WHITE PAPER

# The Criticality of Crisis Communications in a Data Breach Response Plan

## Executive Summary

Crisis communication – in the form of a carefully architected and tested plan that goes beyond an organization's security and IT groups to include all relevant business units – is essential to mitigate the impact of a data breach. The ultimate goal of a crisis communications program is to define the steps that an organization must take to convey appropriate information to every affected stakeholder – both internal and external.

Effective crisis communications can be challenging for security professionals accustomed to speaking in technical rather than business language; the need to communicate these complex issues in business terms may compound such challenges. Nevertheless, information security is clearly more than just an IT issue; it's a business imperative that requires a proactive approach to anticipating key issues, crafting responses, and mitigating cost and risk. An organization's CISO and directors must lead this process, setting the tone – and the agenda – for the rest of the organization.

This white paper will detail why a crisis communication strategy is vital for an effective data-breach response and share recommendations on creating a comprehensive crisis communications plan to mitigate impact to the organization and alleviate stakeholders concerns.

### Who Should Read This White Paper

» Board of Directors
» C-Suite
» CISO/CSO's
» Directors of Security

### What You Will Learn:

- **The hidden costs of a data breach that a crisis communications plan can help mitigate**
- **How to test and refine your plan**
- **10 vital questions to ask when crafting a crisis communications plan**

# The Current Situation

When it comes to network security and data breaches, it is commonly accepted – even for organizations with best-in-class security and data privacy factors – that a breach is more a question of "when" than "if."

Even as data breach incidents become more common, they are also getting more costly. According to a recent study by the Ponemon Institute, the average total organizational cost of all types of data breaches in the United States has increased 21% over the past three years.1 In addition, the cost of each lost or stolen record increased 15% year over year.2 The Ponemon Institute notes that while the costs of notifying customers in the event of a data breach are typically relatively low, cost associated with lost business, reputation damage and customer churn is increasing steadily. In 2015, for example, enterprises that suffered a data breach reported an 18% increase in lost business cost attributable to the incident.[3]

The time it takes to identify a breach also affects the cost, according to the Ponemon Institute. Malicious attacks can take an average of 256 days to identify, while breaches resulting from human error take about 158 days to spot.[4] While any breach can cause significant damage in a matter of hours or even minutes, the additional time required to identify malicious attacks can expose an organization to significant additional damage to key systems and data sources.

With costs only expected to increase, and with the likelihood of a data breach standing at 22% for a minimum of 10,000 compromised records[5], it is critical to have a crisis communications plan in place well before a breach occurs. Without such a plan, organizations may miss the chance to properly inform customers or employees – making crucial decisions on the fly and improvising a response plan – rather than taking a proactive approach to anticipating and addressing key issues in a coherent and systematic fashion.

