WHITE PAPER

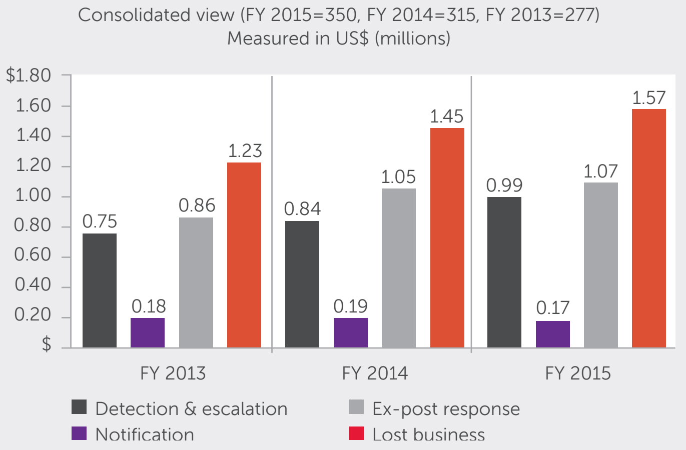
Determining the True Costs of a Data Breach

Executive Summary

According to the Identity Theft Resource Center, the number of data breaches tracked in the United States reached an all time high of 783 in 2014. This is a 27.5% increase over the number of breaches reported in 2013. The number of data breach incidents tracked in the United States since 2005 also hit a milestone of more than 5,000 and involved an estimated 675 million records.[1]

When an incident occurs, the natural reaction is to think about the short-term impact. Most companies focus on assessing the damage; developing a response; and securing funds to pay for fines, legal fees, consulting third parties, and consumer identity protection services. The real challenge is to mitigate risk to the organization from the long-term effects, such as class-action lawsuits, damage to brand reputation, erosion of consumer trust, and lost business opportunities. This paper takes an in-depth look at the true costs — both short and long term — of a data breach, and provides steps and tips that executive teams and security leaders can use to determine and reduce the true cost of a data breach.

Figure 1: Trends in four data breach cost components over three years



Source: Ponemon Institute, *2015 Cost of a Breach Study: Global Analysis*

What You Will Learn

- Current state of breaches
- Overview of short-term costs
- Overview of long-term costs
- 6 steps for determining the true costs of a data breach
- Tips for reducing the cost of a breach

Who Should Read This White Paper

» Boards of Directors
» CEOs
» CISOs/CSOs
» Directors of IT/Security

[1] Identify Theft Resource Center, "Identity Theft Resource Center Breach Report Hits Record High in 2014" January 12, 2015; accessed 7/15/15; http://www.idtheftcenter.org/ITRC-Surveys-Studies/2014databreaches.html

Compiling the Complete Picture

Recent high-profile breaches have resulted in executive shakeups and measurable breach costs as high as nine figures after insurance and deductions. However, calculating the intangible long-term costs is difficult due to the many variables that can negatively impact the bottom line. Organizations that have experienced recent data breaches are still in the process of uncovering these costs, such as: business opportunities lost due to the distraction of these crises, erosion of investor and consumer confidence, abnormal churn, and increased acquisition costs just to name a few. Before delving into these costs and how to assess and develop effective strategies, it's important to understand the nature of the threat.

The rising tide

When it comes to cyber security, the challenge for organizations is they have to be right all of the time. Hackers on the other hand only have to be right one time. Unfortunately, hackers are only part of the equation because data breaches come in many forms. Although malicious or criminal attacks account for almost half of data breach root causes, human error and system glitches are also susceptible areas.

