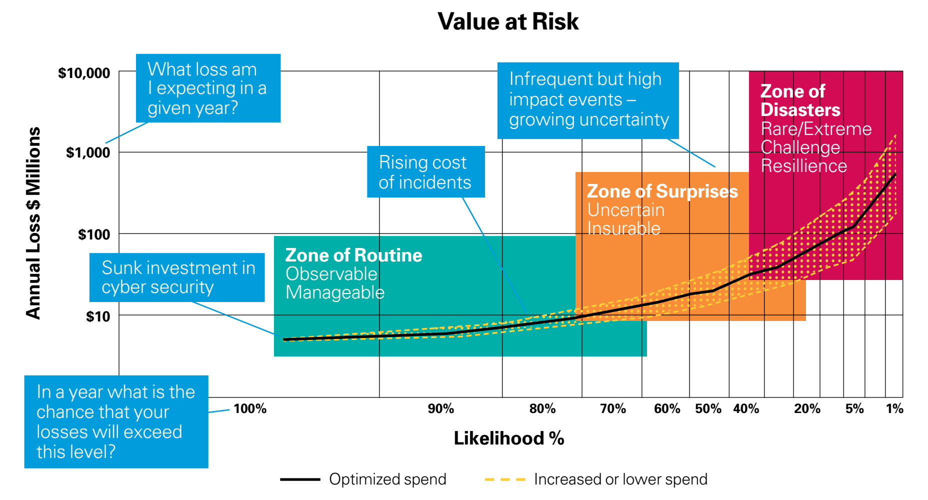
As a first step in the process, we must quantify the risk, a unique "value at risk" calculation that incorporates breach likelihood (recall: the IT professional has conceded that a cyber breach is a matter of when, not if) and its corresponding business impact. These risks must be viewed through the lenses of cyber threat to business objectives: How does a cyber threat actor interrupt or prevent the achievement of core business goals, such as capitalizing on megatrends, adopting new digital channels, or overseas expansion? Simultaneously, consider which assets are most critical to enabling these business objectives and evaluate the cyber threat landscape for risks to these key, crown-jewel assets.

The inverse relationship bears close scrutiny as it illuminates both common, expected risks — those that are observable and manageable — as well as those that occur less frequently — high impact events with growing uncertainty — that test a firm's resiliency. [See figure 1.]

Once the risk is quantified, link decision-making to the amount of risk that the enterprise is willing to assume. For those whose brand reputation is fragile and unable to sustain a sizable interruption, decisions will reflect a risk view that places value firmly in a manageable zone of routine, where losses are minimal and predictable. Some may be able to assume more elevated risk profiles, either those tied to surprises that may be insurable, while others may be able to withstand disasters — extreme events that, though rare, inflict maximum loss.

Finally, once the firm quantifies risk and makes decisions about its risk tolerance, it should pursue programs that accommodate those perspectives, modifying existing initiatives while undertaking new ones in an ongoing effort to mitigate vulnerabilities. For example, a company seeking to expand via acquisition may need to focus on building quickly-extensible IT services, including security capabilities designed to be consumed across a number of different platforms, mitigating the risk incurred by a new division's people and technology. Conversely, a company planning a series of divestitures should be focusing security efforts on identifying sensitive data assets and the capability to restrict access quickly following the separation.

FIGURE 1



Source: KPMG LLP, 2016

5 ways to combat cyber fatigue

2 Regularly measure the effectiveness of your security investments

Most companies do not fully understand the full amount that they spend on cyber security. It's not that they are unwilling to determine that cost; rather, the process is fraught with complexities, making it impractical for many to complete the process with sufficient precision. As a result, they are unable to produce an operating model that mitigates risk while optimizing cost.

The true and total security cost includes those elements that are easy to tally, such as hardware and software components — as well as those less tangible elements, such as those tied to one's third-party contracts (IT hosting, supply chain services), labor, regulatory compliance, vendor and supplier management, among others. The latter are far more difficult to uncover and tally, particularly in complex sourcing arrangements. For instance, is a patching service level agreement with an outsourcer a component of the security program? What about the cost incurred by vendors to comply with controls required in third-party risk programs?

A complete and detailed capabilities model is required at this stage in the process, defining what will count as a comprehensive analysis across every phase of operations, delivering complete transparency into a firm's current allocation of resources and a plan of action tied directly to risk tolerance. These capabilities, when tied to the risks they mitigate, enable a comparison of dollar value at risk to cost of protection. These analyses often depend on the use of unbiased and independent third parties, as the results may point towards a drop in spend with some suppliers or even refocused or reduced headcount.

Finally, the assessment is more than a one-and-done proposition and must be conducted regularly in order to provide accurate insights.

Training Day

While change management by its very nature demands additional training of personnel, when it comes to cyber security, hands-on experience is the most effective way to facilitate adoption across the enterprise. In particular as data breach scenarios can be complex, we frequently take our clients through "tabletop exercises" that simulate cyber incidents and prompt a genuine response. Such an approach provokes a deeper consideration of the implications that accompany a breach while helping employees identify gaps and areas that need improvement.

