



2012 CyberSecurity Watch Survey

How Bad is the Insider Threat?



© 2012 Carnegie Mellon University

NO WARRANTY

THIS MATERIAL OF CARNEGIE MELLON UNIVERSITY AND ITS SOFTWARE ENGINEERING INSTITUTE IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

This presentation may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other use. Requests for permission should be directed to the Software Engineering Institute at permission@sei.cmu.edu.

This work was created in the performance of Federal Government Contract Number FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center. The government of the United States has a royalty-free government-purpose license to use, duplicate, or disclose the work, in whole or in part and in any manner, and to have or permit others to do so, for government purposes pursuant to the copyright license under the clause at 252.227-7013.

CERT® is a registered mark owned by Carnegie Mellon University.





How Bad Is the Insider Threat?

2012 CyberSecurity Watch Survey -1

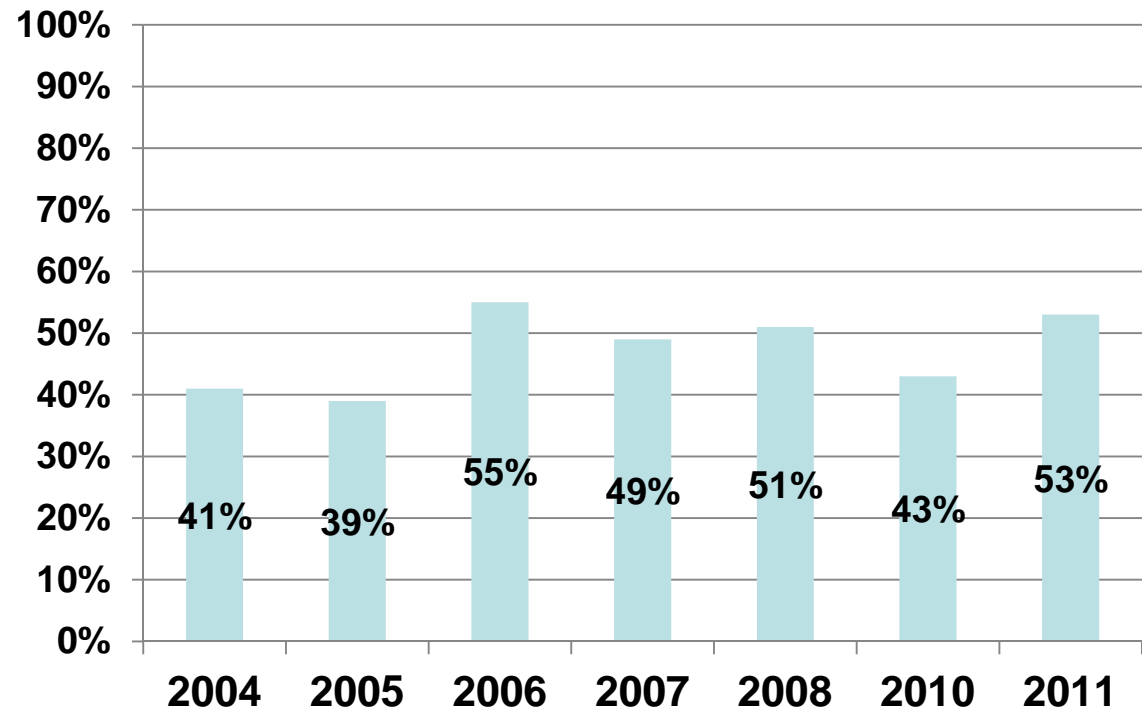
CSO Magazine, USSS, CERT & Deloitte

479 respondents

Percentage of Participants Who Experienced an Insider Incident

33% of organizations have more than 5000 employees

40% of organizations have less than 500 employees



Source: 2012 CyberSecurity Watch Survey, CSO Magazine, U.S. Secret Service, Software Engineering Institute CERT Program at Carnegie Mellon University and Deloitte, September 2012.