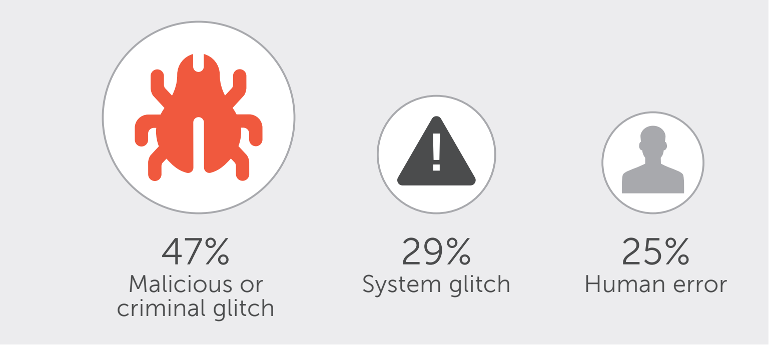


Figure 2: Distribution of the benchmark sample by root cause of the data breach

Source: Ponemon Institute, *2015 Cost of a Breach Study: Global Analysis*

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 three years. In addition, the cost of each lost or stolen record increased 15% year-over-year.[2] The point being, breaches can happen in many forms and the associated costs are growing in all scenarios.

In the following sections, we will review short- and long-term costs with the purpose of helping business leaders plan for the full consequences of a breach and provide guidance on how to decrease impact to the organization.

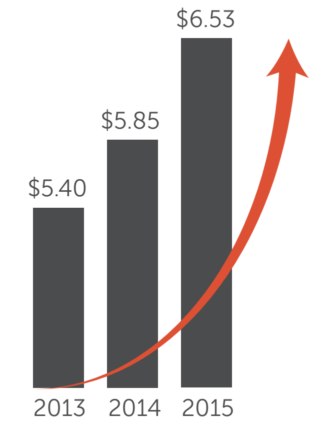


Figure 3: Average total organizational cost of a data breach in the US over three years

Source: Ponemon Institute, *2015 Cost of a Breach Study: Global Analysis*

The immediate

Short-term costs of a data breach typically include activities that revolve around assessing the immediate data loss or disruption, responding to the attack, and ongoing communications with shareholders and the public during the aftermath. While generally realized upfront and easier to calculate, these costs need to be taken into consideration when looking at the full picture of a data breach to understand the risk level and what gaps can be closed. The following provides an overview of some of the key short-term costs that must be kept top of mind:

- **Fines.** Regulatory fines can reach into the tens of millions and possibly more according to the type of data breached and the subsequent regulations violated.
- **Legal fees.** Fees can include an organization's outside counsel and any plaintiff legal fees assigned if the organization is sued.
- **Communications/PR.** Engaging a public relations firm in a reactive scenario can be costly and time consuming when time is of the essence.
- **Crisis Team management.** Unexpected costs, such as hiring, onboarding, and compensation and benefits, may be incurred when ramping up a qualified team.

[2] Ponemon Institute, *2015 Cost of Data Breach Study: Global Analysis,* May 2015.

- **Consulting/Third-Party involvement.** Without an incident response retainer or a fully developed incident response plan, bringing on a consulting firm or third party to conduct forensics, remediation and recovery tasks can prove costly and time consuming.
- **Loss of staff.** According to a new survey released by the New York Stock Exchange, board members said they are more likely to hold the CEO accountable after a breach[3] — signaling a shift away from putting the onus squarely on the CISO. That said, recent fallout from major high profile breaches in 2014 and 2015 has resulted in IT and security executives leaving voluntarily, or being fired.
- **Identity protection.** This includes associated costs of offering and monitoring any illegal financial activity on customers' or clients' affected accounts.
- **Establishing call centers.** It is necessary to quickly build capacity to field calls from customers and provide information about the scope of the breach and who is affected.

The long tail

Although the short-term costs covered in the previous section may seem like common knowledge, it's the unknowns that pose the greatest risk to an organization's health in the long run. While calculating these potential costs can be more difficult and be more theoretical in nature, they must be accounted for in order to see the full picture and identify gaps in people, process and technology. When looking at it from a risk perspective, these are the implications that are of the most interest. While short-term costs have more direct impact on current-quarter balance sheets, long-term costs have implications on the overall health of the organization. In fact, leadership is beginning to realize that their jobs are on the line as a direct result of many of these lingering implications. The following are some of the long-term costs that need to be considered when assessing the potential impact of a breach to your organization:

