What Are You Doing to Keep My Data Safe?

Cyber Fatigue and the Growing Divide Between Customer Expectations and Corporate Data Protection

Orson Lucas CISA, CRISC, CIPP, MSc

Consumers are becoming increasingly savvy and aware of the sensitivity of their data, underscored by numerous high profile data breaches over the past 5–10 years. With this increased awareness has come an implicit expectation that companies with whom they do business and whose services they consume are good stewards of this data and provide adequate protection. At the same time, in many industries there is a growing sense of cyber fatigue (appetite for seemingly perpetual growth in cybersecurity spending with little demonstrable direct return on investment). This article will explore the dichotomy between intrinsic consumer expectations and concerns around protection of their data and corporate investment trends around cybersecurity, with the objective of outlining a risk-based approach to prioritization of cyber risk mitigation.

O. Lucas, CISA, CRISC, CIPP, MSc
is a Managing Director with KPMG LLP's Cyber Services practice.
olucas@kpmg.com

Introduction

Data is being created at a volume unparalleled in human history. The explosion of new technology and digital media such as smart phones and tablets has led to an exponential rise in the amount of data generated. In fact, IBM has estimated that by 2020 Web sites, smart phones, and sensors that comprise in part the Internet of Things will generate 44 zetabytes of data ([NYT16]). Because the collection and use of data has become so pervasive, many consumers simply assume that it will be protected from loss, damage or unauthorized exposure (often, even at a level higher than they themselves would protect the data).

This is one of the reasons that data breaches get as much publicity as they do – beyond the sensationalistic news stories, data breaches represent an implicit (and sometimes) explicit "breach" of trust between the business and its customers. Once lost, this trust can be difficult to rebuild and often requires a number of years, many millions of dollars, potentially senior leadership changes, and increased regulatory scrutiny for a period of time.

At the same time, there has been a substantial downgrade in security spending by companies across industries over the past several years: 49% of business respondents in KPMG's 2016 Consumer Loss Barometer said they did not use capital funds to invest in Cybersecurity during the last 12 months ([KPMG16]).

Because cybersecurity is a risk-based discipline and is very difficult for many security leaders to effectively tie spending back to either a return on investment or a tangible risk mitigation, there is a growing sense of unrest and frustration at the executive level that money spent to reduce cyber risk may be a misplaced investment. As will be demonstrated in this article though, while there may be opportunities for companies to be more thoughtful on the way they leverage limited resources around cybersecurity (spending and human resources), those that scale back investment in cybersecurity infrastructure, resources, and governance may do so at their own peril.

Evolving Customer Demands and Expectations

In today's connected society, consumers are socially-empowered, tech-savvy, connected, and mobile. Consumers have either adapted their lifestyles to modern technology or were simply born into the digitally connected world. Nowhere is this more apparent than in the realms of social media, mobile and the Internet of Things.

Social Media

Today's consumer uses social media sites as a means to interact with other people, share pictures and files, consume news, listen to music, and research and purchase products. This interaction with other people lulls consumers into a false sense of security. "Everyone is connected," so it is a reasonable thing to do.

That said, approximately 64% of consumers reported that they are concerned that their social media platform will be hacked, and consumers also reported that they would switch their social media provider if their social media account was hacked provided that an option existed ([KPMG16]). Yet, 43% of consumers reported accepting friend requests from others who they do not know ([Forr16]). This behavior clearly demonstrates that the consumer does not fully understand the risks associated with this technology.

Mobile

In today's world there is also a need for consumers to be mobile which has resulted in the expectation of public Wi-Fi connections in public areas such as airports, restaurants, and hotels. Approximately 68% of consumers are concerned that personal information may be stolen while using a public Wi-Fi network ([KPMG16]). Consumers expect the provider of the public connection to provide a secure connection, which means a password-protected connection. Nevertheless, with the need to be connected, consumers will connect to unsecure, public Wi-Fi connections. After all, others are connected so it must be okay.

Internet of Things (IoT)

As the IoT market evolves and competition increases, the IoT consumer will be more concerned with cybersecurity. With the rapid speed-to-market of some of these products, consumers need to understand and trust that the IoT companies are securing not only the devices but the infrastructure and that the data that is being collected and analyzed is protected. Consumer trust should be a result of the IoT provider's ability to secure its ecosystem rather than the result of brand dominance. Consumers reported that 61% would use more IoT devices if they had greater confidence in the IoT ecosystem's security ([KPMG16]).

