

## New Era of 'Mega Breaches' Signals Bigger Payouts and Shifting Behavior for Cybercriminals

Symantec Report Reveals the Number of Mega Data Breaches went from 1 in 2012 to 8 in 2013; 552 Million Identities Exposed in 2013



**MOUNTAIN VIEW, Calif. – April 8, 2014** – After lurking in the shadows for the first ten months of 2013, cybercriminals unleashed the most damaging series of cyberattacks in history. Symantec's Internet Security Threat Report (ISTR), Volume 19, shows a significant shift in cybercriminal behavior, revealing the bad guys are plotting for months before pulling off huge heists – instead of executing quick hits with smaller rewards.

“One mega breach can be worth 50 smaller attacks,” said Kevin Haley, director, Symantec Security Response. “While the level of sophistication continues to grow among attackers, what was surprising last year was their willingness to be a lot more patient – waiting to strike until the reward is bigger and better.”

In 2013, there was a 62 percent increase in the number of data breaches from the previous year, resulting in more than 552 million identities exposed – proving cybercrime remains a real and damaging threat to consumers and businesses alike.

“Security incidents, managed well, can actually enhance customer perceptions of a company; managed poorly, they can be devastating,” wrote Ed Ferrara, VP and principal analyst, Forrester Research. “If customers lose trust in a company because of the way the business handles personal data and privacy, they will easily take their business elsewhere.”<sup>1</sup>

### Defense is Harder than Offense

The size and scope of breaches is exploding, putting the trust and reputation of businesses at risk, and increasingly compromising consumers' personal information – from credit card numbers and medical records to passwords and bank account details. Each of the eight top data breaches in 2013 resulted in the loss of tens of millions of data records. By comparison, 2012 only had a single data breach reach that threshold.

“Nothing breeds success like success – especially if you're a cybercriminal,” said Haley. “The potential for huge paydays means large-scale attacks are here to stay. Companies of all sizes need to re-examine, re-think and possibly re-architect their security posture.”

Targeted attacks were up 91 percent and lasted an average of three times longer compared to 2012. Personal assistants and those working in public relations were the two most targeted professions – cybercriminals use them as a stepping stone toward higher-profile targets like celebrities or business executives.

## **How to Maintain Cyber Resiliency**

While the increasing flow of data from smart devices, apps and other online services is tantalizing to cybercriminals, there are steps businesses and consumers can take to better protect themselves – whether it be from a mega data breach, targeted attack or common spam. Symantec recommends the following best practices:

For Businesses:

- *Know your data:* Protection must focus on the information – not the device or data center. Understand where your sensitive data resides and where it is flowing to help identify the best policies and procedures to protect it.
- *Educate employees:* Provide guidance on information protection, including company policies and procedures for protecting sensitive data on personal and corporate devices.
- *Implement a strong security posture:* Strengthen your security infrastructure with data loss prevention, network security, endpoint security, encryption, strong authentication and defensive measures, including reputation-based technologies.

For Consumers:

- *Be security savvy:* Passwords are the keys to your kingdom. Use password management software to create strong, unique passwords for each site you visit and keep your devices – including smartphones – updated with the latest security software.
- *Be vigilant:* Review bank and credit card statements for irregularities, be cautious when handling unsolicited or unexpected emails and be wary of online offers that seem too good to be true – they usually are.
- *Know who you work with:* Familiarize yourself with policies from retailers and online services that may request your banking or personal information. As a best practice, visit the company's official website directly (as opposed to clicking on an emailed link) if you must share sensitive information.

Symantec will be hosting a webinar on this year's ISTR results on Tuesday, April 15, 2014 from 10:00 to 11:00 a.m. PDT. For more information or to register, please go [here](#).

## **About the Internet Security Threat Report**

The Internet Security Threat Report provides an overview and analysis of the year in global threat activity. The report is based on data from Symantec's Global Intelligence Network, which Symantec analysts use to identify, analyze, and provide commentary on emerging trends in attacks, malicious code activity, phishing, and spam.

## **About Symantec**

Symantec Corporation (NASDAQ: SYMC) is an information protection expert that helps people, businesses and governments seeking the freedom to unlock the opportunities technology brings – anytime, anywhere. Founded in April 1982, Symantec, a Fortune 500 company, operating one of the largest global data-intelligence networks, has provided leading security, backup and availability solutions for where vital information is stored, accessed and shared. The company's more than 20,000 employees reside in more than 50 countries. Ninety-nine percent of Fortune 500 companies are Symantec customers. In fiscal 2013, it recorded revenues of \$6.9 billion. To learn more go to [www.symantec.com](http://www.symantec.com) or connect with Symantec at: [go.symantec.com/socialmedia](http://go.symantec.com/socialmedia).

**NOTE TO U.S. 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.*

<sup>1</sup> *New Research: CISOs Need To Add Customer Obsession To Their Job Description*, Ed Ferrara Forrester Research, Inc. Blog Post, March 2014