- **Abnormal turnover of customers.** This is perhaps one of the scariest long-term costs for business leaders. The thought of customers turning to competitors out of fear presents an uphill battle and long-term effects on quarterly results. Interestingly, industries with the highest churn rate are healthcare, pharmaceuticals and financial services.
- **Increased customer acquisition activities.** Directly correlated to abnormal turnover, acquisition costs quickly escalate and have an impact on the bottom line. Dollars spent to initially acquire those customers are lost and even more money will need to be invested to get them back. As the old adage goes, "it costs $10 to get a new customer but only $1 to keep them." If that proves to be true in a breach scenario, long-term costs can perpetuate significant financial implications.
- **Reputation loss and goodwill.** These are probably the most difficult long-term costs to tangibly calculate. One way to think about it is the number of times the organization is mentioned in the media. Some of these breaches become the hot story of the day or week. Every mention has a direct impact on reputation. Unfortunately, many times, the real truth about the breach and the potential impact on customers are misrepresented, and the initial knee jerk reaction from customers and clients is worse than the actual breach itself.

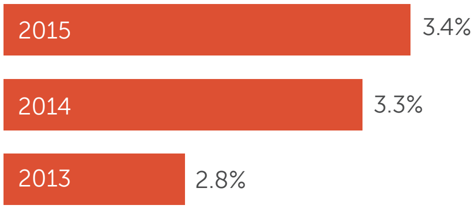


Figure 4: Abnormal churn rates in the US over three years

Source: Ponemon Institute, *2015 Cost of a Breach Study: Global Analysis*

- **Notification to outside firms.** A breach can affect not only the targeted organization, but also its partners, supply chains and their customers. Think about a retailer breach scenario where credit card information is stolen. A small credit union is now responsible for issuing new cards to its members. This has a direct financial impact on the credit union for cost of new cards, postage, covering fraudulent charges as well as the inconvenience to the cardholders.

[3] New York Stock Exchange and Veracode, *Cybersecurity in the Boardroom*, 2015.

- **Increased security investments.** A breach usually exposes a vulnerability. With this vulnerability comes an investment to fill the gap once it's been remediated. These costs can include people, process or technology.

- **Higher incident, forensic, audit and compliance costs.** Once breached, the resulting compliance requirements can be time-consuming and expensive. Add to that new processes and auditing, and the long-term costs begin to escalate.

- **Class-action lawsuits.** This can be a result of cases based on alleged negligence, failure to protect data, unreasonable delay in remedying suspension of service or loss of data, violations of various applicable state/federal laws, and more.

- **Time lost/resources pulled from other projects.** A breach usually requires an "all hands on deck" approach. This can pull not just security and IT personnel off of projects but other business groups such as compliance, privacy and more to help remediate, thus losing time on projects critical to business success.

6 Steps for Determining the Potential Cost of a Breach

While identifying and understanding the short- and long-term costs is important, the real key is preparedness. Estimating what a breach might cost *today* can help a company better develop a plan for the day when an event *does* occur. Determining potential losses can highlight key areas of opportunity for enhancing security strategy, focusing budget and resources on the right vulnerabilities, and preparing the company to respond quickly and resolve a breach more effectively.

The virtue of a fast response is that it minimizes impact. Imagine the difference if:

- A denial of service attack on your online banking application lasted hours instead of days.

- You lost one blueprint for one product instead of losing your entire product suite...which ends up in a foreign competitor's hands.

- You did or did *not* have to send out breach notification issues and reissue cards to millions of customers.

Business and security leaders have a responsibility to ensure that a security incident response plan is in place, practiced and optimized before such an event occurs.

Part of this incident response plan is identifying key areas of greatest vulnerability and potential loss that would lead to the greatest breach costs.

When calculating these costs, it's tempting to rely on an average of financial loss published by other companies in your industry or peer group, but that can be misleading at best. The long-term costs of breaches experienced by other organizations in your industry have likely yet to be fully realized. What's more, each company's business and assets are unique and handled differently, and, therefore, are vulnerable in different ways.

Leading practice suggests that determining the potential costs of a breach is best done in the context of the company's own environment. Here are six steps that business leaders can take to prepare more accurate calculations:

1. **Catalog the organization's major business processes.** Ask key questions such as, "How does our business connect to the internet to make money and run our operations?" Wherever an organization conducts transactions with customers, links to trading partners, automates critical operational controls, conducts banking, or allows for employee logins, a potential vulnerability exists. It's important to think of the company's key processes as a potential pathway for hackers to exploit, particularly in situations where the perimeter is expanding (M&A, international outposts, supply chains) or where administrative controls are not tightly managed (international expansion, rapid growth).

