IBM & Ponemon Institute Study: Data Breach Costs Rising, Now $4 million per Incident
Wednesday, June 15, 2016 10:00:00 AM (GMT)

ARMONK, N.Y., June 15, 2016 /PRNewswire/ -- IBM Security (NYSE: IBM) today announced the results of a global study analyzing the financial impact of data breaches to a company's bottom line. Sponsored by IBM and conducted by the Ponemon Institute, the study found that the average cost of a data breach for companies surveyed has grown to $4 million, representing a 29 percent increase since 2013.

Cybersecurity incidents continue to grow in both volume and sophistication, with 64 percent more security incidents reported in 2015 than in 2014.[1] As these threats become more complex, the cost to companies continues to rise. In fact, the study[2] found that companies lose $158 per compromised record. Breaches in highly regulated industries were even more costly, with healthcare reaching $355 per record – a full $100 more than in 2013.

Slow Response and Lack of Planning Cost Companies Millions
According to the study, leveraging an incident response team was the single biggest factor associated with reducing the cost of a data breach – saving companies nearly $400,000 on average (or $16 per record). In fact, response activities like incident forensics, communications, legal expenditures and regulatory mandates account for 59 percent of the cost of a data breach.[2] Part of these high costs may be linked to the fact that 70 percent of U.S. security executives report they don't have incident response plans in place.[3]

The process of responding to a breach is extremely complex and time consuming if not properly planned for. Amongst the required activities, a company must:

- Work with IT or outside security experts to quickly identify the source of the breach and stop any more data leakage
- Disclose the breach to the appropriate government/regulatory officials, meeting specific deadlines to avoid potential fines
- Communicate the breach with customers, partners, and stakeholders
- Set up any necessary hotline support and credit monitoring services for affected customers

Each one of these steps takes countless hours of commitment from staff members, taking time away from their normal responsibilities and wasting valuable human resources to the business.

Incident response teams can expedite and streamline the process of responding to a breach, as they're experts on what companies need to do once they realize they've been compromised. These teams address all aspects of the security operations and response lifecycle, from helping resolve the incident, to satisfying key industry concerns and regulatory mandates. Additionally, incident response technologies can automate this process to further speed efficiency and response time.

The study also found the longer it takes to detect and contain a data breach, the more costly it becomes to resolve. While breaches that were identified in less than 100 days cost companies an average of $3.23 million, breaches that were found after the 100 day mark cost over $1 million more on average ($4.38 million).

The average time to identify a breach in the study was estimated at 201 days, and the average time to contain a breach was estimated at 70 days.

The study found that companies that had predefined Business Continuity Management (BCM) processes in place found and contained breaches more quickly, discovering breaches 52 days earlier and containing them 36 days faster than companies without BCM.[4]

Analyzing the Cost of a Data Breach
The annual Cost of a Data Breach study examines both direct and indirect costs to companies in dealing with a single data breach incident. Through in depth interviews with nearly 400 companies across the globe, the study factors in costs associated with breach response activities, as well as reputational damage and

the cost of lost business.

"Over the many years studying the data breach experience of more than 2,000 organizations in every industry, we see that data breaches are now a consistent 'cost of doing business' in the cybercrime era," said Dr. Larry Ponemon. "The evidence shows that this is a permanent cost organizations need to be prepared to deal with and incorporate in their data protection strategies."

For more details on the study, the full report is available on the IBM X-Force Research Library. Country-specific reports are also available for the United States, United Kingdom, Germany, Australia, France, Brazil, Japan, Italy, India, the Arabian region (United Arab Emirates and Saudi Arabia), Canada and South Africa.

This year, IBM increased its investment in the Incident Response market with the acquisition of Resilient Systems. Resilient's Incident Response Platform (IRP) empowers security teams to analyze, respond, and mitigate incidents faster and more efficiently. The newest version of the platform, announced today, includes Resilient Incident Visualization, which graphically displays the relationships between Indicators of Compromise (IOCs) and incidents in an organization's environment.

"The amount of time, effort and costs that companies face in the wake of a data breach can be devastating, and unfortunately most companies still don't have a plan in place to deal with this process efficiently," said Ted Julian, Vice President, Resilient an IBM Company. "While the risk is inevitable, having a coordinated and automated incident response plan, as well as access to the right resources and skills, can make or break how much a company is impacted by a security event."

IBM also recently launched IBM X-Force Incident Response Services, which include consulting and managed security services to help clients manage all aspects of responding to a cyber breach.

About IBM Security
IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned IBM X-Force® research, enables organizations to effectively manage risk and defend against emerging threats. IBM operates one of the world's broadest security research, development and delivery organizations, monitors 20 billion security events per day in more than 130 countries, and holds more than 3,000 security patents. For more information, please visit www.ibm.com/security, follow @IBMSecurity on Twitter or visit the IBM Security Intelligence blog.

About IBM Resiliency Services
IBM Resiliency Services offers an innovative portfolio of resiliency solutions and services, including Business Continuity Management, that assist virtually every aspect of business disruption Today, more than 6,000 IBM resiliency professionals build, deploy, and manage industry-leading cloud capabilities to help you maintain continuous business operations and improve overall resiliency for your organization. For more information, visit http://ibm.co/1cqLDOz and follow @IBMServices.

Media Contact:
Cassy Lalan
IBM Security Media Relations
319-230-2232
cllalan@us.ibm.com

[1] X-Force IBM Cyber Security Intelligence Index, April 2016
[2] 2016 Cost of Data Breach Study: Global Analysis, June 2016
[3] The Cyber Resilient Organization: Learning to Thrive Against Threats, Ponemon Institute, 2015
[4] 2016 Cost of Data Breach Study: Impact of Business Continuity Management

Logo - http://photos.prnewswire.com/prnh/20090416/IBMLOGO

Countries: United States
Industries: Computer Electronics, Hardware & Software, High Tech Security
Languages: English
Primary Identifiers: IBM-US
Related Identifiers: IBM-US