CYBERSECURITY

Cyber Risk Monitoring & Management

How to Safeguard Your Brand's Integrity

Quest

WHO ARE WE?

Quest Technology Management

Quest *is a trusted name in the Technology Integration industry, with years of experience in helping customers secure their systems, applications, and environments. Our team of certified security experts can help you protect yourself and your company against cyber threats while improving your security posture. We offer our customers consulting and professional services in all security verticals, from access control and network security to cloud computing and security design.*

Security begins with awareness, and we regularly release white papers to help our customers understand common cybersecurity threats like phishing, malware, ransomware, etc., and how to implement controls to protect against them.

Contact Us Today

IN THIS ISSUE

Introduction

What is Reputation in the Context of Cybersecurity?

A Solution: Cyber Risk Management

How Cyber Risk Management Works

The Role of Continuous Monitoring

How can we help?

Introduction

We are living in the digital age where branding on the Internet and social media is crucial for businesses to stay relevant. Businesses have invested millions to build their brands on these platforms to take advantage of their reach; however, these fantastic business opportunities also bring new types of risks and challenges. One of the most dangerous risks to a business's brand and reputation is that of cyberattacks, which that can instantly damage the victim's position within the industry. The financial impacts of a cyberattack and breach are far-reaching, eventually extending to regulatory fines, reduced market share, and most importantly, a loss in customer confidence.

As a result, reputation and cybersecurity monitoring have become closely linked. In this ebook, we discuss how these two subjects intersect and what measures you can take to manage your cyber risk.

What is Reputation in the Context of Cybersecurity?

Reputation is one of a business's most essential yet intangible assets. It has become even more critical nowadays, due to the fact that news can propagate in minutes over social media. Businesses must work hard to build and maintain their brand and foster customer trust. An important part of this is assuring customers that their data is safe with you—and this is where cybersecurity comes in. As cyberattacks become increasingly common, all it takes is one successful attack for that trust to be lost, so it is crucial to protect your business and your customers' data against all threats.

To do this, companies must focus on the following areas:

- **Security:** Companies must invest in state-of-the-art cybersecurity controls to protect against new and sophisticated types of cyberattacks. Cybercriminals are using more and more advanced techniques to try and gain access to customer data. Customers have also become more tech-savvy and want assurance that their data is safe.
- **Transparency:** Additionally, companies must foster transparency and assure customers about how they maintain their cybersecurity posture. This can be done via independent certifications and attestations. When a company is transparent, its customers feel more confident that the company is doing everything it can to ensure their data remains safe.

Both of these activities foster trust and loyalty with the customer. It signals to existing and new clients that the company cares about its reputation and that cybersecurity is not an afterthought.

Neglecting either of these areas can have severe implications for the company. One example would be a large data breach that affected a popular IT company in 2020. Attackers could abuse the update mechanism to distribute their malicious code to this company's customers, which resulted in several high-profile customers—including the US government—being breached. This incident cast serious doubt on the company's overall security posture and ability to secure future updates. Their stock price also took a serious hit as investors lost confidence in the company. The incident was a media headline with long-lasting negative publicity for the company's brand that still exists to date. This incident is often cited as an example of how supply chain attacks happen.

This demonstrates how neglecting cyber risk can have profound long-term implications on a company's reputation. Due to social media, negative news about a cyber incident can spread like wildfire even if the company is able to prevent any major damage. Perception affects reality, as the saying goes, and many customers will see a failure of cybersecurity as a failure of trust.

A Solution: Cyber Risk Management

Cyber risk management is a solution to the aforementioned issues. It is an area that deals specifically with identifying, assessing, and mitigating risks to a company's brand, especially in cyberspace. A single breach can devolve into a media crisis and cause irreparable damage to a company's reputation, so cyber risk management aims to identify these issues before they occur, rather than simply being a reactive method.

Cyber risk management breaks down the impact of these issues into the following areas, each of which have their own impacts:

1. Impact on Shareholders: Cyberattacks typically lead to a direct negative impact on a company's stock prices. Shareholders may sell stock and make decisions based on the long-term damage done to a company's brand, and dividends can be held back in anticipation of the upcoming costs. While stock prices can rebound, this is not always the case, and they can remain reduced for extended periods.

2. Impact on the Company's Overall Value: A name associated with a cyberattack can result in a tarnished brand, which can impact a company's valuation. Once customers subconsciously start to associate the name with a cyberattack, it can take years for that perception to fade. The impact can also be internal—employees may want to leave the company and seek a more stable and trustworthy business.

3. Impact on the Company's Market Standing: A combination of these two issues can lead to customers moving away from a brand and to its competitors, leading to a loss in market share. This effect is not just restricted to customers—future partnerships and acquisitions can also become challenging.

Cyber risk management aims to solve these problems and bridge the gap between public relations and cybersecurity. It recognizes that cyberattack threats are not just technical, but can also have long-lasting reputational implications.

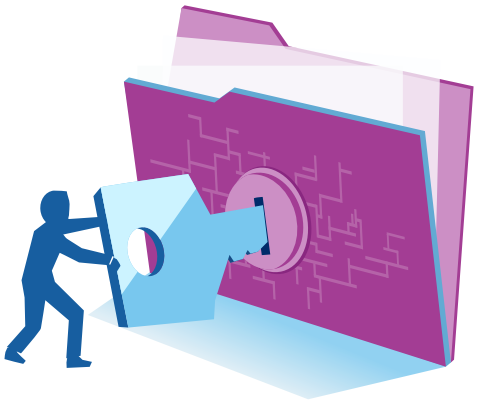
How Cyber Risk Management Works

Cyber Risk Management requires a strategic approach to identify and mitigate those issues that can harm a company's brand. It comprises a mixture of process and technical controls to work effectively. Appropriately implemented, it can be the difference between a minor incident and a full-blown media crisis.

