Security

Companies Reveal Where IT Security Falls on Their Priority List, Their Greatest IT Security Threats and Fears, and The Severity of Breaches When They Occur

SPONSORED BY

Executive Summary

Given the growing threat of data breaches in corporate America, companies across all industries are re-evaluating and tightening IT security policies. To provide a glimpse of companies' views when it comes to securing devices and computers, as well as the severity and costs to businesses when a security breach unfolds, Penton Research conducted a survey of 468,863 subscribers of Penton brands, specifically targeting those holding an executive management or IT job title.

The 2015 *IT Security* survey, found that the majority of respondents (64%) consider security a top priority among their company's IT initiatives. Furthermore, companies revealed ways that their businesses were negatively impacted by security outages. Overall, 8% of respondents experienced at least one hardware security breach within the past two years, with more than a fourth of those reporting stolen data or a halt in operations. When it came to software security breaches, 16% of respondents experienced at least one within the past two years, with 19% of those reporting stolen data and 27% reporting a halt in operations.

Respondents revealed their deepest IT security fears, with 25% identifying the loss of customer data as their greatest fear, 19% saying it was the loss of operations or productivity and 15% said it was a loss of corporate data. Respondents also shared which vendors they rely on most when looking for comprehensive security solutions, with the majority of respondents (41%) choosing HP, followed by Dell (39%) and Lenovo (12%).

The white paper provides further insights regarding which types of security solutions companies employ, their satisfaction with those solutions, their security policies for personal devices and what they believe are their primary threats regarding IT security. The survey offers a comparison of how small and medium-sized businesses (SMB) with between 10 and 999 employees conduct their IT security versus enterprise companies with 1,000 or more employees. In addition, the survey reveals candid responses from company management and IT professionals regarding the severity and effects when security breaches occurred. We hope executives, IT professionals and developers will find value in these insights as they explore new and more effective ways to bolster IT security policies for today's businesses and their customers.

About the Survey

OVERVIEW

The marketing research arm of Penton conducted the survey *IT Security,* including all methodology, data collection and analysis. Data was collected from February 26 through March 11, 2015. Methodology conforms to accepted marketing research methods, practices and procedures.

OBJECTIVES

This survey was conducted to seek executive management and IT professionals' views regarding the importance of IT security, as well as the security solutions they currently employ and their satisfaction with these solutions. It also addresses companies' first-hand experience with security breaches within a two-year period, as well as the impact and severity of the security breach. Furthermore, it helps provide context regarding companies' security policies for personal devices, primary threats to security and greatest IT security fears, as well as which vendors companies believe offer the most comprehensive security solutions.

METHODOLOGY

On February 26, 2015, Penton Research deployed email invitations to participate in an online survey to 468,863 subscribers of Penton brands, specifically targeting subscribers with executive management and IT titles. By March 11, 2015, Penton Research received 1,902 completed surveys, for an effective response rate of 0.4%. Of those, 810 represented companies with at least 10 employees, of which the following analyses are based on.

