



2010 CYBERSECURITY WATCH SURVEY: CYBERCRIME INCREASING FASTER THAN SOME COMPANY DEFENSES

According to survey, multiple attacks occurring within larger organizations and insiders remain most costly threat

Framingham, Mass.—Jan. 25, 2010 —Cybercrime threats posed to targeted organizations are increasing faster than many organizations can combat them, according to the 2010 CyberSecurity Watch Survey conducted by [CSO magazine](#), the leading resource for security professionals, and sponsored by [Deloitte's](#) Center for Security & Privacy Solutions. Moreover, the survey suggests the threat of cybercrime is heightened by current security models that are only minimally effective against cyber criminals.

More than 500 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, Software Engineering Institute CERT® Program at Carnegie Mellon University and Deloitte's Center for Security & Privacy Solutions, a new security solutions innovation center.

"Coupled with organizations' misperceptions of the effectiveness of current security models, the survey suggests that most entities employ traditional 'wall-and-fortress' approaches to security," said Ted DeZabala, principal, Deloitte & Touche LLP and national leader of Deloitte's Security & Privacy services. "Organizations can take a more effective approach by looking at themselves as cyber criminals do, focusing on what assets are at risk of leaving the organization through the IT environment as well as the threats entering the organization through the same means. In other words, a risk-based approach."

Repeat offense on the rise

The [2010 CyberSecurity Watch Survey](#) uncovered a drop in victims of cybercrimes (60% vs. 66% in 2007), however, the affected organizations have experienced significantly more attacks than in previous years.

Between August 2008 and July 2009 more than one third (37%) of respondents experienced an increase in cybercrimes compared to the previous year. While outsiders (those without authorized access to network systems and data) are the main culprits of cybercrime in general, the most costly or damaging attacks are more often caused by insiders (employees or contractors with authorized access). One quarter of all cybercrime attacks were committed by an unknown source.

"It is alarming that although most of the top 15 security policies and procedures from the survey are aimed at preventing insider attacks, 51% of respondents who experienced a cyber security event were still victims of an insider attack. This number is holding constant with the previous two surveys (2007 and 2006)," said Dawn Cappelli, technical manager of the Threat and Incident Management Group at CERT. "Insider incidents are more costly than external breaches, according to 67% of respondents. CERT has been working with government and industry leaders to develop recommendations for new solutions to this problem using commercial and open source tools, and invite organizations to share their insights with us."

-more-

Security Budgets Soar

Although the number of incidents rose, the ramifications have not been as severe. Since 2007, when the last cybercrime survey was conducted, the average monetary value of losses resulting from cybercrimes declined by 10%. This can likely be attributed to an increase in both IT security spending (42%) and corporate/physical security spending (86%) over the past two years.

“The Secret Service’s international network of 29 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 assistant director Michael Merritt of the U.S. Secret Service. “The aggressive proactive approach of combining resources with international, federal, state, and local law enforcement partners, the private sector, and academia through our Electronic Crimes Task Forces has proven to be a very effective tool in combating the transnational cyber criminal organizations that are currently targeting the U.S. financial infrastructure. This collaborative approach has been so successful that in 2009, our Electronic Crimes Task Forces led the investigation into two of the largest data breach cases ever prosecuted in the United States.”

As technology advances, so do the methods to commit cybercrimes. Outsiders invade organizations with viruses, worms or other malicious code, phishing and spyware, while insiders most commonly expose private or sensitive information unintentionally, gain unauthorized access to/use of information systems or networks and steal intellectual property.

The survey finds that insiders most often use their laptops or copy information to mobile devices as a means to commit electronic crimes against their organization. The 2010 CyberSecurity Watch Survey uncovered the fact that data is often downloaded to home computers or sent outside the business via email. This may lead to damaged organizational reputations and may put organizations in violation of state or federal data protection laws.

