



WebSense Security Survey: IT Stresses as Data Breaches Put Jobs on the Line

IT managers feel that getting a divorce or losing their job is less stressful than looking after company confidential data

SAN DIEGO—October 20, 2011— How are IT managers coping with today's fast-changing threat landscape? Are they properly protected against the latest data-stealing malware? And would employees report if they compromised corporate data? To find out these answers and more, Websense, Inc. (NASDAQ: WBSN), a global leader in content security and data theft protection, commissioned independent research firm Dynamic Markets to survey 1,000 IT managers and 1,000 non-IT employees in the U.S., UK, Canada, and Australia about the latest threats to corporate and personal security, including modern malware and advanced persistent threats (APTs).

The research reveals that serious data breaches have occurred compromising CEO and other executives' data, confidential customer data, and data necessary for regulatory compliance. IT managers are feeling the pressure and saying that data loss incidents put their jobs on the line and that the stress of managing their company confidential data is greater than divorce, managing personal debt, or a minor car accident. But help is on the horizon as headline-grabbing security incidents have promoted data security talks amongst top management and have driven focus on security, including the need for additional budget. [Click here to download the full report](#) entitled Security Pros & 'Cons': IT professionals on confidence, confidential data, and today's cyber-cons.

Key findings:

Stress of Security

- **Data breaches put IT jobs on the line.** 86 percent said that their job would be at risk if a security incident were to occur, including if a CEO or other executive's confidential data is breached (36 percent); data needed for compliance is lost (34 percent); and if confidential information is posted on a social networking site (34 percent).
- **Confidential data breaches.** Shockingly, a full 24 percent reported that the CEO's or other executives' confidential data had been breached. 34 percent report losing data needed for compliance. 34 percent state that confidential information has been posted on a social networking site and 37 percent say that data has been lost by employees.
- **Hidden data loss and social media risks.** 20 percent stated that data affected by regulatory compliance was compromised. 20 percent have seen confidential information posted on social networking sites. 34 percent of employees who accidentally compromise data wouldn't tell their boss.

- **72 percent say protecting company data is more stressful than getting a divorce, managing personal debt, or being in a minor car accident.** 14 percent say losing their job would be less stressful than staying in their current role.

Sufficient Protection?

- **Necessary but not sufficient.** There are indications that antivirus and firewall solutions may have been oversold as a panacea, creating a false sense of security. While AV and firewalls are still certainly necessary, they are not sufficient to stop modern malware and advanced data-stealing attacks. Only 48 percent of respondents use systems that prevent confidential data from being uploaded to the web. Yet 60 percent worry about advanced persistent threats and 19 percent said they have been a victim of this type of attack. Only two percent of respondents had a DLP solution that protects their data at rest, in use, and in motion. However, as a result of recent high-profile data breaches, 23 percent began or accelerated a data loss prevention project.

Hope on the Horizon

- **Data security talk now involves top management.** 91 percent of IT security managers report that new levels of management have engaged in data security conversations in the last year, including the head of IT (43 percent), managing director (38 percent), and CEO (33 percent). This means that until recently, the head of IT was often not involved.
- **Headline-grabbing security incidents are impacting IT planning.** More than 60 percent of IT managers concede that recent well-publicized security incidents have affected their planning. Most have made multiple changes: more than 40 percent have increased spending, focused attention internally on testing and overhauling existing policies, have implemented new solutions, and imposed new restrictions on users. Nearly a quarter have begun or accelerated a full DLP project.

Quotes

“This survey shows that companies need to recalculate their assumptions about how well their data is protected,” said Tom Clare, Websense senior director of Product Marketing. “When asked about real-time protection solutions in place, many respondents listed product and vendor names that don’t offer real-time protection at all.

He continued, “Advanced threats are using attack elements and methods that AV was not designed to address—and are written and tested specifically to bypass AV. Companies need a robust, layered security strategy—like our Websense® TRITON™ solutions—that can truly protect them from modern malware in the wild and effectively keep their confidential data protected however it’s being used.”

Multimedia Elements:

A full copy of the Websense survey on “Security Pros & ‘Cons’: IT professionals on confidence, confidential data, and today’s cyber-cons” can be downloaded at <http://www.websense.com/content/websense-security-survey-security-pros-and-cons.aspx>.

[Click to download an infographic](#) of the Websense “Security Pros & ‘Cons’: IT professionals on confidence, confidential data, and today’s cyber-cons” survey.

[Click to share](#) the Websense “Security Pros & ‘Cons’: IT professionals on confidence, confidential data, and today’s cyber-cons” survey on **Facebook**.

[Click to share](#) on **Twitter**:

New survey: IT managers feel getting a divorce or losing their job is less stressful than looking after data <http://ow.ly/72LIT> @Websense

Websense Links:

Facebook: [“Like” Websense](#).

Twitter: Follow [@Websense](#).

About Websense, Inc.

Websense, Inc. (NASDAQ: WBSN), a global leader in unified web security, email security, and data loss prevention (DLP) solutions, delivers the best content security for modern threats at the lowest total cost of ownership to tens of thousands of enterprise, mid-market and small organizations around the world. Distributed through a global network of channel partners and delivered as appliance-based software or Security-as-a-Service (SaaS), Websense content security solutions help organizations leverage web 2.0 and cloud-based communication, collaboration, and social media, while protecting from advanced persistent threats and modern malware, preventing the loss of confidential information, and enforcing internet use and security policies. Websense is headquartered in San Diego, California with offices around the world. For more information, visit www.websense.com.

Follow Websense on Twitter: www.twitter.com/websense

Join the discussion on Facebook: www.facebook.com/websense

###

Websense Media Contact:

Patricia Hogan

Websense, Inc.

(858) 320-9393

phogan@websense.com