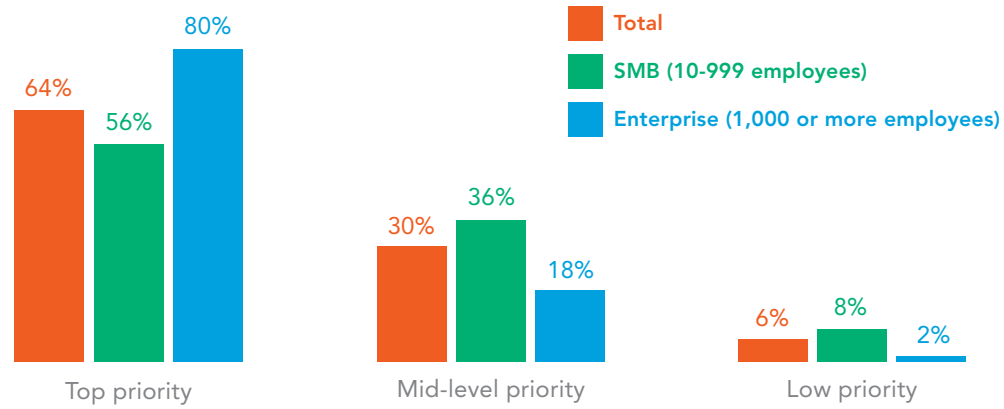
RESPONDENT PROFILE

The respondents to this survey work in a variety of industries, including manufacturing (11%), Information Technology (10%) and government (9%), along with foodservice (8%), financial services (7%), health care (7%), education (7%), transportation (6%) and construction (5%), among others. Most respondents hold an Information Technology role within their organization (47%), followed by an executive management role (25%). Companies with 10 employees or more are represented in the sample, including SMBs with 10 to 999 employees (63%) and enterprise companies with 1,000 or more employees (36%). These companies range from having no dedicated IT professionals in their company to more than 20 IT professionals or a partially or fully outsourced IT department. Twenty-seven percent of respondents are the final purchase decision-makers for technology, whereas 29% influence purchasing decisions, 30% make recommendations and 15% have no involvement in purchasing decisions within their companies.

Key Findings

The 2015 *IT Security* survey found that the majority of respondents (64%) consider security a top priority among their company's IT initiatives. Among enterprise companies with 1,000 or more employees, 80% indicated that security was a top priority. In addition, 56% of SMB respondents with more than 10 employees but fewer than 999 employees said that security was a top priority.

How important is security with regard to your company's other IT initiatives? Security is a...

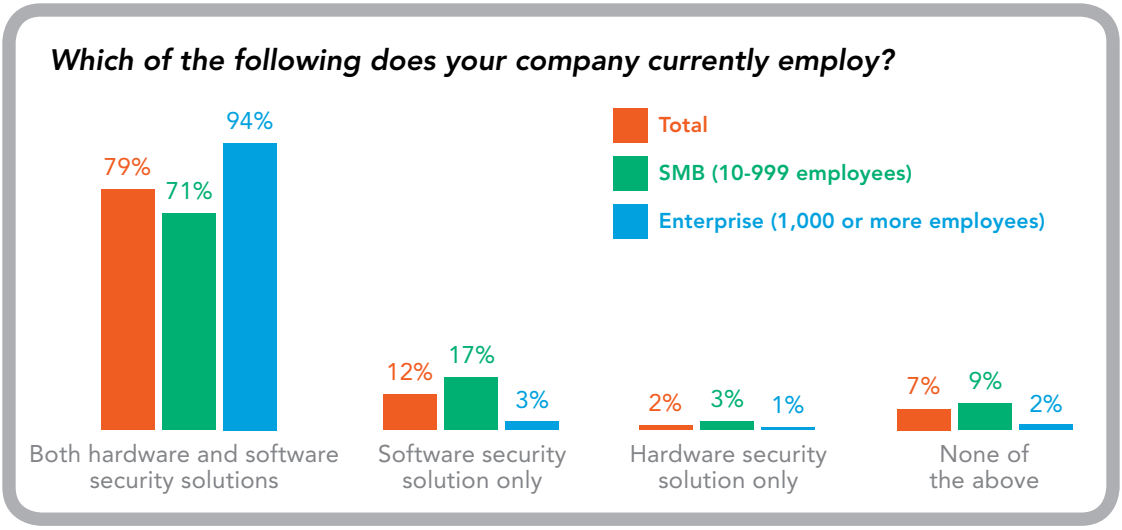


Base: All respondents (n=810), including SMBs (n=515) and Enterprise companies (n=295).

Only 6% of total respondents reported that security was a low priority. When considering company size, only 2% of enterprises and 8% of SMBs place security toward the bottom of their priority list. The remaining 30% of respondents view IT security as a mid-level priority.

What Are Companies Doing To Stay Secure?