3 Develop/align the right cyber risk management model

Once you understand your cyber assets and how they are managed, begin structuring an effective cyber risk management model, one that incorporates fundamental cyber security practices as well as your risk tolerance, all in an effort to maximize your investment. It would make sense to align this to your larger enterprise risk management framework to help ensure consistency in measuring and reporting risks. At this stage, ensure that all stakeholders understand that risks exist — and will exist. As an organization, what is needed is a process to manage the risks and clearly understand the residual risks. This process really helps ensure that all the security investments are tightly coupled with risk mitigation, and there is a way to manage or recalibrate them on an ongoing basis.

5 ways to combat cyber fatigue

4 Continually update your model to reflect emerging threats

Cyber security is an elusive target, an ongoing challenge that mandates continual vigilance. At the same time, rest assured that, like fraud, cyber security is addressable and manageable. To do so requires modifying your corporate mindset away from "fix, fix, fix" — an entirely reactive process that will never adequately protect your assets. Instead, accept that it is a systematic business issue that will need ongoing funding to address, adding new capabilities as the need arises. Such an approach shifts the focus from a technology spend and instead repositions it as an innovation spend, a more practical characterization that facilitates corporate growth and the ability for it to evolve fluidly as business models dictate.

Also, consider your assets in the broader context of your business and its true cost of security services to protect them, allocating resources intelligently — efficiently — based on that analysis, keeping in mind that the allocation will change as your business evolves and grows.

5 Build/promote risk-aligned security organization

In addition to the systemic changes around identifying, measuring and managing cyber risks, one of the important but often overlooked aspects is building and continually developing a risk-aligned culture in the security and larger organization. This often entails a transformation that would shift the focus from security projects and activities to risk mitigation initiatives. These transformations are successful only if cybersecurity is elevated as a strategic priority and a top-down focus is established on managing cyber risks through the security program. Any initiative undertaken in the security area needs to be aligned with a risk which is tied to a threat and crown jewel/business driver. Many organizations take this as an opportunity to do a skill analysis of their security teams in order to evaluate readiness to adopt and align with this model.

Case study

A global CPG company engaged KPMG to perform a cyber assessment of its operations. After developing a list of priority issues for the client, the company agreed to allocate roughly $20 million annually to address. We followed up with them two years later to monitor their progress, discovering that the firm continued to budget for the list of issues highlighted two years earlier. We instructed them to reprioritize the list each year based on their current state of operations.

What does good look like?

Cyber security requires ongoing vigilance and a continual refinement of business operations.

Start with what matters to the business

Ensure traceability at all stages back to the business drivers

Fully integrate strategy, execution and operations

Perform intelligent risk management, ensuring decisions are made consciously

Employ a disciplined change management process to ensure all aspects of capability are defined

Develop a comprehensive model that supports all aspects of cyber security capabilities

Feedback loop: Adapt as circumstances change

Conclusion: From cyber-weary to cyber-energized

So you're tired of hearing the "same old, same old" request from IT? And only to learn that your efforts, no matter how well-intentioned, are essentially futile?

A breach — *breaches* — will occur.

Previously, you reacted reflexively:

"We need to spend more, more, more."

"Again, and again, and again."

The drumbeat goes on.

So how much *is* enough? What is the best remedy?

We believe what you actually need is a more intelligent way to address cyber security while reversing your restless devolution into cyber fatigue. Rather than resolving to just the mantras of "fix, fix, fix" and "spend, spend, spend," the prudent executive will implement a new model that helps maximize the value of security investments — balancing risk acceptance, mitigation and transfer with the protection of a firm's assets. It's the difference of transforming your business strategy from one that's draining and reactive to one that's energized and proactive.

Balancing risk acceptance, mitigation and transfer with the protection of a firm's assets

Author biographies

Gavin Mead

Gavin is a Principal in KPMG LLP's (KPMG) Atlanta office. He has led and executed projects around the world and cross-sector, spanning cyber strategy, identity management, large-scale technology transformation, GRC enablement, third-party risk assurance, and global incident response.

Tony Buffomante

Tony is a Principal in KPMG LLP's (KPMG) Chicago office. He is the firm's US Cyber Security Services Leader; and over the course of his career, has led cyber security assessments, strategies and implementations for the largest global organizations across industry sectors.

Contact

KPMG AG	**Roman Haltinner**	**Marc Bieri**	**Gerben Schreurs**	**Matthias Bossardt**
Badenerstrasse 172	Director	Director	Partner	Partner
PO Box	Cyber Security	Cyber Security	Cyber Security	Head of Cyber Security
CH-8036 Zurich				
	+41 58 249 42 56	+41 58 249 64 05	+41 58 249 48 29	+41 58 249 36 98
kpmg.com	rhaltinner@kpmg.com	marcbieri@kpmg.com	gschreurs1@kpmg.com	mbossardt@kpmg.com

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received, or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation. The scope of any potential collaboration with audit clients is defined by regulatory requirements governing auditor independence.