

Symantec-Sponsored Ponemon Report Finds Negligent Employees Top Cause of Data Breaches in the U.S. While Malicious Attacks Most Costly
Tuesday, March 20, 2012 12:00:00 PM (GMT)

http://media.marketwire.com/attachments/201010/647074_NI-SYM_Horiz_web300x79.jpg

Symantec Corp. (NASDAQ: SYMC) and the Ponemon Institute today released the findings of the [2011 Cost of Data Breach Study: United States](#), which reveals negligent insiders are the top cause of data breaches while malicious attacks are 25 percent more costly than other types. The study also found organizations which employ a chief information security officer (CISO) with enterprise-wide responsibility for data protection can reduce the cost of a data breach by 35 percent per compromised record. The organizational cost of a data breach was \$5.5 million last year. The seventh annual Ponemon Cost of a Data Breach report is based on the actual data breach experiences of 49 U.S. companies from 14 different industry sectors.

[Click to Tweet:](#) Ponemon Institute report finds insiders pose greatest data breach threat: <http://bit.ly/xoX1jv>

"This year's report shows that insiders continue to pose a serious threat to the security of their organizations," said Francis deSouza, group president, Enterprise Products and Services, Symantec Corp. "This is particularly true as the increasing adoption of tablets, smart phones and cloud applications in the workplace means that employees are able to access corporate information anywhere, at any time. It is essential for companies to put the proper information protection policies and procedures in place to counterbalance these new realities."

Additional key findings from the report include:

- *Negligent insiders and malicious attacks are the main causes of data breach* . Thirty-nine percent of organizations say negligence was the root cause of the data breaches. For the first time, malicious or criminal attacks account for more than a third of the total breaches reported in this study. Since 2007, they also have been the most costly breaches. Accordingly, organizations need to focus on processes, policies and technologies that address threats from the malicious insider or hacker.
- *Certain organizational factors reduce the overall cost* . If the organization has a CISO with overall responsibility for enterprise data protection the average cost of a data breach can be reduced as much as \$80 per compromised record. Outside consultants assisting with the breach response also can save as much as \$41 per record. When considering the average number of records lost or stolen, all of these factors can provide significant and positive financial benefits.
- *Specific attributes or factors of the data breach also can increase the overall cost* . For example, in this year's study organizations that had their first ever data breach spent on average \$37 more per record. Those that responded and notified customers too quickly without a thorough assessment of the data breach also paid an average of \$33 more per record. Data breaches caused by third parties or a lost or stolen device increased the cost by \$26 and \$22, respectively.
- *Detection and escalation costs declined but notification costs increased*. Detection and escalation costs declined from approximately \$460,000 in 2010 to \$433,000 in 2011. These costs refer to activities that enable a company to detect the breach and whether it occurred in storage or in motion.
- *More customers remain loyal following the data breach* . For the first time, fewer customers are abandoning companies that have a data breach. However, certain industries are more susceptible to customer churn, which causes their data breach costs to be higher than the average. Taking steps to keep customers loyal and repair any damage to reputation and brand can help reduce the cost of a data breach.
- *The cost of data breach declined* . For the first time in seven years, both the organizational cost of data breach and the cost per lost or stolen record have declined. The organizational cost has declined from \$7.2 million to \$5.5 million and the cost per record has declined from \$214 to \$194.

"One of the most interesting findings of the 2011 report was the correlation between an organization having a

CISO on its executive team and reduced costs of a data breach," said Dr. Larry Ponemon, chairman and founder of the Ponemon Institute. "As organizations of all sizes battle an uptick in both internal and external threats, it makes sense that having the proper security leadership in place can help address these challenges."

The U.S. Cost of a Data Breach Study was derived from a detailed analysis of 49 data breach cases with a range of nearly 4,500 to 98,000 affected records. It takes into account a wide range of direct business costs, including engaging forensic experts, outsourcing hotline support and providing free credit monitoring subscriptions and discounts for future products and services. Indirect costs include in-house investigations and communication, as well as the extrapolated value of customer loss resulting from turnover or diminished acquisition rates. The average cost of a data breach does not apply to catastrophic breaches (study excludes data breaches of more than 100,000 records) given they are not typical of those experienced in the United States. Companies analyzed were from 14 different industries, including finance, retail, healthcare, services, education, technology, manufacturing, research, transportation, consumer, hotels and leisure, media, pharmaceutical and communications.

Symantec recommends the following information protection best practices:

- Assess risks by identifying and classifying confidential information
- Educate employees on information protection policies and procedures, then hold them accountable
- Implement an integrated security solution that includes reputation-based security, proactive threat protection, firewall and intrusion prevention in order to keep malware off endpoints
- Deploy data loss prevention technologies which enable policy compliance and enforcement
- Proactively encrypt laptops to minimize consequences of a lost device
- Implement two factor authentication
- Integrate information protection practices into businesses processes

Companies can analyze their own risk by visiting [Symantec's Data Breach Risk Calculator](#). Based on seven years of trend data, the calculator takes into account an organization's size, industry, location and security practices to estimate how much a data breach would cost on both a per record and organizational basis. It is available at <http://www.databreachcalculator.com>.

Resources

- [U.S. Cost of a Data Breach Report](#)
- [Symantec's Data Breach Risk Calculator](#)
- [Cost of a Data Breach Press Kit](#)
- [Blog Post: Negligent Employees and Malicious Attacks Cause 75% of Data Breaches](#)
- [Blog Post: Insider Data Theft: When Good Employees Go Bad](#)
- [Infographic: Cost of a Data Breach](#)
- [SlideShare: Cost of a Data Breach](#)
- [Symantec's Encryption Offerings](#)
- [Symantec's Data Loss Prevention Offerings](#)

Connect with Symantec

- [Follow Symantec on Twitter](#)
- [Join Symantec on Facebook](#)
- [Subscribe to Symantec News RSS Feed](#)
- [View Symantec's SlideShare Channel](#)
- [Visit Symantec Connect Business Community](#)

About the Ponemon Institute

The Ponemon Institute is dedicated to advancing responsible information and privacy management practices in business and government. To achieve this objective, the Institute conducts independent research, educates leaders from the private and public sectors and verifies the privacy and data protection practices of organizations in a variety of industries.

About Symantec

Symantec is a global leader in providing security, storage and systems management solutions to help consumers and organizations secure and manage their information-driven world. Our software and services

protect against more risks at more points, more completely and efficiently, enabling confidence wherever information is used or stored. More information is available at www.symantec.com.

NOTE TO EDITORS: If you would like additional information on Symantec Corporation and its products, please visit the Symantec News Room at <http://www.symantec.com/news>. All prices noted are in U.S. dollars and are valid only in the United States.

Symantec and the Symantec Logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

FORWARD-LOOKING STATEMENTS: Any forward-looking indication of plans for products is preliminary and all future release dates are tentative and are subject to change. Any future release of the product or planned modifications to product capability, functionality, or feature are subject to ongoing evaluation by Symantec, and may or may not be implemented and should not be considered firm commitments by Symantec and should not be relied upon in making purchasing decisions.

Technorati Tags

Symantec, data loss prevention, encryption, security, data breach

[Add to Digg](#) [Bookmark with del.icio.us](#) [Add to Newsvine](#)

CONTACT: Cassie StevensonSymantec Corp.+1 (415) 533-2720cassie_stevenson@symantec.comEmily ButlerConnect Public Relations+1 (801) 373-7888emilyb@connectpr.com

Countries: US

Primary Identifiers: NLOK-US

Related Identifiers: NLOK-US