



# 2013 US State of Cybercrime Survey

## How Bad is the Insider Threat?



## Report Documentation Page

*Form Approved*  
*OMB No. 0704-0188*

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

|  |                                    |   |                             |                     |                                 |
|--|------------------------------------|---|-----------------------------|---------------------|---------------------------------|
| 1. REPORT DATE<br><b>AUG 2013</b>  | 2. REPORT TYPE                     | 3. DATES COVERED<br><b>00-00-2013 to 00-00-2013</b> |                             |                     |                                 |
| 4. TITLE AND SUBTITLE<br><b>2013 US State of Cybercrime Survey: How Bad is the Insider Threat?</b>   |                                    | 5a. CONTRACT NUMBER                                 |                             |                     |                                 |
|  |                                    | 5b. GRANT NUMBER                                    |                             |                     |                                 |
|  |                                    | 5c. PROGRAM ELEMENT NUMBER                          |                             |                     |                                 |
| 6. AUTHOR(S)   |                                    | 5d. PROJECT NUMBER                                  |                             |                     |                                 |
|  |                                    | 5e. TASK NUMBER                                     |                             |                     |                                 |
|  |                                    | 5f. WORK UNIT NUMBER                                |                             |                     |                                 |
| 7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)<br><b>Carnegie Mellon University, Software Engineering Institute, Pittsburgh, PA, 15213</b> |                                    | 8. PERFORMING ORGANIZATION REPORT NUMBER            |                             |                     |                                 |
| 9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)  |                                    | 10. SPONSOR/MONITOR'S ACRONYM(S)                    |                             |                     |                                 |
|  |                                    | 11. SPONSOR/MONITOR'S REPORT NUMBER(S)              |                             |                     |                                 |
| 12. DISTRIBUTION/AVAILABILITY STATEMENT<br><b>Approved for public release; distribution unlimited</b>  |                                    |   |                             |                     |                                 |
| 13. SUPPLEMENTARY NOTES  |                                    |   |                             |                     |                                 |
| 14. ABSTRACT   |                                    |   |                             |                     |                                 |
| 15. SUBJECT TERMS  |                                    |   |                             |                     |                                 |
| 16. SECURITY CLASSIFICATION OF:  |                                    |   | 17. LIMITATION OF ABSTRACT  | 18. NUMBER OF PAGES | 19a. NAME OF RESPONSIBLE PERSON |
| a. REPORT<br><b>unclassified</b>   | b. ABSTRACT<br><b>unclassified</b> | c. THIS PAGE<br><b>unclassified</b>                 | <b>Same as Report (SAR)</b> | <b>9</b>            |                                 |

---

© 2013 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](mailto: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?*

