proofpoint

August 30, 2010

Proofpoint Survey Finds Email Continues to be the Top Source of Data Loss in Large Enterprises while Risks from Social Media, Mobile Devices Increase

Email, Social Networking Channels and Mobile Devices Main Culprits for Corporate Data Loss; Enterprises Continue to Crack Down on Policy Violations August 30, 2010

August 30, 2010 – Note: A version of this release is also available in German. **SUNNYVALE, Calif. – August 30, 2010** – In its seventh annual study of outbound email and data loss prevention issues, Proofpoint Inc. found that email continues to be the number one source of data loss risks in large enterprises as more than a third (35 percent) investigated a leak of confidential or proprietary information via email in the past 12 months. At the same time, the number of data loss events associated with social media channels continued to increase. Employee misuse of email, work-owned mobile devices, and popular social media tools including Facebook, LinkedIn, Twitter, video sharing sites, forums and blogs resulted in an increasing number of disciplinary actions—including termination—as enterprises demonstrate increasing concern about securing sensitive data.

Background / Availability

- Proofpoint's Outbound Email and Data Loss Prevention in Today's Enterprise, 2010 report is based on a June/July 2010 survey of 261 email and messaging decision makers at large US enterprises (organizations with more than 1000 employees).
- Respondents were asked about the frequency of data loss events in the past 12 months, as well as their concerns, priorities and policies related to email, the Web, social media and other sources of data loss risk.
- The latest version of this report is available at http://www.proofpoint.com/outbound.

Enterprise Data Loss Continues at Alarming Rate

Proofpoint found that, despite a growing awareness of data loss risks, large enterprises continue to be impacted by data loss at a surprising rate:

- Thirty-six percent of respondents said their organization was impacted by the exposure of sensitive or embarrassing information in the past 12 months.
- Thirty-one percent of respondents said their organization was impacted by the improper exposure or theft of customer information in the past 12 months.
- Twenty-nine percent of respondents said their organization was impacted by the improper exposure or theft of intellectual property in the past 12 months.

Risks from Social Media on the Rise

Enterprise concerns and data loss events from social media continued to rise in the past 12 months:

- **Social Networking Sites (such as Facebook and LinkedIn)**: Twenty percent of companies investigated the exposure of confidential, sensitive or private information via a post to a social networking site. Seven percent of companies terminated an employee for social networking policy violations. Twenty percent disciplined an employee for such violations.Fifty-three percent are highly concerned about the risk of information leakage via social networking sites. Fifty-three percent explicitly prohibit the use of Facebook, while 31 percent explicitly prohibit use of LinkedIn.
- **Blog and Message Board Postings**: Twenty-five percent of companies investigated the exposure of confidential, sensitive or private information via a blog or message board posting. Eleven percent of companies terminated an employee for blog or message board posting policy violations. Fifty-four percent are highly concerned about the risk of information leakage via blogs and message boards.
- **SMS and Web-Based Short Messaging Services (such as Twitter)**: Seventeen percent of companies investigated the exposure of confidential, sensitive or private information via one of these services. Fifty-one percent are highly concerned about the risk of information leakage. Forty-nine percent explicitly prohibit the use of Twitter.
- **Media Sharing Sites (e.g., YouTube, Vimeo)**: Eighteen percent of companies investigated the exposure of confidential, sensitive or private information via shared video or audio media. Nine percent of companies terminated an employee for media sharing/posting policy violations. Twenty-one percent disciplined an employee for such violations. Fifty-two percent are highly concerned about the risk of information leakage. Fifty-three percent explicitly

prohibit the use of media-sharing sites.

Mobile Devices Increasing Cause for ConcernM

When it comes to data loss, the physical loss of laptops, smart phones and other mobile devices that contain sensitive information gives IT professionals the greatest cause for alarm (64 percent are highly concerned about this risk):

- Fifty-six percent are highly concerned about data loss via email sent from mobile devices.
- Twenty-two percent investigated the exposure of confidential, sensitive or private information via lost or stolen mobile devices or storage media in the past 12 months.

Email Still the Number One Data Loss Threat

- Thirty-five percent of companies investigated the exposure of confidential or proprietary information via email in the past 12 months. Thirty-two percent investigated a suspected violation of privacy or data protection regulations related to email. Twenty percent terminated an employee for violating email policies. Fifty percent disciplined an employee for such violations.
- Fifty-five percent are highly concerned about the risk of information leakage via the organization's email system. On average, respondents estimate that as many as one in five outbound email messages contains content that poses a legal, financial or regulatory risk.
- Thirty-seven percent employ staffs to monitor the content of outbound email and 48 percent perform regular audits of outbound email content.

SaaS and Cloud Computing as a Source and Solution for Data Loss Risks

Enterprise IT decision makers continue to be evenly split on whether SaaS and cloud computing increase data loss risks:Just under half of respondents (49 percent) agree with the statement, "The trend toward using SaaS and cloud computing solutions in the enterprise seriously increases the risk of data leakage."

In spite of these concerns, SaaS security solutions are increasingly popular with respondents and significant numbers of them already use or intend to use SaaS for a variety of email security and compliance functions:

- More than half of respondents (52 percent) say they have already deployed a SaaS solution for protecting inbound email against spam and malware. An additional 17 percent "will definitely" deploy such technology in the future.
- Thirty-one percent of respondents say they have already deployed a SaaS solution for outbound data loss prevention and compliance functions. An additional 19 percent say they "will definitely" deploy such technology in the future.

The Recession has Increased the Risk of Data Loss

- In the past 12 months, 21 percent of companies investigated a suspected leak or theft of confidential or proprietary information associated with an employee leaving the company (e.g., through voluntary or involuntary termination).
- Fifty-eight percent of respondents say that budget constraints have negatively impacted their organization's ability to protect confidential, proprietary or sensitive information. Fifty-three percent say the same of IT staff reductions in the past 12 months.

Supporting Quotes

"The level of concern and anxiety about corporate data loss is on the rise, and the recession has only increased the pressure on companies to enforce corporate email and social media policies. It's no longer just an IT department concern. We're seeing C-level executives and management paying attention as data loss becomes a very real, public threat to companies." Gary Steele, CEO, Proofpoint, Inc.

"Enterprise IT professionals are faced with trying to minimize data loss risks across an ever-growing number of channels. And for every high-profile data loss event you see in the mainstream media, there are many more that you never hear about. Employees should also be aware of these concerns, the policies their employers have put around electronic communications and the serious consequences for violating those policies." Keith Crosley, director of market development, Proofpoint, Inc.

Video / Photos

Video: http://bit.ly/cpKxLZ

Audio: http://bit.ly/9hMBnr

Additional Resources

Webinar: http://bit.ly/czT3iL

Slideshow: http://slidesha.re/daITWZ

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.