Process Level

At this level, leadership involvement is critical for the success of the cybersecurity risk program. An executive sponsor should be present so that all stakeholders understand the importance of this program.

- **Risk Identification:** Risks to a company's brand are identified via market research, stakeholder interviews, social media monitoring, etc. At this phase, it is crucial to identify those threats that can harm a company's reputation so that efforts to mitigate them can be prioritized.



- **Risk Assessment:** Once an inventory of risks has been created, they are assessed to calculate the impact and probability of them occurring. Multiple factors, such as financial loss, brand perception, etc., are all considered to calculate the risk and prioritize which needs to be mitigated first.
- **Mitigation Strategies:** At this phase, cyber risk management focuses on developing strategies to mitigate the risks with the highest impact and likelihood of occurring. For example, these can involve developing prepared media statements to use during incidents so that no ad hoc statements are given out that can cause confusion. Protocols for internal and external media communication are also set down.
- **Training:** In this stage, stakeholders are trained on various scenarios so they are aware of what role they have to play. For instance, training can involve what sort of secure communication channels to use in case of a severe reputational crisis. It is not advised to use insecure communication when a lot of media scrutiny is present, as eavesdropping might occur.
- **Regular Review and Update:** Regularly reviewing these risks is essential to ensure they stay aligned with the business environment and the company's online presence.

Technical Levels

Once a solid process-level foundation is in place, cyber risk management focuses on putting in strong technical controls to complement these measures. They can comprise a combination of the following:

- **Media and Brand Monitoring:** These solutions track a company's presence across digital platforms and can provide alerts if the brand is mentioned. This helps the company to immediately reach out if negative brand news is being propagated. Google Alerts can be used for this, along with other commercial products.
- **Dark Web Monitoring:** Cybersecurity companies offer these services where they can glean data signals from the underground web about upcoming attacks. This can help companies put in the necessary readiness before a cyberattack and prevent any brand damage. These solutions can also inform a company if their customer details are being sold on the dark web, helping them take action before customers raise the alarm.
- **Internal Security Solutions:** Internal security solutions can be a goldmine of data that can inform companies about potential breaches and attacks from the data they collect. This feeds into the overall cyber risk management framework as a key input.
- **Internal Infrastructure Tools:** The performance and uptime of a company's products can play a large part in its reputation, as nothing quite annoys customers like unannounced downtime. These tools can immediately inform companies if a critical customer-facing system is down, allowing them to initiate business continuity plans.
- **Social Media Management Systems (SMMS):** These platforms allow companies to manage their social media presence and monitor any mentions of their brand. News can travel rapidly on these platforms, making these tools a vital part of the management framework.
- **Data Mining and Analytics Tools:** The data collected from all these sources can become overwhelming to manage, which is where data analytics and mining tools can help. These tools help to identify patterns and trends, such as public sentiment, that might not be immediately apparent. They can leverage machine learning and AI technologies to make sense of the massive amounts of data generated on social media.
- **Third-Party Monitoring:** Threats can even originate from trusted third parties, so companies must ensure they have visibility into all the third parties and service providers that have been given access within their network. This will enable them to take proactive action if any supply chain risks occur.

As shown above, cyber risk management consists of many layers at both the process and technical levels. The process layer consists of identifying risks and ensuring stakeholders know what to do, while the technical side consists of tools that help mitigate potential threats.

The Role of Continuous Monitoring

Most of the technical solutions previously mentioned have a common underlying theme: continuous monitoring. This plays a crucial role in cyber risk management, as it enables proactive response to any threats that can damage a company's brand. By enabling real-time visibility into a company's digital presence, companies can detect a minor issue before it cascades into a significant problem. This can also boost a company's reputation for being vigilant regarding its cybersecurity posture, resulting in increased customer trust and stakeholder confidence. Companies can showcase their effective response as a market differentiator and position themselves as a leader in the market when it comes to reputational risk management.

To illustrate, most of the cloud giants like AWS, Azure, Google, Salesforce, etc. provide insights into the uptime and health of their systems. This enables them to share any downtime or performance issues and demonstrate the speed of their response when such issues happen, fostering a culture of transparency.

Continuous monitoring is not just restricted to detecting and responding to threats and anomalies. It can also offer insights to companies that can be used for further improvements down the road. By taking a data-centric approach to cyber risk management, companies can justify future investments and preempt any potential threats before they materialize.

The Way Forward

In today's digital era, a single viral post or video can cause severe damage to a company's reputation and brand within the industry, making cyber risk management an absolute necessity. This framework is a powerful tool for companies to protect their reputation, demonstrate their effective risk posture to customers and stakeholders, and prevent disjointed responses when incidents occur. Implementing cyber risk management is a journey, not a destination, so all companies should begin learning about it at the earliest opportunity.

Want to learn more?

Let's have a conversation.

How can we help?®

www.questsys.com

1.800.326.4220

Quest TECHNOLOGY MANAGEMENT®