CSO CERT Software Engineering Institute Carnegie Mellon. Deloitte.

2011 CYBERSECURITY WATCH SURVEY: ORGANIZATIONS NEED MORE SKILLED CYBER PROFESSIONALS TO STAY SECURE

According to survey, more attacks are committed by outsiders but attacks by insiders are viewed to be the most costly to organizations

Framingham, Mass.—January 31, 2011 —Organizations are encountering more cybersecurity events; however the events, on average, are costing significantly less than in the previous year, according to the 2011 CyberSecurity Watch Survey conducted by *CSO* magazine, the leading resource for security professionals, and sponsored by Deloitte. Twenty-eight percent of respondents have seen an increase in the number of events in the 2011 study and 19% were not impacted by any attacks, compared to 40% in the 2010 study.

More than 600 respondents, including business and government executives, professionals and consultants, participated in the survey. The survey is a cooperative effort of CSO, the U.S. Secret Service, the Software Engineering Institute CERT® Program at Carnegie Mellon University and Deloitte.

“Organizations are becoming more strategic in how they prevent and respond to cybersecurity events such as the advanced persistent threat (APT),” said Ted DeZabala, national leader of Deloitte’s Security & Privacy services. “However, while the survey suggests that the annual monetary losses from events have dropped from $395,000 in 2010 to $123,000 per organization in 2011, we believe these numbers are a result of organizations associating incidents to different domains such as privacy and fraud rather than traditional cybersecurity. Further, this metric alone could be misleading as reported events, sophistication of attacks and external attribution have all increased while the perceived effectiveness of technology-based defenses has decreased.”

Insider Attacks Are More Damaging

The 2011 CyberSecurity Watch Survey uncovered that more attacks (58%) are caused by outsiders (those without authorized access to network systems and data) versus 21% of attacks caused by insiders (employees or contractors with authorized access) and 21% from an unknown source; however 33% view the insider attacks to be more costly, compared to 51% in 2010. Insider attacks are becoming more sophisticated, with a growing number of insiders (22%) using rootkits or hacker tools compared to 9% in 2010, as these tools are increasingly automated and readily available.

Not only are insider attacks monetarily costly, but they also cause additional harm to organizations that can be difficult to quantify and recoup. Harm to an organization’s reputation, critical system disruption and loss of confidential or proprietary information are the most adverse consequences from insider cybersecurity events, according to respondents. The public may not be aware of the number of insider events or the level of the damage caused because 70% of insider incidents are handled internally without legal action, which is consistent with the 2010 study.

“Technical defenses against external attacks and leakage of well-formatted data like social security numbers and credit card numbers have become much more effective in recent years,” said Dawn Cappelli, technical manager of the Insider Threat Center at CERT. “It is a much more challenging problem to defend against insiders stealing classified information or trade secrets to which they have authorized access or against technically sophisticated users who want to disrupt operations. CERT has been working with government and industry groups to develop solutions to this problem using commercial and open source tools. We invite organizations to share their insights with us."

Unknown Supplier Processes and Foreign Entity Threats Drive Concerns

Organizations must be focused on cybersecurity events directed at their company and their supply chain and need to understand how vendor partners are prepared to deal with events. The largest category of concern within the supply chain is with third-party vendors (55% in 2011 vs. 49% in 2010). Respondents are also concerned with contractor (49%) and software (42%) awareness and preparedness.

Another cybersecurity threat is the concern of cybersecurity attacks from foreign entities, which has doubled in the past year from 5% in 2010 to 10% in 2011.

Skilled Cyber Professionals and Technological Capabilities Greatest Defense

According to the 2011 study, unintentional exposure of private or sensitive information has significantly declined since 2010 (31% in 2011 vs. 52% in 2010). Organizations have taken several steps to reduce this exposure including providing cybersecurity training (65%) and the implementation of internal monitoring tools like data loss prevention (DLP) (65%).

Organizations are using more programs to address cybersecurity risks, including access management (80%), intrusion detection systems (69%), vulnerability management (65%) and identity management (64%). Since 2010, the biggest swing in implementation is vulnerability management systems which grew to 65% from 48% in 2010. These systems identify vulnerabilities and allow organizations to put mitigation plans into place.

