



CSO Magazine 2009 'State of the CSO' Survey

Executive Summary

Security Professionals Not Optimistic Cyber Security Will Improve Under Stimulus Plan

Security professionals lack confidence the homeland security and law enforcement provisions in President Obama's stimulus plan will improve cyber security in the United States, according to an exclusive survey conducted by CSO in March. More than half of the 256 security professionals responding (56 percent) are "not very confident" (24 percent) or "not at all confident" (31 percent) that cyber-security will improve under the current plan. Only one-third of security professionals surveyed are "very confident" (6 percent) or "somewhat confident" (26 percent) in President Obama's plan (12 percent aren't sure citing lack of familiarity with details in the plan). Additionally, almost one third of security professionals (32 percent) say they are not satisfied with national policy regarding security matters, up slightly from the 27 percent reported last year.

Breaking out the results by company size, more respondents in large companies lack confidence that homeland security and law enforcement provisions in the current stimulus plan will improve U.S. cyber security; nearly two-thirds of security professionals in companies with \$1 billion or more in annual revenue (65 percent) cite a lack of confidence versus 58 percent of their small company counterparts and 50 percent of those responding from mid-size organizations. Security professionals in the manufacturing sector are the least confident with over two-thirds "not very confident" (12 percent) or "not at all confident" (54 percent) that stimulus plan provisions will improve U.S. cyber security.

Security Awareness and Training Still Lags, Particularly for Mid-Market Companies

Although security training and employee awareness has improved from 5 years ago, room for improvement exists. Over one quarter of security professionals (27 percent) don't train employees in security areas such as visitor policies, physical and electronic access, email and Web usage while 30 percent don't train employees in the sanctions and consequences of a security policy breach. Thirty-five percent of respondents report that not all of their organizations' employees consider security to be part of their every day responsibilities while an equal number say managers within the organization don't understand their roles and responsibilities with regards to security.

Although more mid-market companies are incorporating security considerations into their business processes (72 percent versus 58 percent in 2008), fewer of these provide employees with security-related training. Just over half of security professionals in mid-market companies (54 percent) say their employees receive training in security policy, down from 65 percent last year. And only 48 percent of mid-market respondents say their employees are trained in the sanctions and consequences of a security policy breach, down from 56 percent last year. Roughly one-third of mid-market respondents (35 percent) disagree that all managers in their organizations understand their roles and responsibilities in regards to security, down from 28 percent in 2008.



Methodology

CSO magazine's "State of the CSO" survey was conducted with the objective of understanding how the role of the CSO continues to evolve in today's business climate. The survey was administered online to a sample of the CSO audience from March 9 to April 3, 2009. Findings shown are based on the responses of 256 security professionals from a broad range of industries including government and nonprofits (23 percent), financial services (20 percent), high tech, telecom and utilities (17 percent), healthcare (11 percent) and manufacturing (9 percent). Sixty eight percent of respondents are the single point of contact for security matters for their organizations' executives. Company size distribution by annual revenue is as follows: <\$100 million (small): 23 percent, \$100 million - \$999.9 million (mid-size): 20 percent, \$1 billion or more (large): 37 percent. The margin of error on a sample size of 256 is +/- 6.1%. Percentages may not sum to 100 due to rounding. Not all respondents answered every question.

Highlights by Question

Level of Responsibility

Security professionals responding are most likely to be in charge of information security (60 percent), business continuity/disaster recovery (44 percent) and security-related audit (38 percent). Privacy (59 percent), fraud protection (53 percent), investigations (52 percent) and security-related audit (52 percent) are the most frequently cited areas in which respondents are likely to be involved.

Reporting Structure

Thirty-two percent of security professionals surveyed report to the CIO or CTO while 20 percent report to the CEO/president.

Background

More security professionals across all size companies have an information systems background (77 percent versus 58 percent in 2008 and 52 percent in 2006). The percentage of respondents coming from law enforcement continues to decrease; 9 percent have a law enforcement background compared to 16 percent last year and 22 percent in 2006.

Degrees and Certifications

Certified Information Systems Security Professional (CISSP) certification is the most frequently mentioned degree or certifications held by respondents (30 percent) followed by MBA (25 percent). Twenty three percent hold some other advanced academic degree.