Defining the Consumer

- **Connected** – Twitter, Facebook, Pinterest, & Snapchat
- **Conscious** – socially, ethically, & environmentally aware
- **Empowered** – many outlets to express their opinion
- **Individual** – expect a personalized experience
- **Vulnerable** – more exposed to risk
- **Informed** – unlimited information at their fingertips & are constantly looking for more

Forgive and Forget?

Over 60% of consumers are concerned that use of social media, mobile apps, or interconnected products will be hacked exposing their information. Nevertheless, consumers may be willing to forgive and forget provided

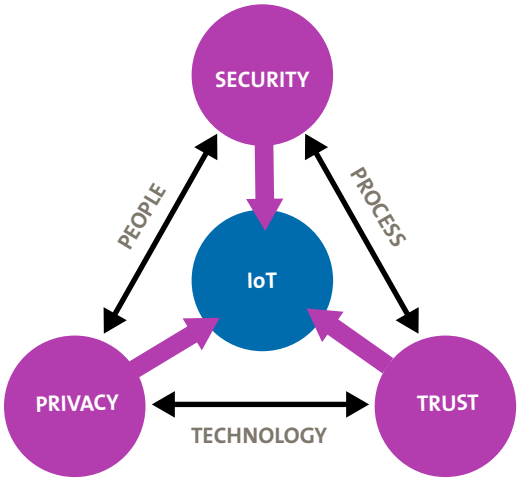

Figure 1. **IoT core components.**

IT and information security leaders still struggle to effectively communicate cybersecurity risks

companies cover losses promptly, communicate the breach transparently, and demonstrate that proactive steps are being taken to prevent future security breaches ([KPMG16]). According to KPMG ([KPMG16]), while most consumers acutely feel the sting of a data breach, 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. Additionally, 82% of consumers would not pay moderately more to switch to a provider that guaranteed it would not collect their PII, even if their current provider suffered a breach.
- *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.

This insight and similar research should directly factor into cybersecurity risk modeling and risk-driven decision making by Information Security and business executives.

The Evolution of Corporate Cybersecurity and Onset of Cyber Fatigue

Board members and senior executives are under a constant barrage of information from internal parties (IT and information security leadership), peers, and news sources about the complexity of cybersecurity threats. While this focus is in many cases well-founded, there has undoubtedly been a pendulum shift over the past several years as audit committees, board members, and CEOs seek to avoid becoming the next major breach (and perform appropriate due diligence to help alleviate concerns around personal liability). In fact,

- 88% of Boards say that their strategic risk register includes a cybersecurity risk category ([GOVU16]).
- 74% of Audit Committees plan to devote more or significantly more agenda time to cybersecurity, including data privacy and protection of intellectual property. 55% of Audit Committees think more agenda time should be devoted to cybersecurity ([KPMG15a]).
- 29% of CEOs list cybersecurity as the issue that has the biggest impact on their company today ([KPMG15b]).

Despite the attention cybersecurity risk is receiving right now, many IT and information security leaders still struggle to effectively communicate cybersecurity risks in clear and concise business terms, in a way that is easily digestible by executive management. For example, it is not an uncommon practice for a Chief Information Officer (CIO) to present to the audit committee and provide assurance around the company's security posture as conveyed through the fact that a new Intrusion Prevention System (IPS) has been purchased and installed, or that the number of systems missing patches has dropped by X%. This disconnect in the ability to effectively assess and articulate cybersecurity risk has resulted in many cases in a growing sense of cyber fatigue.

Though by no means a comprehensive list, several common indicators of cyber fatigue include:

- Consistent, year-over-year double-digit, compound annual growth in cyber budgets over the last five years with limited results
- Ever-increasing depth and breadth of executive and board briefings on cyber issues
- Continual net addition of cyber-related technologies – with few, if any, being retired
- Frustration with a lack of clear correlation between cybersecurity spending and risk reduction

What Does This Dichotomy Mean for Businesses and Consumers?