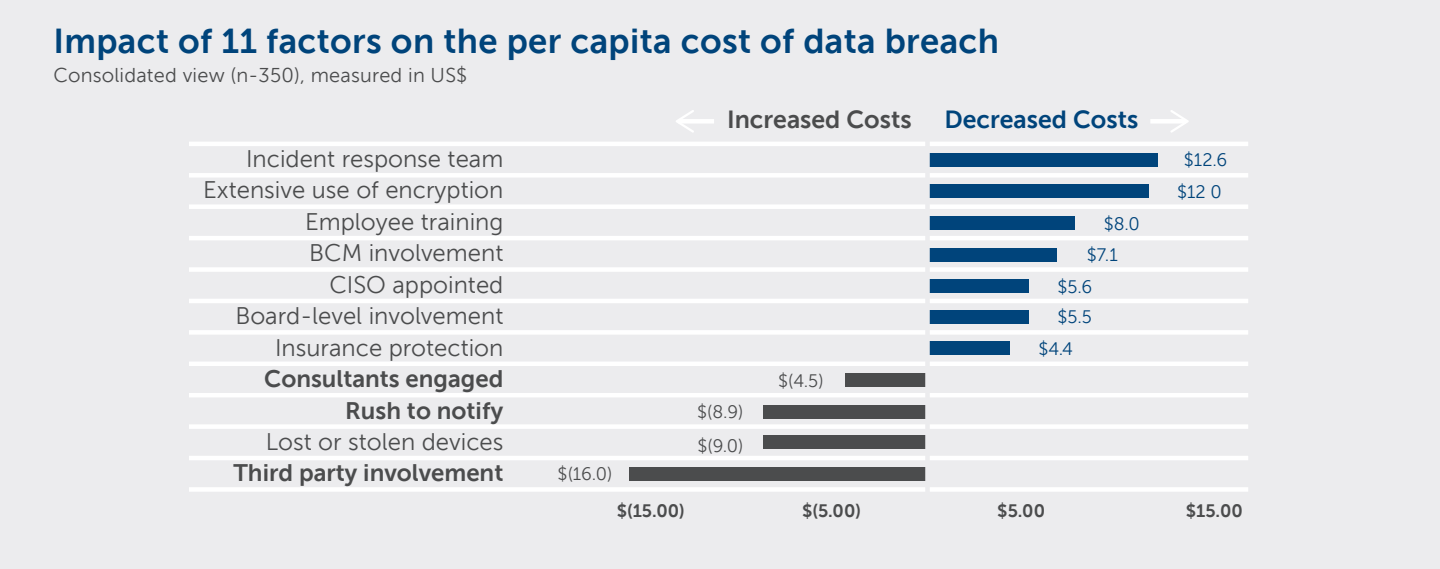


Figure 1: Ponemon Institute, *2015 Cost of Data Breach Study: Global Analysis,* May 2015, p. 14

1 Ponemon Institute, *2015 Cost of Data Breach Study: Global Analysis,* May 2015, p. 8.
2 Ponemon Institute, *2015 Cost of Data Breach Study: Global Analysis,* May 2015, p. 6.
3 Ponemon Institute, *2015 Cost of Data Breach Study: Global Analysis,* May 2015, p. 3.
4 Ponemon Institute, *2015 Cost of Data Breach Study: Global Analysis,* May 2015, p. 4.
5 Ponemon Institute, *2015 Cost of Data Breach Study: Global Analysis,* May 2015, p. 22.

# 10 Vital Questions to Ask When Crafting a Crisis Communications Plan

1. What assets are at risk for being breached? What is the most valuable data we have?
2. On which of our data sets would we be required to report a breach? What are their vulnerabilities, and how are they protected?
3. Who are the stakeholders that would need to be informed of a breach (customers, employees, investors)? How is the message going to be different for each group, and what role does each stakeholder play in resolving or recovering from the breach?
4. Who is involved in the crisis communications program? Testing and refinement? Does each person know their role?
5. What are the different levels of communication in case of a breach? Who will be engaged to manage communications with the media in the event of a breach? Who will communicate with regulators or government agencies, if necessary?
6. Do we engage with a PR firm to help handle communications? If so, which PR firm will we use, and are they on retainer and ready to help, or will we need to spend time educating them about our business and industry?
7. How will customers be notified of the breach?
8. Who will manage educating internal stakeholders and employees on the details of the breach and how to discuss the breach with customers?
9. What will be done to remediate this breach, and who will be involved?
10. Who is the public face of the breach?

# The Hidden Costs of a Breach

Being in reactive mode can exacerbate the scale and duration of the problems associated with the hidden costs of a breach. At a time when a company is increasing its security investments and incurring unexpected costs from remediating a breach, it may also have to divert time and resources from other business activities to reassure the public, shareholders and employees that it is taking the necessary steps to protect data and reduce the risk of another data-breach incident. When decisions must be made on the spot, without a plan in place, it is far more likely that an organization will incur costs such as:

## Revenue and Reputation

The issue of lost business is just one of the many "hidden costs" associated with data breaches. These hidden costs, which have increased by 28% since 2013[6], include customer turnover and the price of acquiring new customers, as well as reputation damage and loss of goodwill. Millions of dollars in customer-acquisition investments may be squandered, and organizations must re-invest even more money to restore this lost market-share potential in the wake of a breach. Calculating reputation damage and lost confidence is difficult, but the lost revenue from customers who refuse to give a company a second chance has proven to be very costly.