# 2013 US State of Cybercrime Survey -1

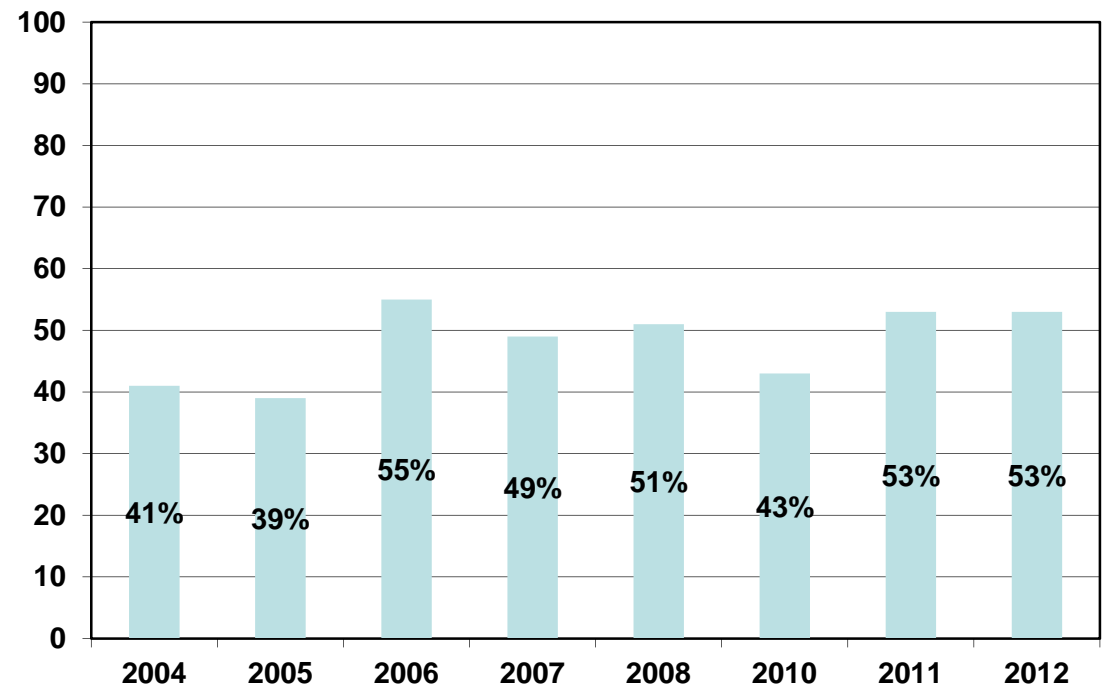
CSO Magazine, USSS, CERT & Deloitte

501 respondents

## Percentage of Participants Who Experienced an Insider Incident

*34% of organizations have more than 5000 employees*

*40% of organizations have less than 500 employees*



Source: 2013 US State of Cybercrime Survey, CSO Magazine, U.S. Secret Service, Software Engineering Institute CERT Program at Carnegie Mellon University and Price Waterhouse Cooper, June 2013.

# 2013 US State of Cybercrime Survey -2

*53 % of respondents* | Damage caused by insider attacks more damaging than outsider attacks

## Most common insider cyber incident

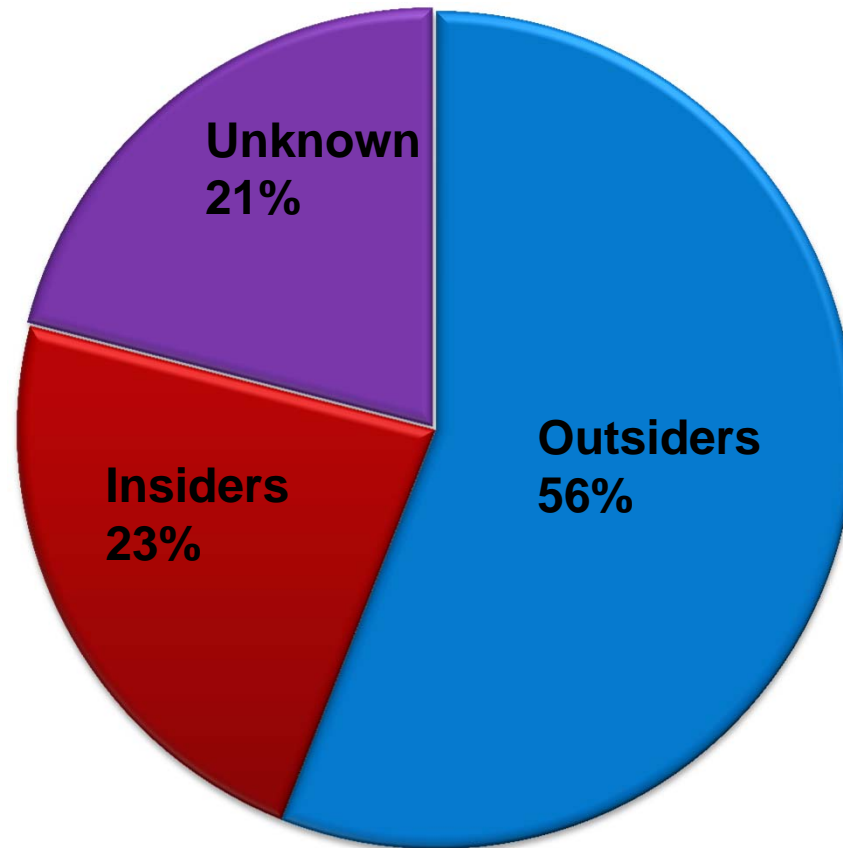
|   |       |
|---|-------|
| Unintentional exposure of private or sensitive data                                     | (34%) |
| Theft of intellectual property (IP)   | (34%) |
| Unauthorized access to/ use of information, systems or networks                         | (30%) |
| Theft of other (proprietary) info including customer records, financial records, etc... | (31%) |

Source: 2013 US State of Cybercrime Survey, CSO Magazine, U.S. Secret Service, Software Engineering Institute CERT Program at Carnegie Mellon University and Price Waterhouse Cooper, June 2013.

