CYBER RISK APPETITE:

Defining and Understanding Risk in the Modern Enterprise

Managing risk is a balancing act for organizations of all sizes and disciplines. While some organizations take on too much risk, others arguably do not take on enough. Complicating this equation is the emergence of cyber as one of the most impactful sources of risk in the modern enterprise. In fact, cyber security is now increasingly reviewed by corporate boards of directors and often discussed with financial analysts who see cyber security risk as an imminent and paramount business risk. Because the consequences of cyber security failures can be damaging to business revenues and brand reputation, CEOs have lost their positions as a result of data breaches and inept preparation and planning.

According to Deloitte Advisory Cyber Risk Services "the fundamental things that organizations undertake in order to drive performance and execute on their business strategies happen to also be the things that actually create cyber risk. This includes globalization, mergers and acquisitions, extension of third-party networks and relationships, outsourcing, adoption of new technologies, movement to the cloud, or mobility. And they are not going to stop doing these things any time soon. Cyber risk is an issue that exists at the intersection of business risk, regulation, and technology. Executive decision-makers should understand the nature and magnitude of those risks, consider them against the benefits a strategic shift would deliver and then make more informed decisions."

Accordingly, organizations must now factor cyber into their risk appetite and explicitly define the level of cyber risk that they are willing to accept in context of their overall risk appetite. This paper will provide a foundation for organizations looking to better understand cyber risk including; a systematic process for defining and comprehensively categorizing sources of cyber risk, a description of key stakeholders and risk owners within the organization, and finally, outline the basics of how to think about calculating cyber risk appetite.

Defining Cyber Risk

Cyber risk is commonly defined as exposure to harm or loss resulting from breaches of or attacks on information systems. However, this definition must be broadened. A better, more encompassing definition is "the potential of loss or harm related to technical infrastructure or the use of technology within an organization."

Events covered by this more comprehensive definition can be categorized in multiple ways. One is intent. Events may be the result of deliberately malicious acts, such as a hacker carrying out an attack with the aim of compromising sensitive information, but they may also be unintentional, such as user error that makes a system temporarily unavailable. Risk events may come from sources outside the organization, such as cybercriminals or supply chain partners, or sources inside the organization such as employees or contractors.

Combining these two dimensions leads us to a practical framework for inventorying and categorizing cyber risks:

- **Internal Malicious:** Deliberate acts of sabotage, theft or other malfeasance committed by employees and other insiders. For example, a disgruntled employee deleting key information before they leave the organization.
- **Internal Unintentional:** Acts leading to damage or loss stemming from human error committed by employees and other insiders. For example, in 2013, NASDAQ experienced internal technology issues that caused backup systems to fail.[1]
- **External Malicious:** The most publicized cyber risk; pre-meditated attacks from outside parties, including criminal syndicates, hacktivists and nation states. Examples include network infiltration and extraction of intellectual property, and denial-of-service (DoS) attacks that cause system availability issues, business interruptions, or interfere with the proper performance of connected devices such as medical devices or industrial systems.
- **External Unintentional:** Similar to the internal unintentional, these cause loss or damage to business, but are not deliberate. For example, a third party partner experiencing technical issues can impact system availability, as can natural disasters.

1. http://www.reuters.com/article/us-nasdaq-halt-glitch-idUSBRE97S11420130829

Over the past 15 years, we've systematically connected our economy and our society in some really powerful, compelling ways, but we've done this using technologies that were largely designed for sharing information and making it available – not for protecting that information. Very few organizations are taking into consideration what they, themselves, are doing to unintentionally magnify or create new risk. According to Deloitte Advisory Cyber Risk Services, organizations need to think of the broad swath of things that can potentially happen, but to think about what is likely to happen in their organizations given the specific things they're doing from an operational and information perspective.

Managing Cyber Risk: Who Has a Seat at the Table?