2012 CyberSecurity Watch Survey -2

51 % of respondents Damage caused by insider attacks more damaging than outsider attacks

Most common insider cyber incident

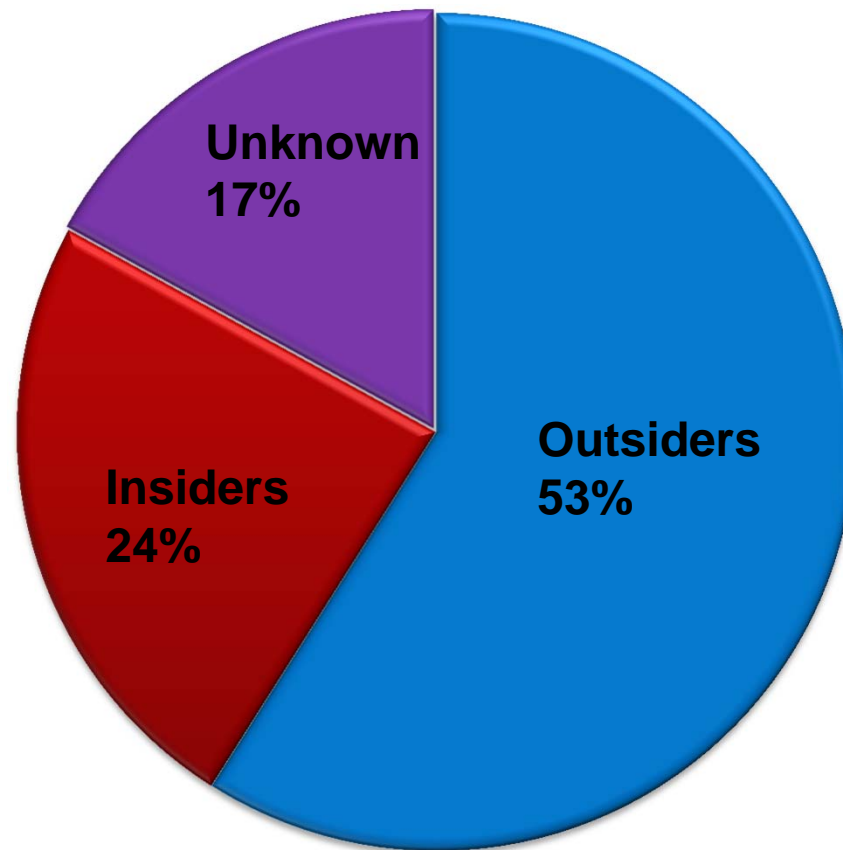
Unintentional exposure of private or sensitive data	(63%)
Access to/ use of information, systems or networks	(34%)
Theft of other (proprietary) info including customer records, financial records, etc..	(17%)
Theft of personally identifiable information (PII)	(15%)

Source: 2012 CyberSecurity Watch Survey, CSO Magazine, U.S. Secret Service, Software Engineering Institute CERT Program at Carnegie Mellon University and Deloitte, September 2012.