The simple fact that such a high percentage of consumers recognize loss or exposure of their sensitive information as an area of concern support the fact that this topic remains top of mind, even where there may be a disconnect between concern and behavior. At the same time, though spending on cyber initiatives by companies has grown steadily over the past few years, a growing sense of cyber fatigue may result in budgets being slashed indiscriminately, which increases the likelihood of unauthorized exposure or access to this information by employees, third parties, or external threat actors. While the majority – 73 percent ([Expe15]) – of companies acknowledge that they *are likely to experience* a data breach, this is not an excuse for neglect or, worse, abandonment.

Common Pitfall	Description
Treating security as a solely technical challenge.	**Myth:** "Because information protection is a technical problem, it demands a technical solution." **Reality:** All investments should be clearly and demonstrably aligned to the company's mission, charter, culture, and values. When cybersecurity is a square peg in a round hole, it often results in well-intentioned users circumventing established processes and controls to complete assigned responsibilities efficiently. Further, solutions that are only technical in nature often fall flat and miss their objectives. True risk mitigation in this space requires a mix of resources, defined process and workflow, governance, and technology enablement.
Security is something the IT department inflicts on me.	**Myth:** "Security is the responsibility of IT. It often causes headaches, but I fail to see the real value." **Reality:** Business process and functional leaders are ultimately accountable for appropriate protection and handling of data, and security is a tool at their disposal to help enable and drive consistency around this. Toward that end, it is important to fully integrate strategy, execution, and operations in an effective cybersecurity program design.
Over (or under) estimating cyber risks.	**Myth:** "Cybersecurity risk is the most important risk our company faces." (Or alternately, "This whole 'Cyber' thing is really overblown.") **Reality:** Many business executives do not fully comprehend risk exposure associated with the loss or exposure of data. All companies should perform intelligent risk management, ensuring decisions are made consciously.
Shipwrecks from product vendor siren songs – especially with smaller and medium-sized businesses, there is a tendency to "do" security (buy a tool, "set it and forget it").	**Myth:** "If I buy __ appliance, we will be secure." **Reality:** There is no single formula that works for all companies. Information security leadership must evaluate what will work most effectively within the context of business and regulatory drivers. Further, feedback loops must be established to help companies adapt as circumstances change, which they inevitably will.

Table 1. **Common security pitfalls.**

What Should Business Leaders Do to Stay Ahead of the Curve?

Cybersecurity requires ongoing vigilance and a continual refinement of business operations. Table 1 describes some common mistakes.

Ultimately, information security and business leaders need to focus on a practical, risk-based approach to information security that helps to ensure limited resources (both people and spending) are allocated as efficiently and effectively as possible. There are seven key things that companies should strongly consider when developing or transforming their cybersecurity program into a risk-based, customer-centric model to avoid common mistakes such as those above:

1. *Listen to the voice of the customer.* Begin with a customer-centric perspective, which can help to both build trust and rapport with your customer base, and help ensure more balanced security spending.
2. *Understand your data.* A risk-based approach to security investment relies on a clear understanding of what data is collected, processed, stored and transmitted internally and to third parties and customers. Furthermore, it is important to maintain this inventory on an ongoing basis based on changes to the business, technical and regulatory environment.
3. *Make measured investments in cyber capabilities based on risk.* Many organizations try to apply "one size fits all" solutions, and as a result, often drastically overinvest or underinvest in the areas of highest risk.
4. *Regularly measure the effectiveness of your security investments.* Investments in security, as with any other business discipline, must be quantified, tracked, measured and reported to stakeholders.
5. *Develop/align the right cyber risk management model.* Thoughtful consideration around a tailored cyber risk management model can substantially streamline and facilitate management of cyber risks.
6. *Continually update your model to reflect emerging threats.* The cyber threat landscape is continually changing, with threat actors continually refining their toolkits. It is important that all companies evaluate and develop controls and procedures to proactively address threats specific to their business model, geography, regulatory environment, and technology portfolio.
7. *Build and promote a risk-aligned security organization.* Security should be firmly embedded within the organizational culture, and elevated as a strategic area of focus at the executive and board level.

Additional detail about these recommended areas of focus is outlined below:

1. Listen to the voice of the customer

As the KPMG Consumer Loss Barometer has shown, you would be hard pressed to find a customer that would not express some level of concern, anxiety, or anger at the news of their sensitive personal information being exposed. However, in some cases (based on the type of data collected from customers, how the data is used, and whether it is shared with any third-party partners) the impact and exposure of an incident or breach may be lower for some customers and industry types than others.