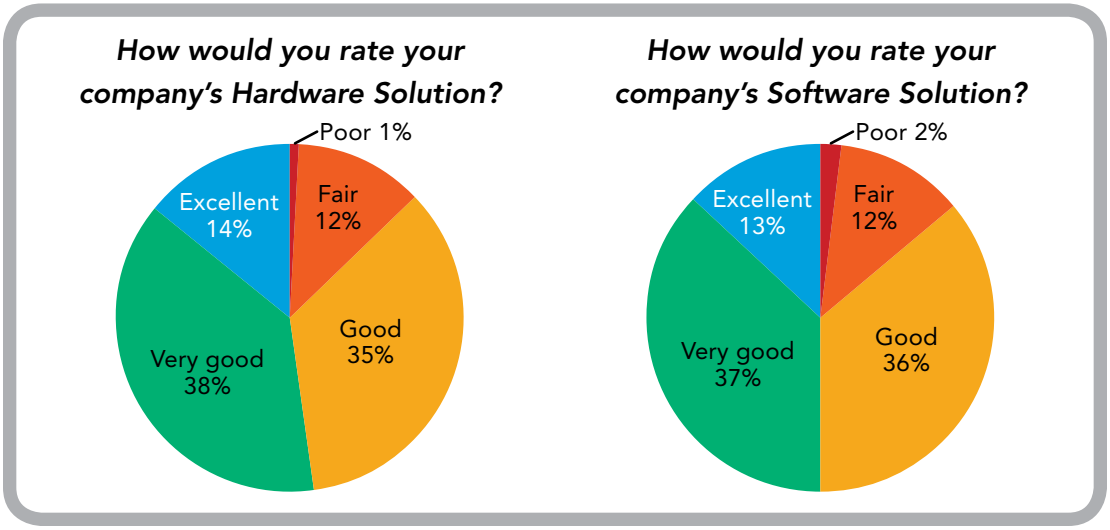
The majority of respondents (79%) employ both hardware and software security solutions. Enterprise companies are more likely to recognize the severity of data breaches, with 94% using both hardware and software security solutions, versus 71% of SMBs using both hardware and software security solutions. Seven percent of total respondents have neither hardware nor software security solutions in place, with that figure coming from 9% of SMBs and only 2% of enterprise companies. Among the companies employing just one security solution, more companies (12%) gravitate toward a software security solution, versus 2% of total respondents enlisting just a hardware security solution.



Base: All respondents (n=810), including SMBs (n=515) and Enterprise companies (n=295).

The Majority of Companies Are Satisfied With Current Security Solutions

When it comes to satisfaction levels regarding current security solutions, 84% of respondents rated their hardware and software solutions positively, with a "good, "very good" or "excellent" rating. Very few respondents who employ a security solution rated the results as "poor." In fact, only 2% of those employing a software solution and only 1% of those employing a hardware solution reported a "poor" rating.

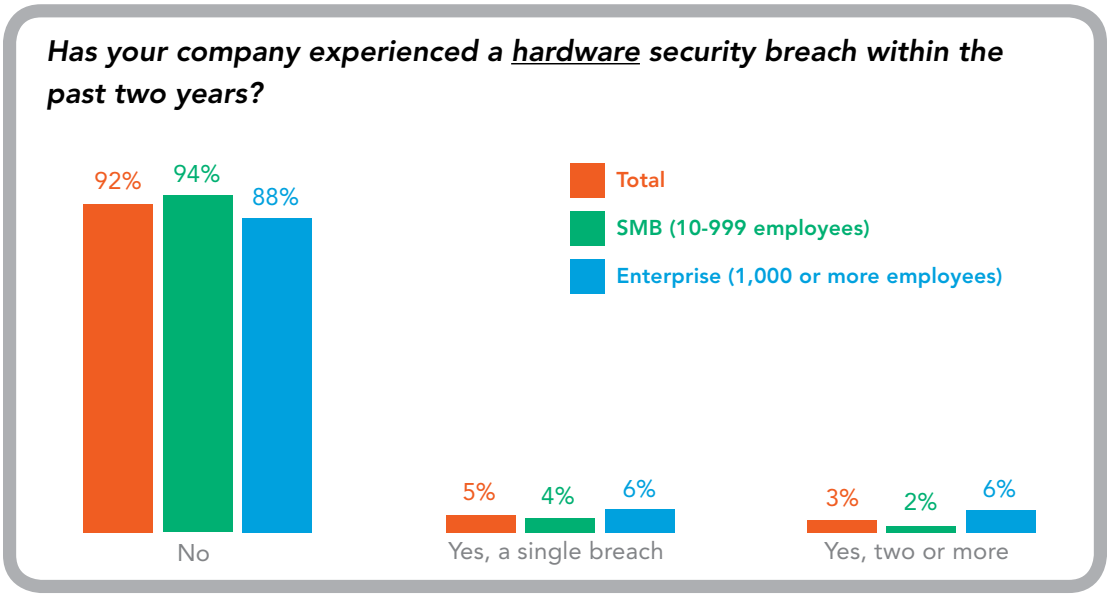


Among the companies expressing concerns about their security solutions, respondents made comments such as "very outdated technology," "seems to not keep up with current trends" and "simple passwords for protection." One SMB respondent voiced a concern that "the president of our company does not understand the enormity of potential IT threats."