"Employees and the technologies they enable are the best line of defense for cybersecurity attacks to reduce organizational risk," said Bob Bragdon, publisher of *CSO* magazine. "The continued effort to empower employees to recognize risks, and the process to report or deter a problem, has been a reason why organizations are more prepared for these attacks and there is optimism that the evolution of preparedness will continue."

"The Secret Service's international network of 31 electronic crimes task forces continuously monitors trends in cybercrime and the impact that this type of criminal activity has on various organizations and the American public," said Kenneth Jenkins, Special Agent in Charge of the U.S. Secret Service Criminal Investigative Division. "Through these task forces, we seek to establish, promote and continue robust public-private partnerships based on the Secret Service's historic strategic alliances with federal, state and local law enforcement agencies, private industry and academic institutions. Together, we can respond to, confront and suppress cybercrime, malicious uses of cyberspace and threats to cybersecurity that endanger the integrity of our nation's financial payments systems and threats against our nation's critical infrastructure."

About the 2011 CyberSecurity Watch Survey

The 2011 CyberSecurity Watch survey was conducted by *CSO* magazine in cooperation with the U.S. Secret Service, the Software Engineering Institute CERT Program at Carnegie Mellon University and Deloitte. The survey was conducted from August 16, 2010, through August 30, 2010. An email invitation with a link to the survey was sent to *CSO* magazine readers/site visitors plus the members and partners of the U.S. Secret Service's Electronic Crimes Task Forces. In all, 607 responses were collected. Margin of error is +/- 4 percentage points. Respondent answers cover the period between August 2009 and July 2010.

For complete survey results please contact lholmlund@cxo.com. For additional insight on the survey and cybercrime from Deloitte please visit: www.deloitte.com/us/securityandprivacysolutions.

NOTE TO EDITORS: Any references to the data from the 2011 CyberSecurity Watch survey must reference *CSO* magazine, U.S. Secret Service, Software Engineering Institute CERT Program at Carnegie Mellon University and Deloitte.

About CSO Magazine

CSO produces award-winning information and community resources for security professionals leading business risk management efforts within their enterprises, as well as creates opportunities for security marketers to reach them. Launched in 2002, the CSO portfolio includes CSOonline.com, *CSO* magazine, CSO Executive Programs and *Security Smart*. The properties provide security professionals in the public and private sectors with analysis and insight on security trends and a keen understanding of how to develop and implement successful strategies to secure all business assets. CSO is published by IDG Enterprise, a subsidiary of International Data Group (IDG), the world's leading media, events, and research company. Company information is available at www.idgenterprise.com.

About Deloitte

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee, and its network of member firms, each of which is a legally separate and independent entity. Please see www.deloitte.com/about for a detailed description of the legal structure of Deloitte Touche Tohmatsu Limited and its member firms. Please see www.deloitte.com/us/about for a detailed description of the legal structure of Deloitte LLP and its subsidiaries.

About the Software Engineering Institute and the CERT Program

The Software Engineering Institute (SEI) is a federally funded research and development center sponsored by the U.S. Department of Defense and operated by Carnegie Mellon University. The SEI helps organizations make measurable improvements in their software engineering capabilities by providing technical leadership to advance the practice of software engineering. The CERT Program serves as a center of enterprise and network security research, analysis, and training within the SEI. For more information, visit the CERT website at http://www.cert.org and the SEI website at http://www.sei.cmu.edu.

About the United States Secret Service

The U.S. Secret Service has taken a lead role in mitigating the threat of financial crimes since the agency's inception in 1865. As technology has evolved, the scope of the U.S. Secret Service's mission has expanded from its original counterfeit currency investigations to also include emerging financial and cybercrimes. As a component agency within the U.S. Department of Homeland Security, the U.S. Secret Service has established successful partnerships in both the law enforcement and business communities – across the country and around the world – in order to effectively combat financial and cybercrimes. More information can be found at: www.secretservice.gov.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Contacts:

***CSO* Magazine**
Lynn Holmlund
508.935.4526
lholmlund@idgenterprise.com

CERT Program
Richard Lynch
412.268.4793
public-relations@sei.cmu.edu

Deloitte
Daniel Mucisko
973.602.4126
dmucisko@deloitte.com

U.S. Secret Service
Joseph Freyre
202.406.9330
joseph.freyre@usss.dhs.gov

###