Courtesy of
FFB Insurance

Reducing Reputational Risks With Cyber Incident Response Planning

In recent years, cyber incidents have surged in both cost and frequency. That's why it's vital for businesses of all sizes and sectors to understand their digital exposures and take steps to minimize damages that may result from cyber incidents. In particular, businesses should consider their reputational risks.

After all, the way a company responds to a cyber incident can make or break its reputation. In the event of a poor response, a company may encounter various consequences—including disgruntled stakeholders, lost customers and diminished market value. Fortunately, businesses can mitigate these reputational damages through effective cyber incident response planning.

This article discusses why reputation matters, outlines how cyber incidents can lead to reputational concerns and provides response planning tips to help reduce such concerns.

Why Reputation Matters

Company brand, or reputation, refers to how a business is viewed in the eyes of others. A company's reputation is one of its most valuable assets. Businesses with good reputations are generally perceived as providing greater value than their competitors. As a result, businesses with respected reputations may benefit from more loyal customers who purchase a broad range of products and services (sometimes even at elevated prices), thus boosting profits, fueling growth and promoting operational success. In short, a company's reputation is essential to its bottom line.

In today's society, a company's brand or reputation can be affected in a number of ways. While a business can strengthen its reputation through marketing and advertisement efforts, consumers have become increasingly interested in others' personal experiences. Thus, consumers are more likely to utilize social media and online reviews when deciding which companies they trust, respect and want to give their money to. As such, it's crucial for businesses to maintain positive customer interactions and ensure their brands are adequately represented online to build good reputations.

In any case, forming a respected company brand or reputation is an ongoing effort that requires continued commitment. And while a business's reputation can take a significant amount of time and dedication to create, it can be easily damaged by a single event—such as a cyber incident.

Cyber Incidents and Reputational Damage

Cyber incidents have become a growing threat, with the majority (98%) of business leaders confirming their companies have been affected by at least one incident in the past year, according to recent research from Deloitte.

Such incidents often carry various financial ramifications. In fact, the latest data breach report from IBM and the Ponemon Institute found that the average cost of a cyber incident currently sits at more than $4 million. These expenses generally include notifying impacted parties, investigating the incident, mitigating damages and adopting cybersecurity initiatives to prevent future incidents.

In addition to such expenses, cyber incidents can also result in lasting reputational concerns, therefore exacerbating costs. According to a Forbes Insight Report, nearly half (46%) of businesses have faced reputational damages due to cyber incidents. After a company experiences a cyber incident, its stakeholders may question its digital hygiene and data protection practices. Furthermore, these parties might lose

confidence in the company's cybersecurity measures and privacy capabilities, resulting in lost funding and reduced customer loyalty. These reputational issues could be particularly prevalent among businesses that face regulatory fines or costly lawsuits stemming from how they responded (or failed to respond) to cyber incidents.

Another result of cyber incidents could be prolonged business disruptions and senior leadership adjustments, which can further fuel stakeholder dissatisfaction and distrust. Such reputational concerns could negatively impact a company's overall value and lead to diminished share prices (if applicable). This concept was evidenced by Pentland Analytics' latest report, which found that companies' market values can drop by as much as 25% in the year following a cyber incident.

Although cyber incidents can carry substantial reputational exposures, there are steps that businesses can take to minimize these risks. Primarily, it's critical for companies to create effective cyber incident response plans. With these plans in place, businesses can ensure proper responses amid a range of cyber incidents, thus minimizing potential losses and maintaining stakeholder confidence.

Creating a Cyber Incident Response Plan

Response planning can help businesses enhance their preparedness for cyber incidents and limit associated damages. In turn, companies' reputations can be upheld during incidents, demonstrating to their stakeholders that they can successfully navigate difficult circumstances. Effective cyber incident response planning requires coordination across a company. Solid response plans should outline:

- Who is part of the cyber incident response team (e.g., company executives, IT specialists, legal experts, media professionals and HR leaders)
- What roles and responsibilities each member of the response team must uphold during an incident
- What the company's key functions are and how these operations will continue throughout an incident
- How any critical workplace decisions will be made during an incident
- When and how stakeholders and the public (if necessary) should be informed of an incident
- What federal, state and local regulations the company must follow when responding to an incident (e.g., reporting protocols)
- When and how the company should seek assistance from additional parties to help recover from an incident (e.g., law enforcement and insurance professionals)
- How an incident will be investigated and what forensic activities will be leveraged to identify the cause and prevent future incidents

Cyber incident response plans should address a variety of possible scenarios and be properly communicated to all applicable parties. These plans should also be routinely evaluated to ensure effectiveness and identify ongoing security gaps.

In addition to forming effective response plans, businesses should make sure to secure adequate cyber insurance. This coverage not only offers protection against financial losses that may result from cyber incidents, but it may also provide access to additional vendors and resources (e.g., legal teams, technology experts, security software, notification centers, forensic specialists, extortion negotiators and crisis resolution professionals) that can help companies effectively respond to such incidents—therefore preventing associated reputational issues.

Conclusion

As a whole, it's clear that cyber incidents are a serious concern for all businesses, threatening both their financial and reputational stability. Yet, through effective response planning, companies can properly prepare for possible cyber incidents and significantly reduce related fallout.

For more risk management guidance, contact us today.