Hardware and software security solutions that were rated as "very good" or "excellent" were described in ways such as "many safety checks," "no major losses," "updated regularly," "fully encrypted" and "many layers."

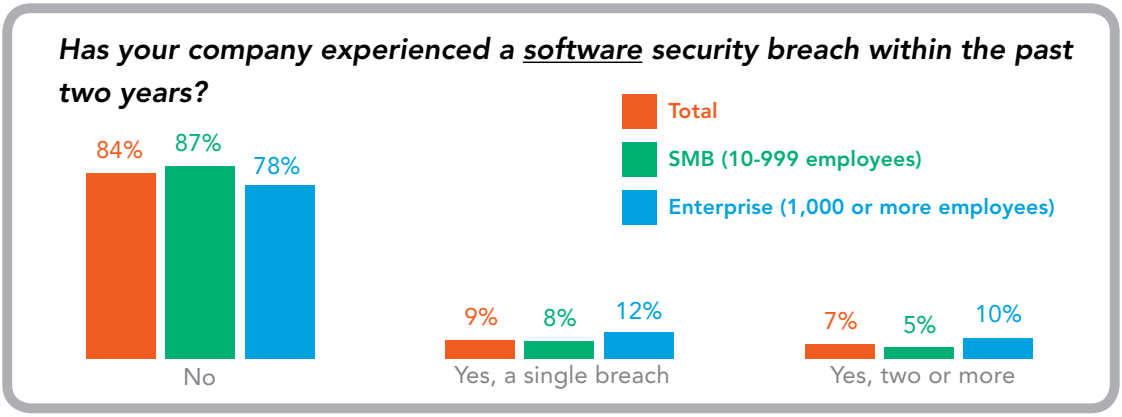
How Many Companies Have Been Impacted By Security Breaches?

Only 8% of respondents experienced a hardware security breach within the past two years, with enterprise respondents more likely to report such a breach (12%) than SMB respondents (6%). The remaining 92% of respondents did not report a hardware security breach.



Base: All respondents (n=810), including SMBs (n=515) and Enterprise companies (n=295).

While software security breaches occurred more commonly, relatively few respondents have experienced one within the past two years (16% overall). Once again, enterprise respondents were more likely to report such a breach (22%) than SMB respondents (13%).



Base: All respondents (n=810), including SMBs (n=515) and Enterprise companies (n=295).

Cost of Security Breaches

More than one-fourth of those experiencing a hardware security breach reported having data stolen (29%) and/or experienced a halt of operations (29%).

Of those companies that reported a software security breach, 19% experienced stolen data and 27% reported a resulting halt in operations.

Companies that experienced a halt in operations reported that these lasted from 30-35 minutes or 4-5 hours to one or two days, one week or even as long as 14 days.

The survey also collected candid responses from company management regarding the severity and effects when security breaches occurred. Below are some of the most noteworthy statements gathered:

Impact of Hardware Security Breaches

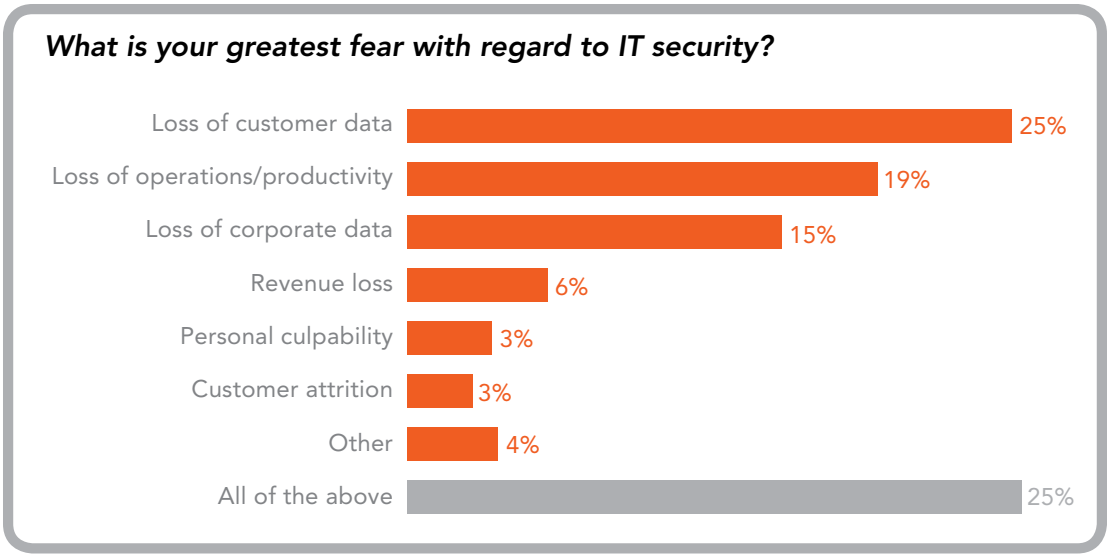
- "$1,500"
- "Customers not using credit cards"
- "Exposed need to hire professional IT services"
- "Lost sales – inability to accept orders"
- "Lost some data"
- "Lost credibility that also potentially decreases the revenue"
- "Money changed from accounts uncontrollably"

Impact of Software Security Breaches

- "Approximately $30,000 (one day of payroll)"
- "Fines, fees and loss of reputation. We were able to cover the costs, through insurance but still feel the consequence of the loss of reputation"
- "Files on network drives encrypted by an encrypted virus"
- "Money was diverted to many unknown accounts"
- "Integrity"
- "$2.5 million in SLA charges, unknown amount of lost-ecommerce transactions"
- "Affected stock price"

Companies' Greatest IT Security Fears

When companies were asked about their greatest IT security fears, one-quarter of respondents identified the loss of customer data as their greatest fear, while 19% said it was a loss of operations or productivity and for another 15% the loss of corporate data was their main concern. However, 22% of respondents did not select just one primary fear and instead chose "all of the above," which also included revenue loss, personal culpability and customer attrition.



Base: All respondents (n=810).

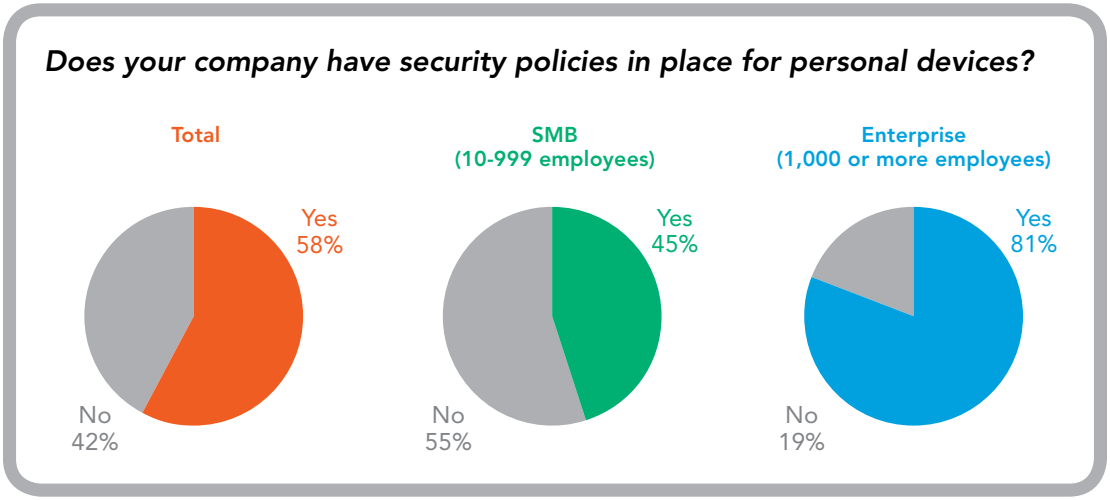
Furthermore, when companies were asked about which security threats they are most concerned about, 36% of total respondents indicated that end users were their primary threat and 36% noted an unedu-

cated staff. This was followed by 34% of respondents who said that failure to take security seriously was their biggest concern. Other concerns were the email system (26%), personally owned mobile devices (25%), inadequate investment in IT solutions (23%) and aging infrastructure (20%). Problematic patches and executive management were also concerns at 17% and 14%, respectively.