As a business leader, you should seek to understand what the true customer impact would likely be in the event of a cyber incident. This can be done through analyst research, expert thought leadership, customer surveys, and industry

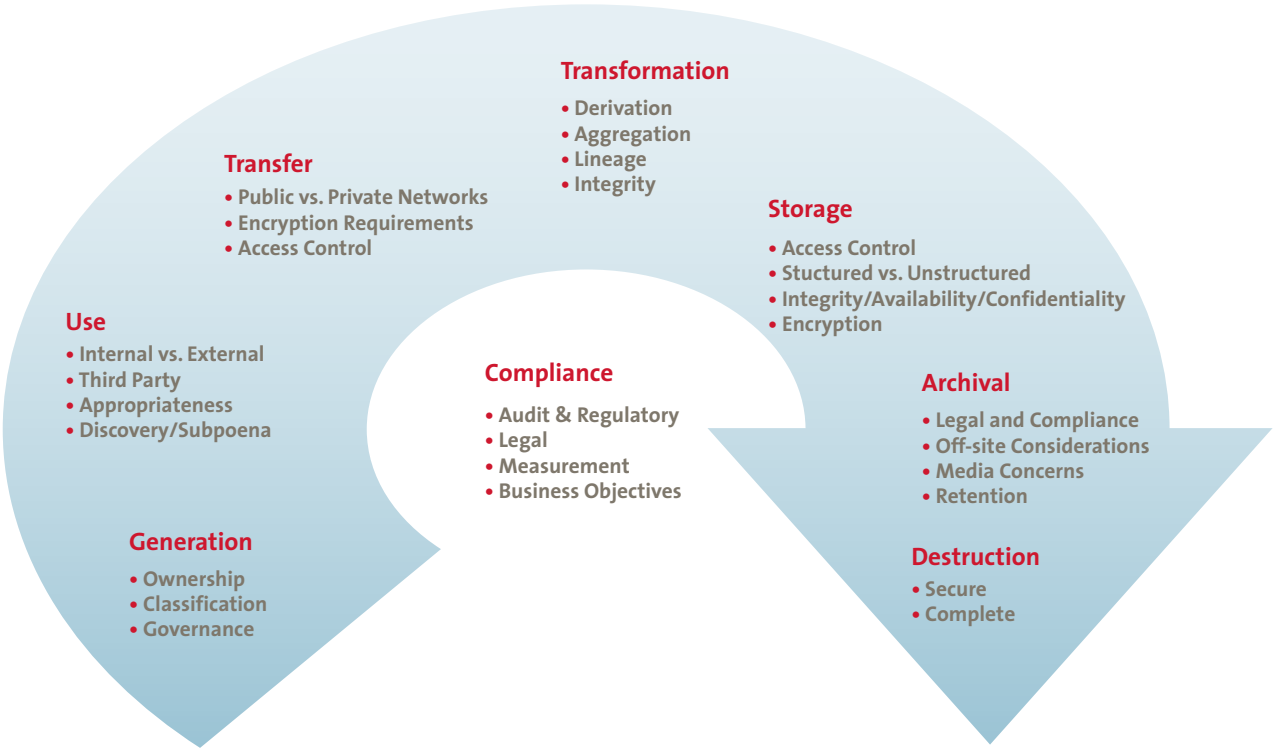

Figure 2. **Information Lifecycle Management Stages.**

peer impact for analogous incidents. This analysis should be used to drive a rough 'order of magnitude' estimate of how much risk can be tolerated, based on factors such as:

- An evaluation of how consumers behave based on the way the loss is reported, the loss itself, and the follow-up (credit monitoring, etc.)
- A comparison to the cost of current cyber program
- Consideration of overlaps in technology
- A review across the suppliers of the ecosystem.

Armed with that information, companies can drive more effective decision making, as risk treatment decisions are not made in a vacuum but with appropriate context. *Ultimately, cybersecurity risk should be treated like any other business risk, whereby risks are identified, assessed (both within an IT an organizational context), and treated to a level aligned with organizational risk tolerance.*

2. Understand your data

A clear understanding of what customer data is collected, stored, processed, shared, and retained/destroyed is fundamental to the ability to effectively protect that information. This life cycle view helps to ensure end-to-end visibility into the processes and resources that touch sensitive data and ultimately allow for granular application of controls based on determination of identified risks (see Figure 2).

