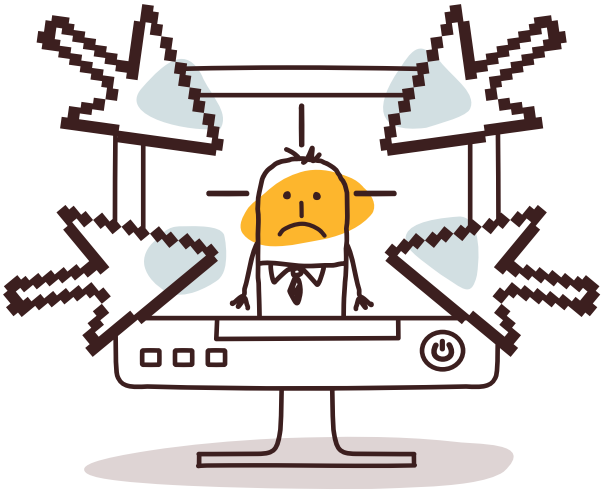
MANAGING REPUTATIONAL RISK IN THE DIGITAL AGE



A company's reputation is a measure of relative public trust and growing it is every organisation's end goal. But the digital age signals a more cautious approach.

By
KATE HOLGATE AND SIOBHAN GORMAN

It is safe to say companies with a strong reputation are trusted more than their competitors, which lowers their operating costs and increases their license to operate.

As a business grows and interacts with a larger and more diverse group of stakeholders, its reputation becomes more broad-based. Historically, this growth has tended to make a company's reputation more resilient. In the digital age, however, this broader exposure increases a company's vulnerability to catastrophic reputational risk.

Directors of companies, whether privately owned start-ups or publicly listed blue chips, are increasingly focused on their role as guardians of corporate reputation.

While the old favourites of scandal and business failure will always be on the "worry list", increasingly, data breaches are taking the top spot with boards and management teams around the world, who are justifiably concerned about the reputational risks from mishandling a breach.

See box for a check list of agenda items that directors can go through to see if their corporate reputational risk can be safeguarded.

In the wake of a string of high-profile breaches across a range of sectors in recent years, it is clear that poorly-managed cyber crises can result in enduring, profound damage.

The Worst that Can Happen

One of the takeaways these crises is that the biggest mistake companies can make is to say too much, too soon, and too confidently.

In the days immediately following a breach, no company can fully know the scope and effects of the incident. Providing too much detail early on is the first step down a road of repeated, and uncomfortable, corrections of your own story, which effectively is a "spin-cycle" erosion of your company's credibility.

Target Corp., for example, initially said 40 million customer records were affected by a breach that occurred on December 2013. A month later however, it revised that figure up to 110 million.

Similarly, Home Depot Corp. in September 2014 said 56 million customer credit card records were affected, and a month-and-a-half later, the total customer records affected came to be 109 million.

U.S. officials said in June 2015 that a hack of the Office of Personnel Management affected four million current and former federal employees, and a month later, said there were two breaches that affected nearly 22 million.

Lines of Defence

When a data breach does unfold, what rules should leadership live by?

First and foremost, focus on authenticity and customer needs. Using overly legalistic and technical language in external statements can be off-putting – especially for customers.

Show stakeholders – employees, business partners, investors, and the public – that you are investigating and managing a breach competently and confidently will help preserve your company's reputation.

That said, the best response to a reputation breach reflects thorough planning and practice. This is prudent as corporate boards are increasingly asking what management is doing to prepare for violations, even as many companies continue to punt on preparedness. At a recent computer security conference in Dallas, only a few hands – of hundreds – went up when attendees were asked if they had ever participated in a company-wide cyber security drill.

Scenario-based planning is one of the most useful actions a company can take in advance of a breach. Developing relevant and usable preparedness materials allows companies to resolve internal frictions before a crisis, address business continuity concerns, and clarify who will speak for the company.

That plan can be tested with a company-wide drill or "war game." Planning should also take into account new cybersecurity threats. Take into reference the latest risks; recent examples include the Big Data Breach, with the theft of troves of data from healthcare companies, the US Office of Personnel Management, and others.

After the deluge ends, the best next step a company can take is to immediately begin preparing for next incident. Assess strengths and weaknesses and incorporate them into your future response plan.

Corporate Reputation: A Director's Check List

In today's hyper-transparent and super-connected world, here are questions for a director to ponder over:

1. **Stakeholders:** How does the company track and engage leading representatives of the groups who can impact the company's future? Do they have what they need to act as ambassadors for the company?
2. **External profile:** How do the company's website and other traditional and digital media assets stack up against its peers? Does it proactively manage its external profile?
3. **Monitoring:** Does the company know what people think about its business, investment case and employee proposition?
4. **Business in society:** Does the business help meet a societal need and how does it demonstrate that aspect of its value?
5. **Thought leadership:** How do you help observers understand your markets and the trends you are seeing?
6. **Big risks:** Has the Board played them out and is there an effective plan in place?

Because hackers often infiltrate corporate computer systems by tricking an employee into unknowingly providing access, another sensible approach is to ingrain cybersecurity into corporate culture through a sustained, internal education campaign. The goal is to both reduce the risk of cyberattacks and ensure that employees understand the importance of the role they play protecting company computer networks. ■

Kate Holgate is the Head of Brunswick Group Singapore and Siobhan Gorman is Director of Brunswick Group Washington DC.