## Employee and Consumer Trust

The hidden costs of a breach don't stop there. Companies also lose the trust of their employees – particularly if employee records are compromised (a common occurrence in high-profile breaches). Shareholder and consumer lawsuits are another possibility, stemming from alleged negligence, failure to protect data and unreasonable delays in remedying the breach. Regulatory actions can be levied if the breach occurs as a result of violating state or federal laws. Additionally, partner firms are affected by a breach, leading to a possible loss of business relationships and disintegration of the supply chain, making it difficult to continue with business as usual.

# Testing and Refining Your Crisis Communications Plan

An effective crisis communications plan isn't just thorough; it must also be tested, refined and reviewed constantly to incorporate real-world situations. Without such testing, a seemingly complete and proactive response plan may quickly fall prey to unforeseen complications.

Consider, for example, the impact of front-line employees in a retail organization. A retail clerk or cashier may be the first – and only – point of contact between the company and its customers, yet these employees may be the last to know about a data breach incident. Customers that learn about the incident through the media may approach a cashier with questions about the safety of their credit card data. If a third party broke the news of the breach while the cashier was working, they may have no idea what happened to prompt the question or how to address it.

In the age of social media, the cashier in such a scenario could also become the face of a breach with customers spreading "news" via Twitter or Facebook based on their interactions with an uninformed source. This illustrates why a plan that focuses on big-picture issues such as media relations may be less effective than a plan that focuses on informing employees quickly about an incident and establishing clear guidelines for discussing the incident.

6 Ponemon Institute, *2015 Cost of Data Breach Study: Global Analysis,* May 2015, p. 18.

This scenario also highlights the need for security and IT professionals to seek business input into a plan. Every unit, from the executive offices to the marketing, sales, human resources, customer service and support departments, needs to be involved in formulating and regularly reviewing the crisis communications plan. Reviews should test various scenarios, consider seemingly unlikely situations and encourage "outside the box" thinking about real-world outcomes. The security leaders ultimately responsible for crafting a plan must bring stakeholder representatives together to run through anything and everything that could happen, outline their roles in a communications plan, and set goals and priorities for managing a crisis.

## Pick a Spokesperson

After a widely publicized breach, there are leaders that exemplify the best way to handle a breach, and that step up to own the problem. As the single face for the company they communicate to the media and to customers. By taking responsibility for the breach, they put a face on the company and are able to help regain the trust of customers, mitigating reputation damage.

Of course this does not eliminate the need for articulate and assertive communication with the outside world – and especially with the news media – in the wake of a breach. An effective crisis communications plan will outline methods to ensure open communications, consistent messaging and an appropriate balance between honesty and disclosure on one hand, and security, business, legal and regulatory compliance imperatives on the other.

Ultimately, crisis communications requires a constant state of vigilance. There must be constant testing and refinement to stay ahead of threats, not just in the IT department but across the enterprise. The plan needs to evolve as the threat landscape evolves, which requires communication between the security team and the business units.

## Conclusion

As many security experts would tell you, the best plan for handling a crisis is to avoid the crisis in the first place. Your data is valuable and is always under constant threat. This makes the crisis communications plan every bit as important as investing in cybersecurity to prevent an attack in the first place. That being said, no matter how hard CISO/CSO and Directors of Security are working to ensure all appropriate measures are taken, it is impossible to anticipate every scenario. By having a plan in place, reviewing and refining it regularly, and involving every unit of the business, you reduce the chances of out-of-control costs and exorbitant customer churn.

For more information, call (877) 838-7947 to speak to a SecureWorks security specialist.
www.secureworks.com