Some key considerations within each life cycle stage are shown in Table 2.

Collection and maintenance of a holistic inventory of customer data instances and flows (not only in general terms, but down to the detailed system and process level) is no small feat. However, it is a required facet of an effective information categorization and classification framework and is necessary to help ensure comprehensive application of controls in the most efficient and effective way possible. Recommended steps to build and maintain such an inventory are outlined in Figure 3.

3. Make measured investments in cyber capabilities based on risk

It is critical that companies quantify cybersecurity risks. This should be accomplished using a "value at risk" calculation that incorporates breach likelihood and its corresponding business impact. These risks must be viewed through the lenses of a 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? Ultimately, this quantification is focused on helping security organizations to better articulate return on security investment (ROSI).

Companies should consider which assets are most critical to enabling core business objectives and evaluate the cyber threat landscape for risks to these key, crown-jewel assets. The inverse relationship also bears close scrutiny as it illuminates both common, expected risks – those that are observable and manageable – as well as those that occur

Stage	Description	Key Considerations
Generation	Describes creation of documents (structured) or system data, either by an internal or external party	• Ownership • Classification • Governance
Use	Describes the purpose for which sensitive data is intended	• Internal versus External • Third Party • Appropriateness • Discovery/Subpoena
Transfer	Descibes the process, controls, and implications associated with data in motion (inside and outside the company perimeter)	• Public versus Private Networks • Encryption Requirements • Access Control
Transformation	Addresses data integrity considerations related to data modification	• Derivation • Aggregation • Lineage
Storage	Refers to on-site storage of physical and/or electronic records, and the processes in place to protect information while still on-site	• Access Control • Stuctured versus Unstructured • Integrity/Availability/Confidentiality • Encryption
Archival	Refers to movement of records offsite for long-term storage	• Legal and Compliance • Off-site Considerations • Media Concerns • Retention • Cost savings (on-site versus off-site)
Destruction	Describes physical/electronic destruction of documents and files	• Secure • Complete • Retention

Table 2. **Key considerations for each information lifecycle stage.**

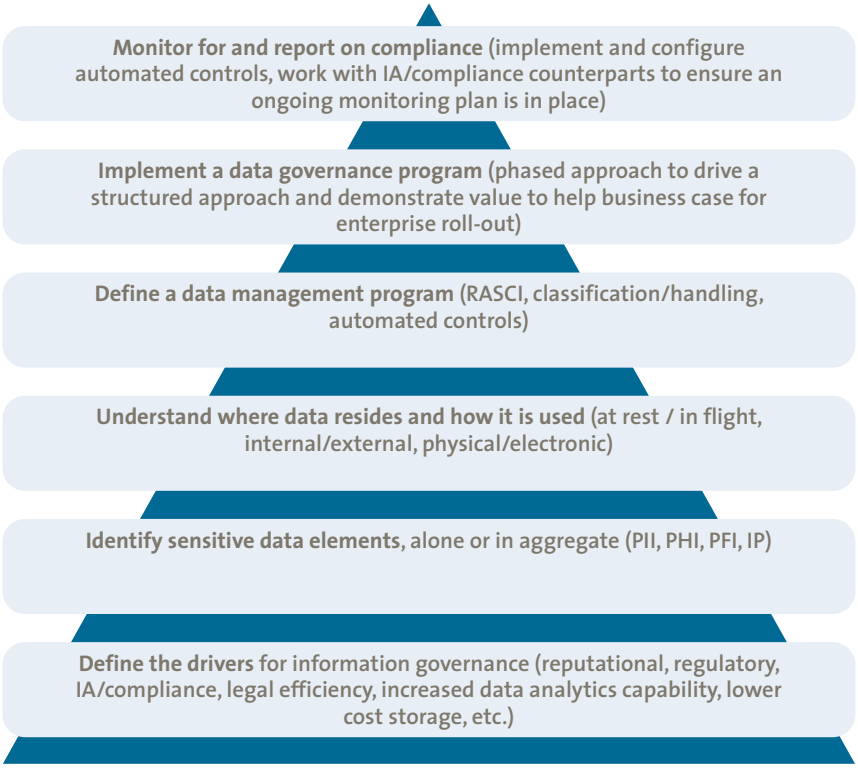

Figure 3. **Information categorization and classification approach fundamentals.**

less frequently – high impact events with growing uncertainty – that test a company's resilience.

