Avoid a Reputational Hit By Preparing Early for All-But-Inevitable Data Hacking

By Ashley McCown

What do **Zappos**, **eHarmony**, **TripAdvisor**, the **University of North Carolina**, the **Utah Department of Health** and **RSA Security** have in common? All have experienced data breaches in the last year or so.

If you are like a lot of organizations that think, "That will never happen to us," then think again:

- Most data breach victims fell prey because they were found to possess an (often easily) exploitable weakness, not because they were pre-identified for attack. (*2012 Data Breach Investigations Report*, Verizon Business)
- In a 2010 study, 46 percent of lost laptops contained confidential data, only 30 percent of those systems were encrypted, and only 10 percent had other anti-theft technologies. (*The Billion Dollar Lost Laptop Study*, Ponemon Institute and Intel Corp.)
- Through 2016, the financial impact of cyber crime will grow 10 percent per year due to the continuing discovery of new vulnerabilities. (*Gartner Top Predictions for 2012: Control Slips Away*, Gartner)
- Deliberate breaches mainly target customer-related information, primarily because it can be used for fraud. (*Internet Security Threat Report Volume 17*, Symantec)
- The average total cost per company that reported a data security breach in 2011 was $5.5 million. (*2011 Cost of a Data Breach: United States*, Ponemon Institute and Symantec)

So what do all these numbers tell us? That no sector is immune, and being hacked or having data stolen is not a matter of *if*, but *when*. The pressures on an organization when its network is compromised and personal data is accessed are overwhelming. The clock starts ticking right away and a slow, unsure response can be deadly.

Advance planning is key, and many of the communications tools you will need can be drafted in advance and fine-tuned when something happens. Although it can be difficult to make the case to budget-conscious CEOs, spending dollars up front on communications planning and training will save money in the long term and help avoid a devastating reputational hit.

No sector is immune, and having a data breach is not a matter of if, but more likely, when. The average total cost per company that reported a data security breach in 2011 was $5.5 million.

Here are five guidelines to get you started:

1. **Find an attorney before you need one.** Identify an attorney with expertise in privacy and data security and establish a relationship. He/she will guide you through all the reporting requirements specific to your industry, in the states in which you do business, and federally. They will counsel you on the potential for litigation and review all written communications. And, they can help on the front end by conducting privacy audits and risk assessments to surface potential vulnerabilities so you can address them before a hacker exposes them.
2. **Update your crisis communications plan to include protocols for reporting a data breach.** The steps to follow are specific and prescribed. Get them committed to paper now so there is no question about what to do first, second and third when a breach occurs.
3. **Draft away.** Nearly all communications materials (media statements, fact sheets, Q&As, letters to employees, customers, clients, patients) can be prepared in advance so there is something to work with when the breach occurs. The time and angst you will save by not having to start from scratch will be incredibly valuable, allowing you to frame the news rather than respond to questions from media or others.
4. **Train and practice, practice and train.** You don't want an actual breach to be the first time you put your plan to the test or the first time your crisis response team (reps from IT, HR, customer service, sales/marketing, etc.) meet and work with each other. Tabletop exercises and drills will show you which parts of your plans work well and which ones need to be retooled. And, for members of the crisis team, drills bring to light how important communication across departments is.
5. **Build a social media presence before a breach.** Depending on the scope of a breach (number of people impacted, number of states impacted, whether the data is being misused), social media can play a significant role. Some industries have blogs dedicated to tracking and dissecting how a network was hacked and how data was moved. Social media networks can light up with complaints from those affected. On the flip side, social media can be a fantastic channel to get your message out and communicate with key audiences, but only if a company has a loyal and engaged following ahead of time. It is impossible to play catch-up and try to build a strong social network once a crisis happens.

Follow these steps, and when the IT department calls to say there has been a breach, your response won't be "Houston, we have a problem." Instead, it will be, "Let's activate the plan and pull the team together." PRN

Ashley McCown is the president of Solomon McCown & Co., a Boston-based strategic communications firm specializing in crisis communications.