Tenure

Security professionals have been in their current position an average of 4 years, 10 months, relatively consistent with the 5 years reported last year.

Role of Security Function

The security leader's role is viewed by senior management as strategic and permanent by a higher percentage of respondents, continuing an upward trend from 5 years ago (70 percent versus 51 percent in 2006 and 17 percent in 2004). The percentage of small and mid-market respondents reporting that security considerations are a routine part of business processes increased from last year (small: 70 percent versus 57 percent in 2008, mid-size: 72 percent versus 58 percent).



Risk Management

Half of those responding say their organization's senior management placed more value on risk management in the past year, down from 62 percent last year. Forty-six percent report no change in the value senior management put on risk management in the past year, up from 33 percent in 2008.

Time Spent on Regulatory Obligations

Fifty-three percent of respondents say the percentage of their time spent attending to regulatory obligations increased over the past year, down slightly from 59 percent in 2008.

Budgeting Process

When asked which methods and calculations are applied in the security budgeting process, 38 percent of security professionals responding cite return on investment (ROI), 34 percent total cost of ownership (TCO) and 17 percent annual loss expectancy (ALE). Half of security professionals responding say they have no formal financial methodology. Forty-six percent use a formal enterprise risk management process or methodology that incorporates multiple types of risk beyond just information security risk or physical security risk.

Job Satisfaction

Overall, the percentage of respondents who are very satisfied with their job increased to 43 percent, from 34 percent in 2008.



Results by Question

Please indicate your level of responsibility/involvement in each of the following areas at your company	In charge	Involved	Not involved
Background checks	10%	28%	61%
Business continuity/disaster recovery	44%	48%	8%
Executive protection	16%	26%	58%
Fraud protection	20%	53%	27%
Homeland security	16%	38%	46%
Information security	60%	35%	5%
Intellectual property protection	34%	50%	16%
Investigations	29%	52%	19%
Personnel security	21%	39%	40%
Privacy	30%	59%	11%
Security of facilities/hard assets	23%	49%	27%
Security-related audit	38%	52%	10%

Are you the single point of contact for security matters for your organization's executives? (That is, do other executives in your company contact you first if they have a physical or information security question?)	Percent
Yes	68%
No	32%

To whom do you directly report?	Percent
CEO/president	20%
COO (Chief Operations Officer) or equivalent	11%
CFO (Chief Financial Officer) or equivalent	4%
CRO (Chief Risk Officer)	2%
CIO or CTO (Chief Information Officer or Technical Officer)	32%
CSO	7%
Head of Human Resources	3%
General Counsel/head of legal	1%
Audit committee (or other branch of Board of Directors)	2%
Head of facilities	1%
Other	18%



How long have you been in your current position?	Percent
Less than 1 year	10%
1 year to 2 years	18%
Between 2 and 3 years	16%
Between 3 and 5 years	17%
Between 5 and 10 years	23%
More than 10 years	15%
Mean (years)	4.80
Median (years)	3.65

What is your background?	Percent
Information systems	77%
Business operations (administration, sales, logistics etc.)	22%
Military	18%
Audit	16%
Physical security	12%
Law enforcement (police, Secret Service, FBI)	9%
Legal	2%
Other	7%

Which of the following degrees and/or certifications do you hold?	Percent
CISA	12%
CISSP	30%
CPP	5%
J.D.	2%
MBA	25%
Military and/or law enforcement rank	15%
PhD	2%
Other advanced academic degree	23%
Other corporate security	3%
Other infosec	21%
Other IT	19%
Other	22%



