Proofpoint, Osterman Research Survey Reveals that when It Comes to Consumerized IT Security and Compliance, Employee Trust Is No Longer an Option

Organizations that Prohibit Consumerized IT May Be Increasing Risk

SUNNYVALE, CA – June 23, 2011 – Proofpoint, Inc., the leading provider of cloud-based email security and compliance solutions, today announced findings from its 2011 Consumerized IT Security Survey. Conducted in conjunction with Osterman Research, the survey polled 632 respondents from enterprises and government agencies to find out how their organizations are responding to security and compliance challenges caused by the onslaught of consumerized IT in the workplace.

The survey revealed that 84 percent of organizations are allowing employees to use consumerized IT such as iPads, iPhones, Facebook, Twitter and IM to conduct business communications. It also revealed that to mitigate associated risks, organizations are turning away from a trust-only approach and implementing three-layer security and compliance strategies that include trust, policy and technology. Seventy-three percent of those polled stated that they are using a combination of policy and trust, 51 percent have implemented strategies that leverage policy, technology and trust, and only 11 percent are relying on “employee good judgment” alone.

“Consumerized IT in the workplace is a fact of life, and organizations recognize that they must act to integrate it in a secure and compliant manner,” said Michael Osterman, principal of Osterman Research, Inc. “Trust will always be an essential part of any security and compliance strategy, but it is encouraging to discover that half of those polled know that trust alone will not provide an effective defense.”

Mobile Devices Are Most-Used Consumerized Technology, Email Is Number 1 Mobile Application

When it comes to consumerized IT, mobile devices such as the iPad and iPhone are the most used, ranking ahead of social platforms such as Facebook, Twitter and LinkedIn. Despite the wide range of applications, features and functions available on consumerized mobile devices, email remains in the lead as the most widely used mobile business communications tool. Sixty-seven percent of respondents said email was the most widely used applications, while only 5 percent said that enterprise applications such as mobile dashboards were the most commonly used. This finding demonstrates that when it comes to the use of consumerized IT, organizations should prioritize mobile devices ahead of social platforms, and that when providing mobile-device security, email should be their primary focus.

“These facts show that the biggest risk exposure from consumerized IT is the use of business email on personal devices,” said David Knight, executive vice president of product management and marketing, Proofpoint. “When developing the technology and policy portions of their three-layer security and compliance strategies, organizations should make sure they have policies and training in place to encourage users to utilize on-device security features such as strong passwords and remote-wipe, and robust perimeter security technologies that can defend against email-borne attacks and data leakage.”

Fortunately, most enterprises have email security technologies, policies and processes in place that provide email encryption, email archiving, email security and data loss prevention (DLP). Organizations that can leverage these capabilities to extend security over mobile email are in a better position to bring all of their mobile devices within the boundaries of security and compliance. Organizations with email capabilities that provide data privacy and protection tools such as automated policy-based encryption will be able to further strengthen mobile defenses.

Anti-Consumerized-IT Policies May Be Increasing Risk

Despite the fact that some organizations have strict policies against consumerized IT, a majority of respondents that prohibit its use believe that employees are using it anyway. Ninety-eight respondents (16 percent of the total respondents) said that their organizations do not allow employees to use consumerized technologies in the workplace, but 64 percent of these organizations suspect that employees are using consumerized IT regardless of policies against it. Despite its widespread use, 56 percent either have no consumerized IT adoption strategy in place or do not know if their company even has a plan. Only 29 percent have an adoption plan, and only 13 percent are in the process of developing a plan to integrate consumerized IT.

“Companies that have no strategy for managing consumer-driven technologies on their network are in serious peril. Sooner or later, an unprotected device, social media or IM platform is going to provide unauthorized access to sensitive or regulated information,” said Knight. “Enterprises that stick their heads in the sand when it comes to consumerized IT are increasing risk at an unquantifiable rate.”
The survey revealed additional salient facts:

- 71 percent of organizations that do not allow consumerized IT in the workplace do nothing more than issue a warning to employees who violate policy
- 72 percent of organizations that do not allow consumerized IT in the workplace are not convinced that it can be used in a secure and compliant manner
- 48 percent of organizations that allow consumerized IT in the workplace allow users to choose which technologies they use
- 48 percent of organizations that allow consumerized IT in the workplace regulate which technologies can be used
- 89 percent of organizations that allow consumerized IT in the workplace say that the Apple iPhone and iPad are the most-used mobile devices
- 49 percent of organizations that allow consumerized IT in the workplace say that Facebook is the most-used social media platform

Methodology and Background

The Proofpoint 2011 Consumerized IT Security Survey polled 632 respondents. Nineteen percent are employed by organizations with more than 1,000 employees, 14 percent are employed by organizations with more than 2,500 employees, and 28 percent are employed by organizations with more than 5,000 employees. Respondents consisted of employees from all levels, including chief officers, IT and IT security and compliance directors, managers and administrators. The majority of respondents are employed by organizations within the financial services industry, with others coming from multiple industries including healthcare, government, retail and manufacturing. The survey was conducted online, over a period of three weeks, with respondents coming from the Proofpoint customer roster and the Osterman Research survey pool. Ninety-seven percent of respondents were from the U.S. Statistical numbers are rounded to the nearest whole number. For a complete copy of the survey, visit: [http://bit.ly/consumerized](http://bit.ly/consumerized)

About Osterman Research

Osterman Research, Inc., provides market research, industry analysis reports, white papers, webinars, surveys and related services for vendors and customers in the messaging, Web 2.0, social media, mobile, collaboration, information management and other markets. Osterman Research continually gathers information from IT decision-makers and end users of information technology. Osterman Research reports and analyzes this information to help companies develop and improve the products and services they offer to these markets or to internal customers.

About Proofpoint, Inc.

Proofpoint focuses on the art and science of cloud-based email security, eDiscovery and compliance solutions. Organizations around the world depend on Proofpoint’s expertise, patented technologies and on-demand delivery system to protect against spam and viruses, safeguard privacy, encrypt sensitive information, and archive messages for easier management and discovery. Proofpoint’s enterprise email solutions mitigate the challenges and amplify the benefits of enterprise messaging. Learn more at [www.proofpoint.com](http://www.proofpoint.com).

Proofpoint is a registered trademark of Proofpoint, Inc. in the US and other countries. All other trademarks contained herein are the property of their respective owners.