2012 CyberSecurity Watch Survey -3

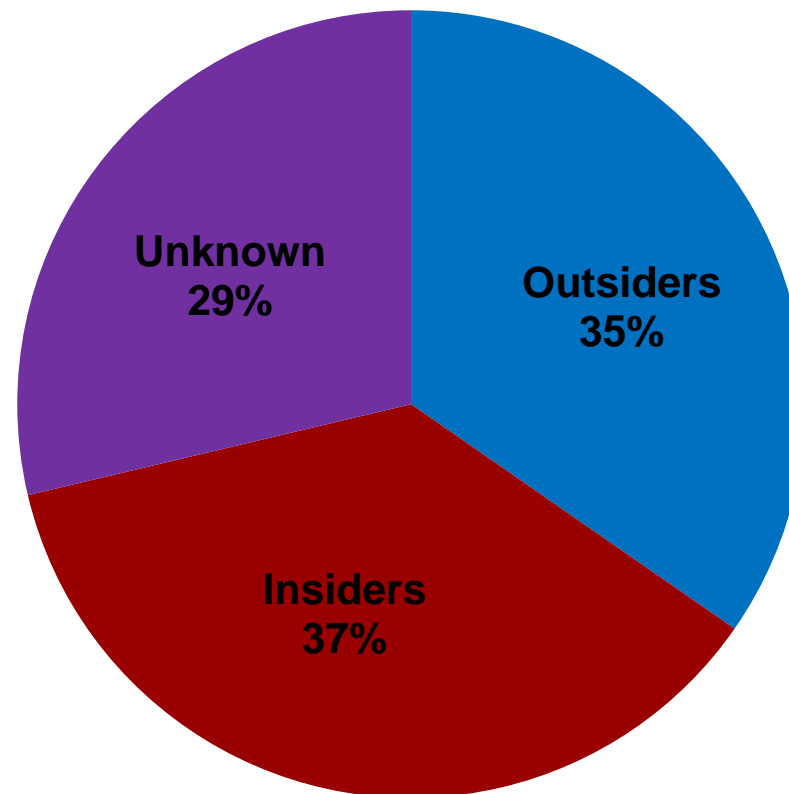
What percent of the Electronic Crime events are known or suspected to have been caused by :



Source: 2012 CyberSecurity Watch Survey, CSO Magazine, U.S. Secret Service, Software Engineering Institute CERT Program at Carnegie Mellon University and Deloitte, September 2012.

2012 CyberSecurity Watch Survey -4

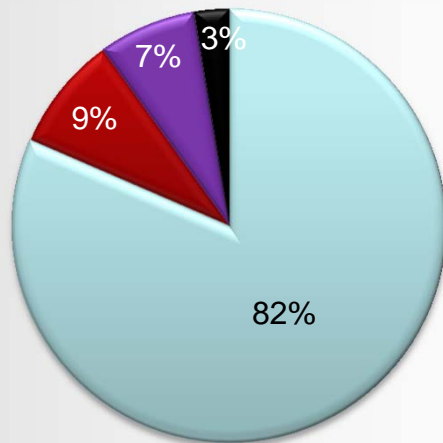
Which Electronic Crimes were more costly or damaging to your organization, those perpetrated by:



Source: 2012 CyberSecurity Watch Survey, CSO Magazine, U.S. Secret Service, Software Engineering Institute CERT Program at Carnegie Mellon University and Deloitte, September 2012.

2012 CyberSecurity Watch Survey -5

How Insider Intrusions Are Handled



- Internally (without legal action or law enforcement)
- Internally (with legal action)
- Externally (notifying law enforcement)
- Externally (filing a civil action)