Please indicate how strongly you agree or disagree with the following statements.	Strongly Agree	Agree	Neither Agree nor Disagree	Disagree	Strongly Disagree
Senior management has established a security policy and auditing process.	25%	47%	14%	10%	3%
Senior management views the security leader's role as strategic and permanent.	23%	47%	18%	9%	3%
Security is viewed as essential to business as opposed to an overhead cost.	23%	38%	22%	14%	2%
Security considerations are a routine part of your company's business processes.	19%	46%	18%	14%	4%
All managers in the organization understand their roles and responsibilities in regards to security.	6%	30%	28%	28%	7%
All employees consider security to be part of their every day responsibilities.	7%	30%	27%	27%	8%
All employees receive training in all security policy topics (visitor policies, physical and electronic access, email and Web use).	20%	39%	14%	21%	6%
All employees are trained in the sanctions and consequences a security policy breach.	16%	38%	16%	23%	7%
Publicly reported data breaches cause senior management at my organization to place more emphasis on risk management	20%	41%	26%	10%	4%

In the past 12 months, has your organization's leadership placed more, less or the same value on risk management?	Percent
More value	50%
Less value	4%
No change	46%

In the past 12 months has the amount of time you spend on regulatory compliance increased, decreased, or remained the same?	Percent
Increased	53%
Decreased	2%
Remained the same	45%



Which of the following methods and calculations do you apply in the security budgeting process? Select all that apply.	Percent
Return on Investment (ROI)	38%
Total Cost of Ownership (TCO)	34%
Economic Value Added (EVA)	9%
Annual Loss Expectancy (ALE)	17%
Net Present Value (NPV)	11%
No formal financial methodology	50%

Does your organization use a formal Enterprise Risk Management process or methodology that incorporates multiple types of risk (in other words, not just information security risk or physical security risk)?	Percent
Yes	46%
No	54%

Rate your satisfaction with the following items	Very Satisfied	Somewhat Satisfied	Neither Satisfied nor Dissatisfied	Somewhat Dissatisfied	Very Dissatisfied
Your job overall	43%	39%	7%	8%	3%
Your organization's acceptance of/support for security	22%	43%	14%	15%	6%
The quality and relevance of PRODUCTS offered by security vendors	8%	54%	26%	11%	1%
The quality and relevance of SERVICES offered by security vendors	9%	45%	29%	13%	3%
The quality and relevance of security standards and best practice guidelines (ISO or NIST standards, for example. NOT meaning government regulations.)	17%	51%	23%	8%	<1%
National policy regarding security matters	5%	33%	31%	23%	9%



How confident are you that the homeland security and law enforcement provisions in President Obama's stimulus plan will improve cyber security in the United States?	Percent
Very confident	6%
Somewhat confident	26%
Not very confident	24%
Not at all confident	31%
Not sure – not familiar enough with plan	12%

What is your exact title?	Percent
CSO (Chief Security Officer)	6%
CRO (Chief Risk Officer)	<1%
CISO (Chief Information Security Officer)	12%
EVP, Senior. VP, VP of Security (incl. corporate, enterprise or global)	4%
Director of Security	16%
Manager of Security	11%
CEO, President, Owner, Partner	4%
CFO, Treasurer, Controller	1%
COO, General Manager, Exec. Director, Managing Director	2%
Privacy or Compliance -related title	<1%
EVP, Senior. VP, VP (other than security)	4%
CIO/CTO	10%
DIR/MGR (other than security)	10%
Gov't/Military titled personnel	2%
Consultant	2%
Other	16%

What is your organization's primary business?	Percent
Government and Nonprofits (including education)	23%
Financial Services (banking, insurance, brokerage)	20%
High Tech, Telecom & Utilities	17%
Healthcare (providers and pharmaceuticals)	11%
Manufacturing (including automotive, aerospace & defense, construction, engineering, chemical, metals & mining)	9%
Services (legal, consulting, real estate)	6%
Retail, Wholesale and Distribution	4%
Advertising/Marketing/PR/Media (publishing, broadcast, online)	4%
Travel and Leisure (cruiselines, hotels, theme parks, casinos)	3%
Transportation (airlines, trucking, railroads, shipping, logistics)	3%



Please select the dollar amount that best represents the annual gross sales or revenues for your corporation or firm, include all plants, divisions, branches, parents, and subsidiaries worldwide.	Percent
\$5 billion or more	16%
\$1 billion to \$4.9 billion	22%
\$100 million to \$999.9 million	20%
Less than \$100 million	23%
Not applicable (e.g., non-profit, government, union)	13%
Not sure	7%

###