Once risk is quantified, consider linking 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. Other companies may be able to assume more elevated risk profiles.

After the company has quantified risk and makes decisions about its risk tolerance, it should pursue programs that accommodate these 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.

Take a true, enterprise risk view of cybersecurity (prioritization within the context of other initiatives).

4. Regularly measure the effectiveness of your security investments

Most companies do not fully understand the cost of cybersecurity. It is not that they are unwilling to determine this cost, but rather that 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.

As with any investment, business leadership should challenge information security leaders to build a business case that clearly articulates and captures the value associated with proposed cyber initiatives. It is important to implement the same structure and rigor within this domain as you would apply to any other functional area within the organization. However, ultimately security is a risk-focused discipline, which means that the true value of information security is its ability to limit risk exposure to a level aligned with organizational risk tolerance.

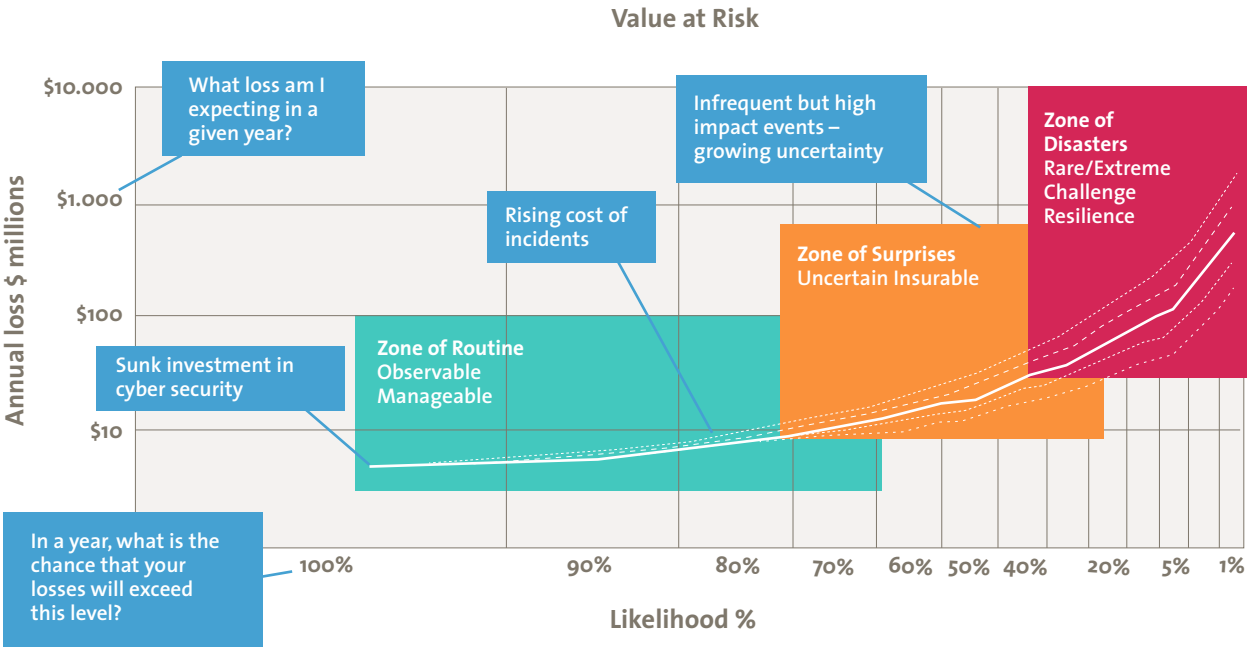

Figure 4. **Value at risk calculation.**

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 the company's third-party contracts (IT hosting, supply chain services), labor, regulatory compliance, and 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?