# 2013 US State of Cybercrime Survey -3

---

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

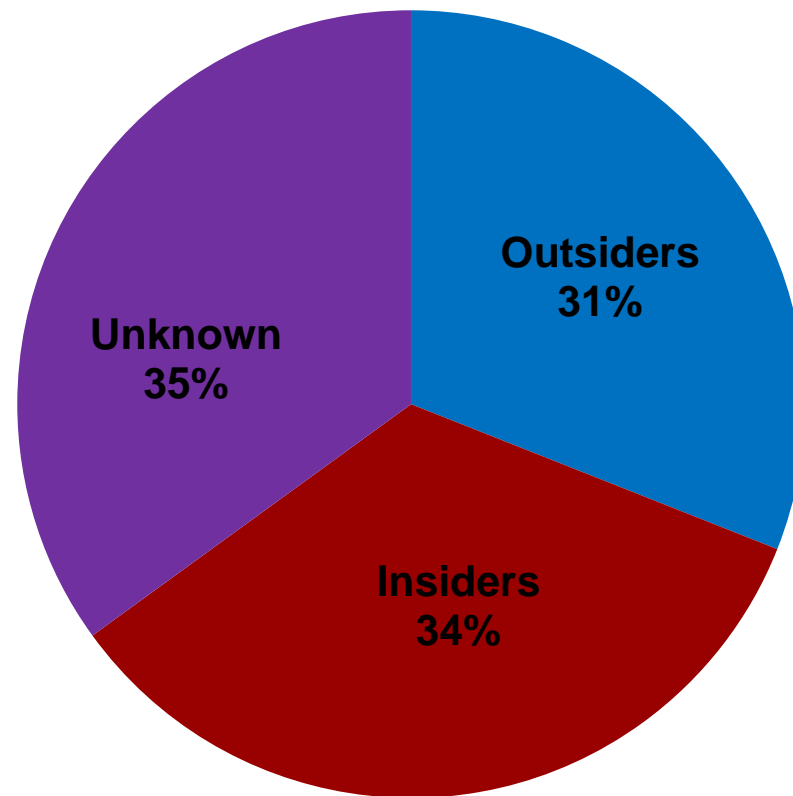


Source: 2013 US State of Cybercrime Survey, CSO Magazine, U.S. Secret Service, Software Engineering Institute CERT Program at Carnegie Mellon University and Price Waterhouse Cooper, June 2013.

# 2013 US State of Cybercrime Survey -4

---

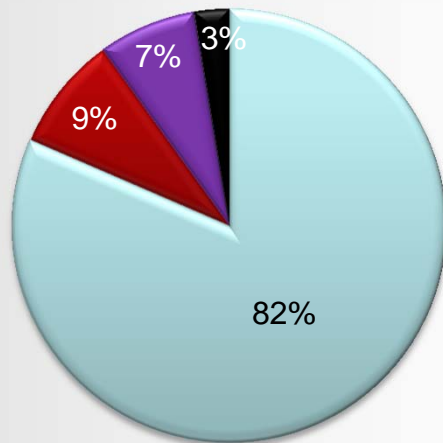
*Which Electronic Crimes were more costly or damaging to your organization, those perpetrated by:*



Source: 2013 US State of Cybercrime Survey, CSO Magazine, U.S. Secret Service, Software Engineering Institute CERT Program at Carnegie Mellon University and Price Waterhouse Cooper, June 2013.