It is not just the legacy definitions of cybersecurity and cyber risk that are incomplete. The list of those responsible for securing physical and digital assets rarely extended beyond IT and physical plant management into the business, which is short-sighted given today's IT-driven, digital businesses. Chief Information Security Officers (CISOs) emerged about a decade ago, but it was not until recently that they have had regular interaction outside of IT management with executive leadership and boards of directors.

Everyone is a source of cyber risk. Public failures become personal. Personal failures become public. Even seemingly small lapses in judgment or policy oversight can have dire consequences. Over sharing on social media can reveal critical personal information that threat actors can use. Not logging out of a system at the end of the day is a wide open door to information thieves.

Underscoring that there are no unaffected parties when it comes to cyber security and managing cyber risk, stakeholders who need to shape policy include unexpected job titles. For example, software engineers and developers must ensure that new releases ship without errors that could be exploited. HR teams use Human Capital Management (HCM) software, often cloud-based, that contains employees' personal information such as social security numbers, home addresses, medical claims and other sensitive information. An enterprise's supply chain, distribution channel, partner network and similar third-parties that routinely have access systems and are often integrated, can inadvertently be a vector for cyber security failures.

Here is a starting point to identify cyber security and cyber risk influencers in the organization:

Each group needs to part of the risk management conversation and understand how they influence and impact the organizations' cyber risk posture.

Key Questions for Stakeholders:

Cybersecurity is at the top of the board room agenda today because it is well understood that cyber stakes have never been higher. The innovations and strategic advances that organizations make will continue to raise the stakes. It is not a problem that can be solved; cyber risk cannot be completely eradicated, but it can be managed to facilitate the success of a company's drive forward.

Decisions about cyber risk appetite need to be made with the business and communicated throughout the organization. It's important to understand the culture of the company and how the key stakeholders answer the following questions:

- What losses would be catastrophic?
- What can we live without and for how long?
- What information absolutely cannot fall into the wrong hands or be made public?
- What could cause personal harm to employees, customers, partners, visitors?

Creating a common risk management taxonomy and language is essential for an organization to understand cyber risk in the context of its overall objectives.

Areas of Impact from Cyber Events

The price of some cybersecurity failures can be measured in monetary units. Hard currency costs include fines, legal fees, lost productivity and mitigation, remediation, and incident response. These hard costs also include fines from lack of compliance.

Other costs are more difficult to quantify. They are qualitative and long-lasting. These include diminished brand equity, reduced goodwill, and the loss of intellectual property, all leading to a weaker market position or, in some cases, complete elimination of competitive advantage. There are third party impacts in both directions. It's possible that a third party experiences a loss event, and while unintentional, this could impact deadlines or worse reveal proprietary information. These costs that are more difficult to quantify still have large, negative impact on the business and must be accounted for.

"The notion of how to show value for cyber risk investment is one that the industry struggles with because success is invisible – it's the absence of a cyber event, or the ability to show that an event had a lesser impact than it might have had. It is difficult to show return on investment for cyber risk programs. Organizations need to develop the ability to demonstrate that the investments they are making are aligned with the actual risks they face. They have to ask if they are making the appropriate investments in security, vigilance, and resilience, and whether those decisions are based on a realistic understanding of the specific risks their organization faces – and the magnitude of impact that a cyberattack could have. Managing cyber risk is not just a cost to the business, but a positive investment to enable the success of strategic growth and performance initiatives," contributes Deloitte Advisory Cyber Risk Services.

Prioritization

Given the myriad sources of cyber risk, with each event having different levels of potential impact, prioritization is critical. Determining how and where to allocate human, financial, and technology resources is a complicated calculus. The formula includes both intangible and tangible assets, is subjective, and includes variables based on institutional comfort, priorities and governance, risk and compliance policies, regulatory obligations, and legal commitments.

A good first step is identifying and classifying applications, databases, systems, and information. A practical classification scheme (in descending order of importance) is:

1. Mission and Business Critical Systems. In aggregate, these are the vital organs of the business where the most sensitive information resides, including intellectual property, information about physical assets, and systems required to run the business. This includes information that can also impact life or death.
2. Core infrastructure, extended ecosystem. Common examples include supply chain management (SCM) applications and partner portals.
3. External, public-facing systems and points of interaction. Common examples include web servers and systems with IP addresses accessible through the internet.