It is incumbent upon information security leadership to establish a clear and concise set of metrics to track, measure, and monitor both program effectiveness and improvement. The goal of the information security organization should be to establish transparency and visibility into data protection risks for the executive management team, helping to drive actionable intelligence and decision making in an appropriate context. At the end of the day, information security should be one of many tools in the executive arsenal to mitigate risk to an acceptable level.

5. Develop/align the right cyber risk management model

An effective cyber risk management model is at the heart of an effective risk mitigation strategy. Leading practice models incorporate fundamental cybersecurity practices as well as tailored organizational risk tolerance, all in an effort to maximize cyber investment.

Further, a cyber risk management model should not operate in a vacuum, but rather help to present a consolidated view of the risk factors within that domain, to be consumed and evaluated as part of a broader enterprise risk management framework. This will help to ensure both consistency in the way cyber risks are reported, as well as helping to ensure cyber risk is evaluated in an appropriate broader, organizational context. From this, critical risks (and associated initiatives) rise to the forefront and receive an appropriate level of attention, focus, and investment.

Information security leadership should work to help ensure management prioritize the concept that risks exist – and *will continue to exist*. In other words, the goal of a cyber risk management model should not be to eliminate the risk of information loss or exposure, but rather to prioritize limited resources to strike the right balance between investment and risk tolerance. This mindset can also help to ensure a proactive, ongoing approach to risk management, with risks managed and recalibrated periodically based on changes to the customer, business, regulatory, and/or technology landscapes.

Finally, 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.

6. Continually update your model to reflect emerging threats

It is critical that information security leaders and business executives stay abreast of emerging threats and trends. Cybersecurity is an elusive target that mandates continual vigilance. At the same time, rest assured that, like fraud, cybersecurity is addressable and manageable. To do so requires modifying your mindset from "fix, fix, fix" – an entirely reactive process that will never adequately protect your assets, to a more systematic, business-focused issue that will require ongoing funding to address new capabilities as the needs arise. Such a shift in mindset shifts the focus from technology spending and repositions cybersecurity as innovation spending, a more practical characterization that facilitates corporate growth and the ability for it to evolve fluidly as business models dictate.

7. Build and promote a risk-aligned security organization

In addition to the systemic changes around identifying, measuring, and managing cyber risks, another important but often overlooked aspect to effective cyber risk management is building and continually developing a risk-aligned culture within the security function, as well as the broader organization. This often entails a transformation that shifts the focus from security projects and activities to risk mitigation initiatives. These transformations are only successful 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 the readiness to adopt and align with this model.

Conclusion

An evolving, maturing set of customer expectations coupled with an increasingly complex and challenging threat landscape requires a thoughtful, risk-based approach to help ensure an effective and efficient information protection strategy. Rather than dancing to the deafening, consistent drum beat 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 is the difference between transforming your business strategy from one that is draining and reactive to one that is energized and proactive.

References

[Expe15] Experian, *2015 Second Annual Data Breach Industry Forecast*, Experian Information Solutions, Inc., 2015

[Forr16] The Forrester Wave™, Information Security Consulting Services, Q1 2016.
The Forrester Wave™ is copyrighted by Forrester Research, Inc. Forrester and Forrester Wave™ are trademarks of Forrester Research, Inc. The Forrester Wave™ is a graphical representation of Forrester's call on a market and is plotted using a detailed spreadsheet with exposed scores, weightings, and comments. Forrester does not endorse any vendor, product, or service depicted in the Forrester Wave. Information is based on best available resources. Opinions reflect judgment at the time and are subject to change.

[GOVU16] GOV.UK, *FTSE 350 Cyber Governance Health Check HM Government*, 2016.

[KPMG15a] KPMG, *Audit Committee Institute Survey 2015*, 2015.

[KPMG15b] KPMG, *2016 KPMG CEO Outlook*, 2016.

[KPMG16] KPMG, *2016 Consumer Loss Barometer: Cyber Industry Survey*, 2016.

[NYT16] The New York Times, *The Data Explosion Makes Storage Tech Exciting*, March 2016, http://www.nytimes.com/2016/03/16/technology/the-data-explosion-makes-storage-tech-exciting.html?_r=0

About the Author

O. Lucas, CISA, CRISC, CIPP, MSc is a Managing Director with KPMG LLP's Cyber Services practice focused on helping complex, global organizations to enhance the maturity of their security programs to protect their most sensitive information assets.

Disclaimer