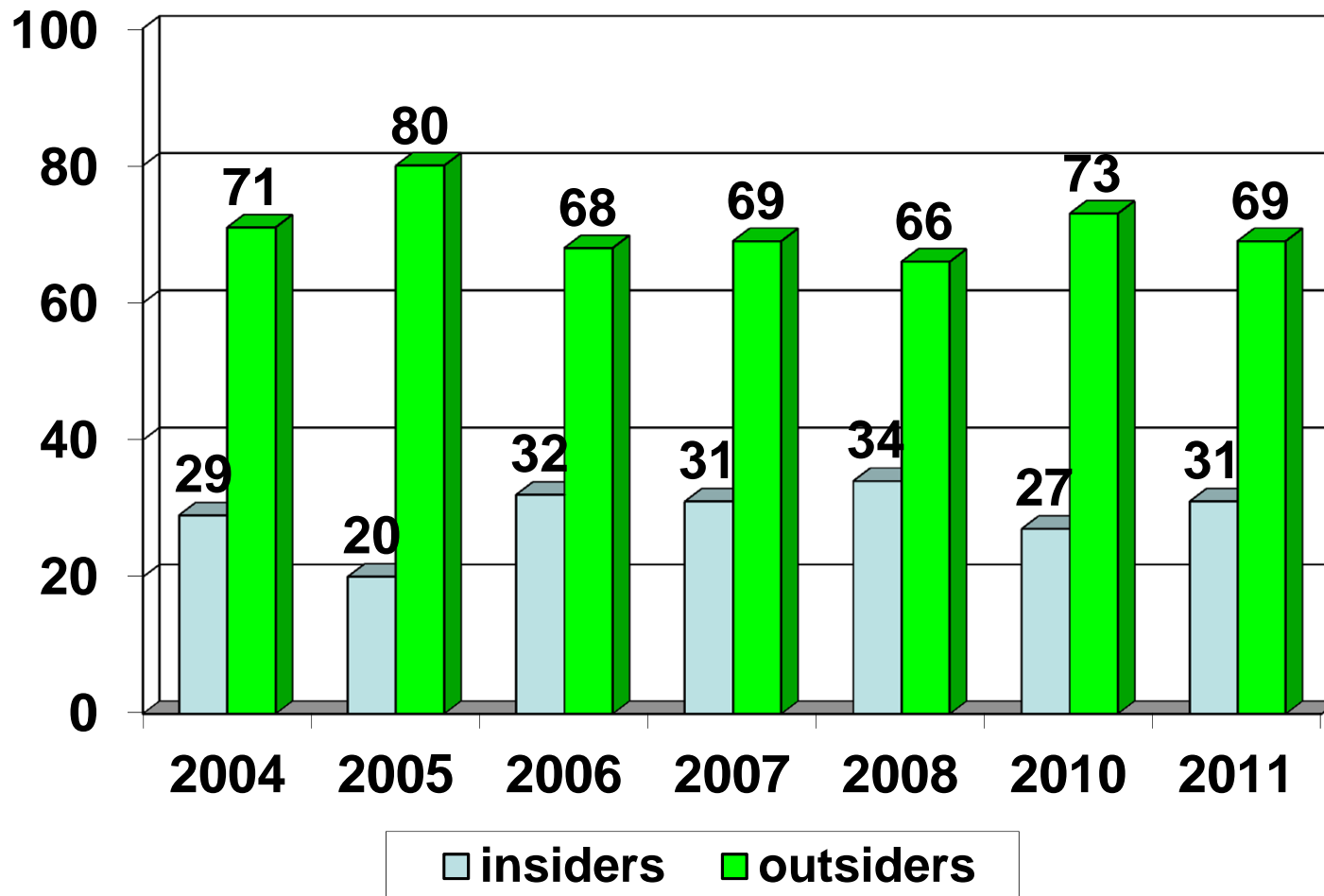
Reason(s) CyberCrimes were not referred for legal action

	2012	2011
Damage level insufficient to warrant prosecution	40%	42%
Could not identify the individual/ individuals responsible for committing the eCrime	37%	40%
Lack of evidence/not enough information to prosecute	34%	39%
Concerns about negative publicity	14%	12%
Concerns about liability	9%	8%
Concerns that competitors would use incident to their advantage	7%	6%
Prior negative response from law enforcement	6%	5%
Unaware that we could report these crimes	4%	4%
L.E. suggested incident was national security related	4%	N/A
Other	11%	11%
Don't know	20%	20%

Source: 2012 CyberSecurity Watch Survey, CSO Magazine, U.S. Secret Service, Software Engineering Institute CERT Program at Carnegie Mellon University and Deloitte, September 2012.

2012 CyberSecurity Watch Survey -6

Percentage of insiders versus outsiders



Source: 2012 CyberSecurity Watch Survey, CSO Magazine, U.S. Secret Service, Software Engineering Institute CERT Program at Carnegie Mellon University and Deloitte, September 2012.