When comparing enterprises with SMB, enterprises believe their primary threat is end users (46%), followed by an uneducated staff (41%). SMBs, on the other hand, are most concerned about failure to take security seriously and an uneducated staff, each of which gathered 34% of responses.

Security Policies for Personal Devices

Many companies are enlisting security policies for personal devices, with 58% of total respondents saying they have a policy in place. This is more common within larger companies, with 81% of enterprise companies having a security policy for personal devices, compared to 45% of SMBs.



Base: All respondents (n=810), including small companies (n=1,081), including medium companies (n=515) and large companies (n=295).

Which Vendors Do Companies Rely On Most for Security Solutions?

Respondents shared which vendors they believe offer the most comprehensive security solution, with the majority of respondents (41%) choosing HP, followed by 39% saying it was Dell and 12% opting for Lenovo. In addition, 7% selected Xerox, 4% Lexmark and 25% chose another security solution.

In Conclusion

The majority of companies surveyed prioritize IT security, recognize the risks associated with failing to secure devices and computers, and implement hardware and/or software security solutions to safeguard their businesses and resources. The good news is that a conversation is happening, and companies are taking steps to address identifiable concerns. To this end, it's important that companies periodically evaluate their IT security policies and encourage ongoing dialogue about new ways for current policies to meet the demands of ever-evolving technologies and security threats.

The good news is that a conversation is happening, and companies are taking steps to address identifiable concerns.

While enterprise companies seem to take the risks and threats of IT security more seriously than SMBs, both types of businesses recognize the negative impact that security breaches can have on their companies. Securing personal devices seems to be one category that SMBs can improve on, since less than half of SMB respondents said they have a policy in place, compared to 81% of enterprises. SMBs can implement security policies for personal devices by considering a range of options, from employing mobile device management systems that can provide encryption, password management and software distribution to educating employees on device security or even conducting a company-wide mobile security audit.

Furthermore, this survey highlights the severity of software and hardware data breaches when they do occur. While some executive and IT professionals' comments regarding impacts such as a loss of revenue (up to millions of dollars in charges in one instance) and loss of productivity (as long as 14 days) are telling, even more so are the comments regarding a loss to reputation and integrity that can take years or even longer to repair. Of course, remaining proactive and committing to preventive measures are the first steps toward minimizing the risk of data breaches and better protecting the reputation and integrity of a company.

Companies in general also indicated areas for improvement concerning IT security. For example, over one-third of respondents said an uneducated staff was their primary IT security threat, and over one-third also indicated that failure to take security seriously was their biggest threat. While recognizing

these concerns is the first step, proactive measures must follow. For example, companies should consider mandatory IT security training for all employees and ongoing education about measures they can take to prevent data breaches, as well as ensuring employees fully understand the consequences and severity of IT security lapses.

The survey also indicates that comprehensive security solutions are available for companies, and the overwhelming majority of businesses employing hardware and software security solutions give them a "good," "very good" or "excellent" rating. For those companies that believe their solutions are not satisfactory, it's of the utmost importance that they seek alternative solutions through methods such as conducting market research or referrals until their needs and expectations are fully met.

About Penton Research

Penton Research, a division of Penton Marketing Services, has been conducting primary business-to-business research since 1989. In addition to the editorial, strategic and promotional research serving Penton's media properties, Penton Research conducts custom proprietary research for manufacturers and service providers in a wide variety of industries.

Its broad offerings capitalize on Penton's deep industry knowledge across 17 vertical markets to develop winning, best-of-breed sales and marketing solutions. Penton Marketing Services, operates from over 20 offices across the globe, including hubs in Washington, DC, New York, Chicago, Cleveland and Colorado. For more information, go to www.pentonmarketingservices.com.