While it may be counter-intuitive to prioritize internal systems as the critical area of focus, it is important to prioritize what could cause the most damage if risk is not appropriately managed. If the focus is solely on what is public and customer-facing, then the organization's most important information or critical systems are being overlooked. These mission critical and business critical systems, if affected, could halt the business entirely, which would have the same implications of a human receiving a jolt to the chest.

Deloitte Advisory Cyber Risk Services adds, "For many organizations, becoming truly resilient to cyberattacks requires more than incremental improvements. It requires organizational transformation that broadens the scope of involvement at the top of the organization and instills focus on business risk, rather than technology controls. It requires the ability to focus investments on mitigating likely outcomes, based on a broad understanding of attacker motives and the ability to anticipate high-impact scenarios."

Cyber Risk Appetite

Risk appetite is the level of tolerance that an organization has for risk. One aspect of the definition is understanding how much risk an organization is willing to tolerate, and the other is thinking about how much an organization is willing to invest or spend to manage the risk. Risk appetite sets the boundaries for prioritizing which risks need to be treated.

Cyber risk appetite should be set by the CEO, CISO and CRO and then shared throughout the organization. Calculating cyber risk through ongoing assessment using defined and proven methodologies and both quantitative metrics and qualitative risk elements is critical to an organization determining how much risk they are willing to accept to achieve specific business goals or objectives. Further, determining cyber risk appetite cannot be a point-in-time exercise. It must become an ongoing process involving constant evaluation and re-evaluation.

While it seems like setting cyber risk appetite may be just technical, there is more to it than that. There are conversations that need to include non-technical functions. Cyber risk appetite ties together operational risk, cyber risk, and enterprise risk in cross-functional conversations. The strategic conversation is about the risk that the organization is willing to take on and what controls it puts in place to prioritize cyber risk management. Setting the appetite is critical to managing the business effectively and efficiently to help an organization know where to invest time and resources.

Conclusion

The ability to quantify cyber risk and make informed decisions about cyber risk appetite will often be the difference between success and failure for modern enterprises. Those who do so effectively will be better positioned to enable continued growth, those who do not will expose their organization to risks with potential calamitous implications. Organizations must take a comprehensive inventory of potential cyber risks, quantify their potential impact, and prioritize them effectively. This process must involve stakeholders across the organization to gain perspective and consensus. It must be an ongoing process involving constant evaluation and re-evaluation. And, this up-to-date understanding must feed into the organizations view of operational and enterprise risk.

This is just the beginning of the discussion, and now that cyber risk appetite has been defined and the key players within an organization have been identified, prioritization of systems and assets is the next step. Cyber Risk Appetite is not just theoretical, but rather it is something that can be modeled and calculated by an organization. This calculus will be explored in our next paper.

About Deloitte Advisory Cyber Risk Services

As part of the market-leading Advisory practice, Deloitte Advisory's cyber risk services help complex organizations more confidently leverage advanced technologies to achieve their strategic growth, innovation and performance objectives through proactive management of the associated cyber risks. With deep experience across a broad range of industries, Deloitte Advisory's more than 3,000 cyber risk services practitioners provide advisory and implementation services, spanning executive and technical functions, to help transform legacy IT security programs into proactive, secure, vigilant and resilient cyber risk programs. Deloitte Advisory Cyber Risk Services works with our clients worldwide to better align cybersecurity investments with strategic business priorities, establish improved threat awareness and visibility, and strengthen the ability of organizations to thrive in the face of cyber incidents

About RSA

RSA provides more than 30,000 customers around the world with the essential capabilities to protect their most valuable assets from cyber risks and threats. With RSA's award-winning products, organizations effectively detect, investigate, and respond to advanced attacks; assure and manage identities; implement governance, risk, and compliance processes; and ultimately, reduce IP theft, fraud, and cybercrime. For more information, go to www.rsa.com.

RSA
www.RSA.com