2. **Identify which processes handle critical data.** Among all those processes — financial transactions, network connections and administrative controls — which ones gather, handle or link to critical data that your company depends on to operate? Think beyond credit card transactions. Which processes collect personally identifiable information for purchasing or marketing purposes? How are administrator credentials assigned? How do employees log in from mobile devices and what measures are in place to ensure their security as they handle sensitive information?

3. **Identify what assets hold or carry that data.** Once you know which processes are moving that critical data, it's important to know where that data is physically located. For example, on a server full of customer data run by a business partner outside your network, or on a CEO's iPad that has the latest new product launch plan on it to review as he travels across the country.

4. **Determine what data threat actors would want to steal.** What do you have that a hacker might want? Credit cards and personal identities are sold on a massive cyber black market in staggering quantities at a reasonable cost. Intellectual property commands a high value on the dark internet, fueled by demand from those who are motivated by espionage or revenge. Disruption is a motivator, too. Access controls are coveted by those who want to cripple a business for political or advocacy purposes, or by organized criminals seeking ransom. Know what might embarrass the organization and anger stakeholders if it was released publicly.

5. **Determine what would be disrupted or cease to happen if those assets were compromised.** In addition to the obvious financial impact, are there possible chain reactions due to interdependent IT processes and technologies? What else might cease to work? Might stakeholders react in a way that causes further harm?

6. **Calculate the potential loss of the systems or breach of data.** By taking methodical steps to understand what hackers want and how they might gain access, you will have an idea of what assets are at the greatest risk and how losing those assets will disrupt the business and harm stakeholders. You'll also have a better sense of the scope of remediation actions that might be required, which in itself is a cost factor.

With all of the above information in hand, the organization is well positioned to make assumptions about which of the previously discussed short- and long-term costs will apply, and plan accordingly. It is important that legal and compliance officers are consulted about what potential liability and regulatory penalties might be triggered by the type and volume of assets or by the severity of impact. Options for cyber risk insurance should also be considered to understand what losses can and can't be offset.

Tips for Reducing the Cost of Breach

Once you understand the costs of a breach to your organization, you can mitigate the overall impact of tangible and intangible effects on the organization with the following tips:

- **Plan from a consequence approach.** Identifying a hierarchy of consequences based on breach scenarios can focus resources on hand and potential investments in people, process and technology. As part of this consequence approach, include scenarios in your business continuity management and disaster planning to ensure that essential functions continue during and after a breach.

- **Establish a comprehensive incident response plan and team (specify people, process and technology needed) and test the plan frequently.** Incorporate business units outside of IT to understand the potential impact of other parts of the organization and their role in the response. Whether the attack is malicious, an insider or a glitch, your entire organization should know — from top to bottom — what their roles are and the implications to each part of the business. Plan for every scenario, from loss of a cabinet full of data to a full-blown breach of customer information. Ensure that public relations are a critical part of your organization's incident response plan. Develop a plan for how you communicate to employees and customers in all scenarios. This should include the people that will communicate with the press, what they say, who they involve, and so on.

- **Engage a third party as part of the incident response plan.** The last thing organizations want to do from a cost perspective is to negotiate an incident response contract in the middle of an attack or remediation period. Third-party responders should have the capabilities to plan for, detect, identify, and extricate threats from the environment, and they should provide the necessary forensics to assess damage and aid recovery. Additionally, establishing an incident response retainer is a good practice to ensure speed of response to reduce the cost of a breach.

- **Train your employees.** Although most breaches are a direct result of intrusion through employee endpoints or error, employees can also be your best allies. Security awareness training can become your first line of defense to prevent the initial intrusion vector of many breaches.

- **Get leadership involved.** Appointing a CISO seems like a forgone conclusion nowadays to enhance an organization's security posture. However, studies show that involving the board of directors in security decisions has a direct dollar correlation to decreasing the cost of a breach. To engage the board, a CISO should look at the security of business systems and information from a risk perspective and convey that in nontechnical terms to a leadership team that has the ability to improve the overall security posture of an organization.