# 2013 US State of Cybercrime 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)

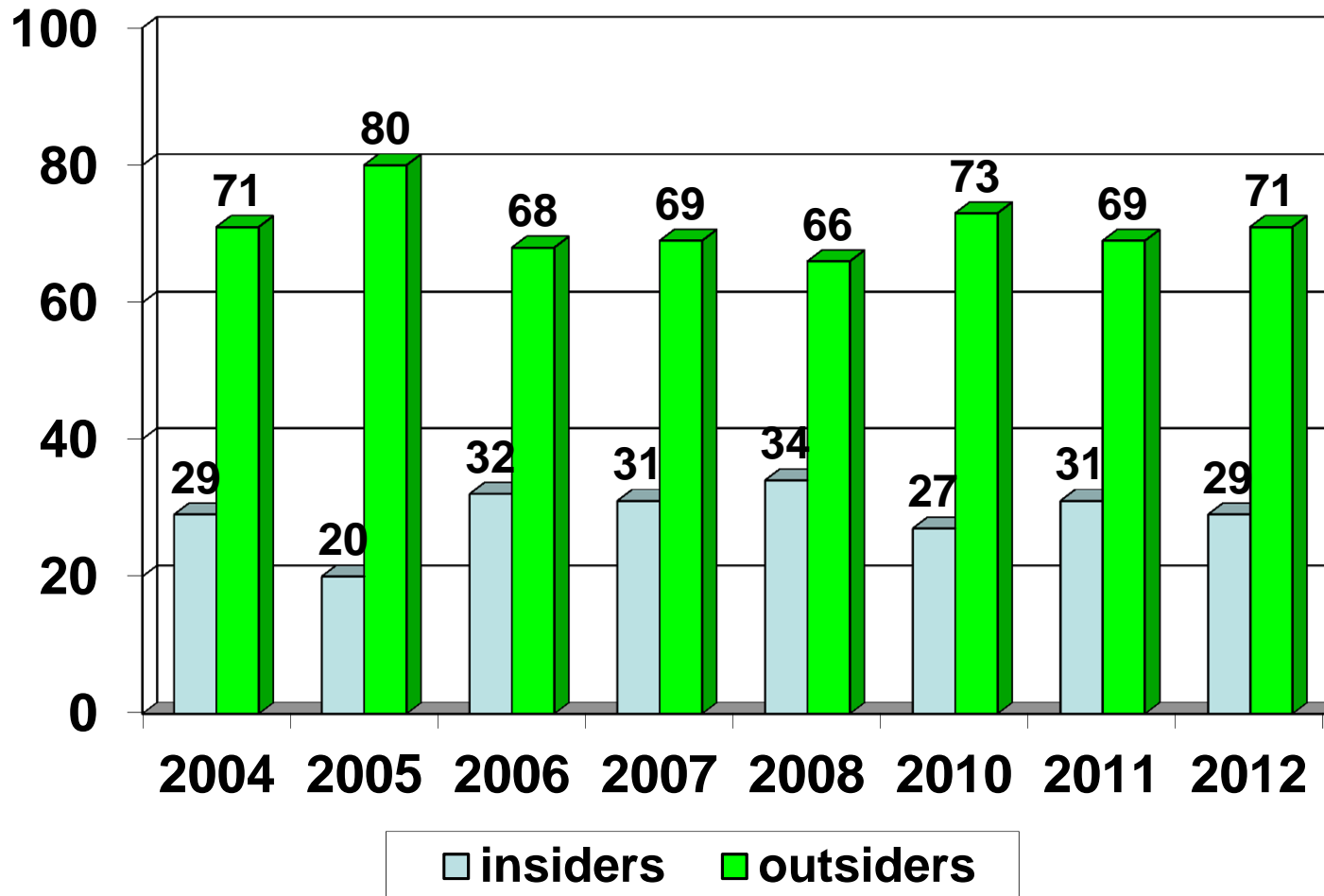
## Reason(s) CyberCrimes were not referred for legal action

|  | 2012 | 2011 |
|--|------|------|
| Damage level insufficient to warrant prosecution                                     | 36%  | 40%  |
| Lack of evidence/not enough information to prosecute                                 | 36%  | 34%  |
| Could not identify the individual/ individuals responsible for committing the eCrime | 32%  | 37%  |
| Concerns about negative publicity  | 9%   | 14%  |
| Concerns about liability   | 7%   | 9%   |
| Concerns that competitors would use incident to their advantage                      | 6%   | 7%   |
| Prior negative response from law enforcement   | 5%   | 6%   |
| Unaware that we could report these crimes  | 5%   | 4%   |
| L.E. suggested incident was national security related                                | 4%   | 4%   |
| Other  | 12%  | 11%  |
| Don't know   | 28%  | 20%  |

Source: 2013 US State of Cybercrime Survey, CSO Magazine, U.S. Secret Service, Software Engineering Institute CERT Program at Carnegie Mellon University and Price Waterhouse Cooper, June 2013.

# 2013 US State of Cybercrime Survey -6

*Percentage of insiders versus outsiders*



. Source: 2013 US State of Cybercrime Survey, CSO Magazine, U.S. Secret Service, Software Engineering Institute CERT Program at Carnegie Mellon University and Price Waterhouse Cooper, June 2013.