Many Cybercrimes Go Unreported

More than half of the respondents (58%) believe they are more prepared to prevent, detect, respond to or recover from a cybercrime incident compared to the previous year. However, only 56% of the participants have a plan for reporting and responding to a cybercrime.

The public may not be aware of the number of incidents because almost three-quarters (72%), on average, of the insider incidents are handled internally without legal action or the involvement of law enforcement. However, cybercrimes committed by insiders are often more costly and damaging than attacks from outside.

“Based on our experiences with a variety of clients in different sectors, we actually think the situation is even worse than first glance,” said DeZabala, of Deloitte. “We believe that most cybercrimes go unreported, not because they are handled internally, but rather because they are never detected in the first place. This is a proverbial ‘tip-of-the-iceberg’ situation, and the implications are significant.”

Leading Practices in Preventing Cybercrime

According to the respondents, there are several security measures that are more effective in protecting an organization from a cybercrime. When trying to deter a criminal, businesses should be:

1. conducting periodic penetration tests of their systems
2. implementing periodic security education and awareness programs for their employees
3. delivering regular communication about security from senior management

The research also finds that businesses are taking steps to identify insider threats. Nearly one-third (32%) of survey respondents now monitor the online activities of employees who may be disgruntled or who have turned in their resignations. In this severe recession security risks have increased among employees who have been fired or laid off.

-more-

“While nothing is a guarantee in deterring cybercrime, implementing a strong protective barrier and providing employees with best practices is the key to protecting your organizations’ assets,” said Bob Bragdon, publisher of *CSO* magazine. “Most organizations have taken these attacks more seriously, and now fewer are being targeted; however, the threats are constantly changing so organizations must communicate, adapt and respond appropriately to a very fluid situation. With more than half of the respondents still concerned about cybercrime, it appears that investments and proactive behavior will continue to be a priority in IT security. “

About the 2010 CyberSecurity Watch Survey

The 2010 CyberSecurity Watch survey was conducted by *CSO* magazine in cooperation with the U.S. Secret Service, Software Engineering Institute CERT Program at Carnegie Mellon University and Deloitte. The survey was conducted from July 29, 2009 through August 20, 2009. An email invitation with a link to the survey was sent to *CSO* magazine readers/visitors and members of the US Secret Service’s Electronic Crime Task Forces. In all, 523 responses were collected. Margin of error is +/- 4 percentage points. Respondent answers cover the period between August 2008 and July 2009.

For complete survey results please visit:

<http://www.CSOonline.com/documents/pdfs/2010CyberSecurityResults.pdf>. 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 2010 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 a subsidiary of International Data Group (IDG), the world’s leading technology media, research and event company. Company information is available at <http://www.idg.com>.

About the Software Engineering Institute and the CERT Program

The Software Engineering Institute (SEI) is a U.S. Department of Defense federally funded research and development center operated by Carnegie Mellon University. The SEI helps organizations make measured 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 Deloitte

As used in this document, “Deloitte” means Deloitte & Touche LLP and Deloitte Services LP, which are separate subsidiaries of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of the legal structure of Deloitte LLP and its subsidiaries.

About the Secret Service’s Electronic Crimes Task Forces (ECTF)

The USA PATRIOT ACT OF 2001 (HR 3162, 107th Congress, First Session, October 26, 2001, Public Law 107-56) mandated the United States Secret Service to develop a national network of electronic crime task forces, based on the New York Electronic Crimes Task Force model, throughout the United States for the purpose of preventing, detecting and investigating various forms of electronic crimes, including potential terrorist attacks against critical infrastructure and financial payment systems.

-more-

The ECTF mission is to establish a strategic alliance of federal, state and local law enforcement agencies, private sector technical experts, prosecutors, academic institutions and private industry in order to confront and suppress technology-based criminal activity that endangers the integrity of the nation's financial payments systems and poses threats against the nation's critical infrastructure. More information on ECTF can be found at: <http://www.ectf.usss.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

Kelly Kimberland

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

###