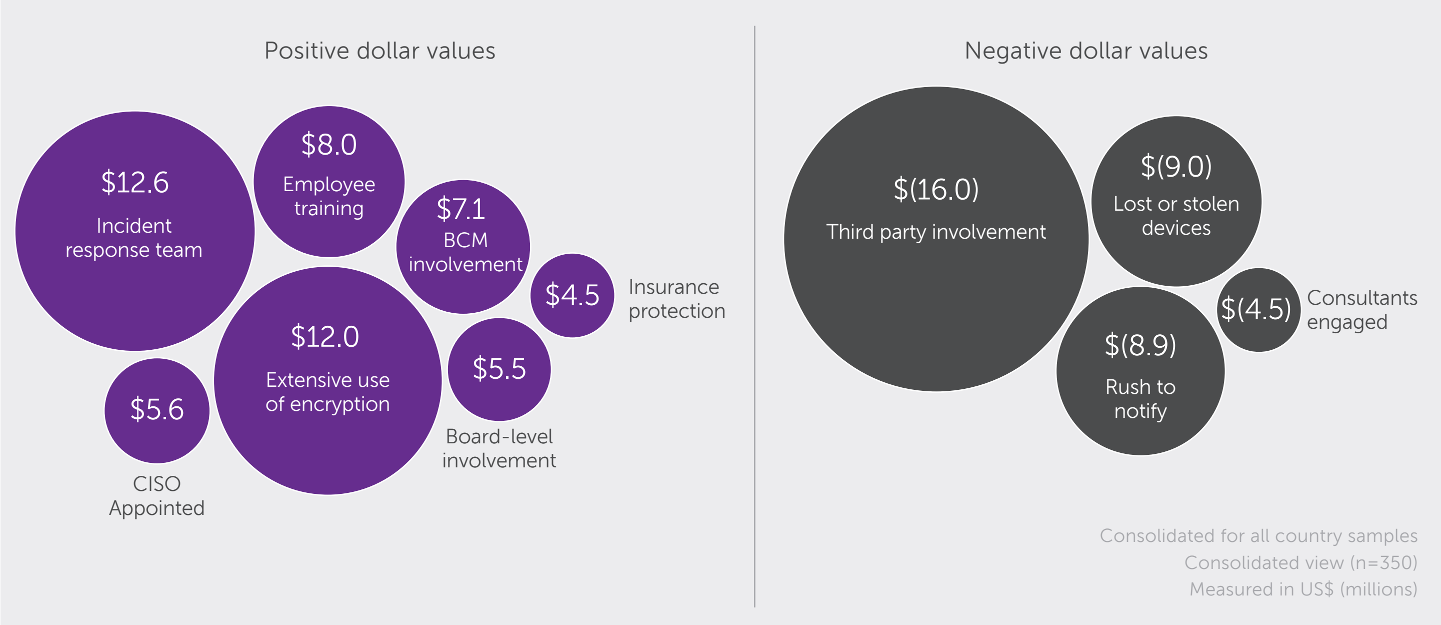


Figure 5: Impact of 11 factors on the per capita cost of a data breach

Source: Ponemon Institute, *2015 Cost of a Breach Study: Global Analysis*

- **Insure your organization.** Purchasing cyber insurance is a good best practice for decreasing some costs of a breach, and can help lower the cost per compromised record. As part of your incident response plan, cyber insurance should be looked at from the standpoint of mitigating risk and potential costs created by vulnerable areas inside and outside of the business environment.

Figure 5 shows the positive dollar values associated with the per capita cost savings that can be realized when organizations implement current best practices and tips — like the ones described above — to help reduce the costs of a breach. The negative dollar values represent an increase in the average per capita cost.

Conclusion

The costs and negative impact of a data breach span a wide range of both short and long term costs that touches almost every aspect of the business. Boards and security leaders must be actively involved in developing a strategic plan that calculates the costs of a data breach unique to their organization and addresses ways to mitigate the potential risk according to areas of greatest opportunity.

By following the steps and tips discussed, organizations can be better prepared for a breach, and minimize the potential impact.

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