OVER 2,560 INTERNAL SECURITY BREACHES
OCCURRED IN US BUSINESSES EVERY DAY

Despite widespread occurrence, only one in five IT professionals consider insider threat to be a security priority.

8813D4
PAYMENT CARD BREACH

3287M8
INDUSTRIAL ESPIONAGE

5734K12
CARELESS USER

6635R8
DATA THEFT

9151P4
I.T SABOTAGE

O ver 666,000 internal security breaches took place in US businesses in the last 12 months, an average of 2,560 per working day, new research has revealed. The findings, revealed by security software provider IS Decisions in a new report, also found that despite this regular occurrence, only 17.5% of IT managers consider insider threats to be in their top three security priorities.

The new report, entitled **'The Insider Threat Security Manifesto: Beating the threat from within'**, highlights the issue of internal security as a greater challenge for larger organisations, with 40% of businesses of over 500 employees having had internal security breaches in the last year. It also compares the occurrence of and IT professional's attitudes towards insider threats in the UK, where the trend was echoed with just 21% voicing concern despite over 300,000 internal security breaches in the last year.

Insider threats continue to be a relatively low priority for IT professionals, with the research finding the issue is trumped by

concern about the threats of viruses (67%), data loss (47%) and hacking (39%). Yet the numbers suggest that the greatest source of data loss is in fact from employees, indicating that IT professionals are negating to look at their own internal structures seriously enough to address their own concerns.

The report also details what areas IT professionals are more concerned about with regards to internal threat, along with how well set up they are to manage the issue. Francois Amigorena, CEO of IS Decisions commented, *"It is human nature to see external sources as your greatest threat, and that coupled with the fact that insider threat is a complex issue to manage has led to IT professionals seemingly turning a blind eye to the issue.*

"These numbers, and the impact that the Edward Snowden case had last year, show clearly that internal security should be higher up the IT agenda. The reality is that it is a very considerable problem, but the good news is that there is a lot that IT departments can do to mitigate the risks. It's a technology issue as well as a cultural one, and can be addressed from both of these angles."

Download the Insider Threat Manifesto:
Beating the threat from within

About IS Decisions

IS Decisions makes it easy to manage and secure your Microsoft Windows and Active Directory infrastructure. With solutions for user access control, file auditing, server and desktop reporting, and remote installations, IS Decisions combines the powerful security today's business world mandates with the innovative simplicity the modern user expects. Over 3,000 customers around the world rely on IS Decisions to prevent security breaches; ensure compliance with major regulations, such as SOX, FISMA and HIPAA; and gain time and cost-savings for IT.

IS Decisions, founded in 2000, is a Microsoft Silver Partner based in Biarritz, France.

Customers include *BAE Systems, BMW, Computer Sciences Corporation, FBI, Frito-Lay, Lockheed Martin, Mitsubishi, TimeWarner, United Nations Organization, US Department of Justice, US Department of Veterans Affairs and US Navy Marine Corps.*

http://www.isdecisions.com

Contact

Chris Bunn
Marketing Director

Email: chris@isdecisions.com
Phone: +335.59.41.42.20

François Amigorena
President & CEO

Email: famigorena@isdecisions.com
Phone: +335.59.41.42.20