STROZ FRIEDBERG

PRESS RELEASE

Senior Managers Account for the Greatest Information Security Risks, Finds New Stroz Friedberg Survey

Employees give corporate America a below-average grade on cyber security effectiveness

NEW YORK, NY, January 7, 2014 – As companies look for solutions to protect the integrity of their networks, data centers, and computer systems, an unexpected threat is lurking under the surface—senior management. According to a new survey, 87% of senior managers frequently or occasionally send work materials to a personal email or cloud account to work remotely, putting that information at a much higher risk of being breached. Released today by global investigations, intelligence, and risk services company Stroz Friedberg, the survey, "On the Pulse: Information Security Risk in American Business," also found that 58% of senior management reported having accidentally sent the wrong person sensitive information, compared to just 25% of workers overall.

Corporate managers also put their companies at risk of intellectual property loss if and when they depart the company. Fifty-one percent of senior management and 37% of mid-level management admit to taking job-related emails, files, or materials with them when they have left past employers. Only one-fifth of lower ranking employees have done so.

"Insiders are by far the biggest risk to the security of a company's sensitive information, whether it's a careless executive or a disgruntled employee. When information is compromised, a company's reputation, customer base, and share price may suffer," said Michael Patsalos-Fox, CEO of Stroz Friedberg. "Our inaugural information security survey demonstrates that companies need to address high-risk security behaviors within the workplace at all levels with a proactive risk mitigation plan."

The national survey of 764 information workers explored the state of information security in U.S. businesses and surveyed respondents online regarding their thoughts on the biggest information security threats, cyber security risk mitigation, company security vulnerabilities, and the state of corporate America's response to cyber threats.

continued…

Whose Job Is It to Safeguard a Company from Cyber Attacks?
The survey found that senior leaders in general believe their own security efforts are inadequate:

- Nearly half (45%) of senior management acknowledge that the C-suite and senior leadership themselves are responsible for protecting their companies against cyber-attacks.
- Yet, 52% of this same group indicated they are falling down on the job, rating corporate America's ability to respond to cyber-threats at a "C" grade or lower.
- Rank-and-file workers differ in their opinions about cyber security accountability, with 54% of those respondents saying IT professionals are responsible for putting the right safeguards in place.

Eric Friedberg, Executive Chairman of Stroz Friedberg, said, "The C-suite is responsible for making the right security investment decisions, but beyond that, leadership needs to create a culture in which all employees recognize their own responsibility for keeping information secure. Companies that are proactive in both measures are the most successful in combating and recovering quickly from a cyber attack."

Employees admit fears regarding the security of their personal information at work, with 73% of respondents reporting concern that a hacker could gain access to their company's network and steal sensitive, personal records such as their Social Security number, birthday, or home address. This worry perhaps reflects their thoughts regarding how well businesses in general are responding to cyber threats and in safeguarding sensitive or proprietary information; more than 60% of employees gave American businesses a "C" or lower when asked to grade their performance on this critical task.

Proliferation of Personal Tech Opens New Security Risks for the Enterprise
The trends of bring-your-own-device (BYOD) and the use of personal online accounts have become prevalent in American businesses, as workers use their personal smartphones, tablets, and preferred cloud providers to stay productive while at work and out of the office. This is opening the door for businesses to encounter new and emerging threats from hackers, malware, and viruses.

- Seventy-one percent of survey respondents admitted to frequently or occasionally sending materials to a personal email account or uploading materials to a personal cloud account. Among this sample:
    - the reason cited most often (37%) is that they have a preference for using their personal computer over their work computer
    - fourteen percent find that it's too much effort to bring their work laptop home with them.

A lack of corporate communication and training is also a likely culprit to explain these behaviors:

- Only 35% of respondents reported receiving regular training and communications on mobile device security from their employers
- Thirty-seven percent of employees received training on social media use
- Employees reported information sharing training just 42% of the time.

continued…

“Because employees use their personal smartphones and other powerful technology increasingly in the workplace, it is crucial for companies to update their technology use policies and training programs,” said Ed Stroz, Executive Chairman of Stroz Friedberg, “Training, along with effective policies and ensuring compliance, are a company’s best lines of defense against insider information security threats. It’s an important part of a holistic security approach that recognizes the interdependency of technical and physical security.”

For further information about the Stroz Friedberg “On the Pulse: Information Security Risk in American Business” survey or to download the infographic report, please visit www.strozfriedberg.com.

Survey Methodology

The 2013 Stroz Friedberg “On the Pulse: Information Security Risk in American Business” survey polled 764 information workers who use a computer for their job between October 28 to November 4, 2013. The nationally representative online survey was conducted by KRC Research, an independent research firm. Respondents worked for companies with more than 20 employees. The margin of error for the entire sample is plus or minus 3.54 percentage points at the 95 percent confidence level.

About Stroz Friedberg, LLC

Founded in 2000, Stroz Friedberg is a global leader in investigations, intelligence, and risk services. It provides expertise in digital forensics, cybercrime and incident response, security science, forensic accounting, compliance, due diligence, data discovery and analytics. Working at the intersection of technology, investigations, regulatory governance and behavioral science, the company is driven by a core purpose—seeking truth so clients can find the assurance and answers they need to move forward with certainty.

With eleven offices across nine U.S. cities, London, and Hong Kong, Stroz Friedberg assists in managing critical risk for Fortune 100 companies as well as 80% of the AmLaw 100 and the Top 20 UK law firms. Learn more at www.strozfriedberg.com.

###

Contact:

Stroz Friedberg
Karen Guterl
kguterl@strozfriedberg.com
212-542-3167

Weber Shandwick
Ben Tanner
btanner@webershandwick.com
212-445-8245