



**The Operations Security
Professional's Association
(OSPA)**

State Of OPSEC Survey

4th Quarter 2009

All data within is cleared for public release. No classified, sensitive or FOUO information shall be present in this report.

OSPA 2009 State Of OPSEC Survey

Table of Contents

Executive Summary	1
Survey Questions	2
Key Findings	3
Data Collection Methodology	5
Results.....	5
Limitations of the Data	10
Conclusions.....	10

OSPA 2009 State Of OPSEC Survey

List of Tables

Question 1: What is your industry/enterprise?.....	5
Question 2: What is the size of your organization?	6
Question 3: In which country is your organization based (or international)?.....	6
Question 4: Does your organization have a formal OPSEC program?	6
Question 5: Are employees required to receive OPSEC instruction and agree to policies as a requirement for employment?.....	7
Question 6: How many personnel in your organization are primarily to OPSEC duties?	7
Question 7: If personnel are assigned OPSEC as a secondary duty, what is their primary job function?	7
Question 8: How much funding does your organization allocate to OPSEC?.....	7
Question 9: How would you rate your organization's understanding and implementation of OPSEC?	8
Question 10: Has your organization experienced a security breach of any type or magnitude within the last year, and in which OPSEC was determined to be a factor? (either where better OPSEC practices could have prevented the breach, or OPSEC-related concepts contributed to the breach).....	8
Question 11: Do you feel that your customers, clients or stakeholders are confident in your ability to protect their information or data?	8
Question 12: Do you feel that your customers, clients or stakeholders are confident in your ability to protect your own information or data?	8
Question 13: Has your organization completed a formal OPSEC survey within the last year?	8
Question 14: Does your organization have a security plan that addresses personal electronic devices?.....	9
Question 15: Does your organization have an OPSEC plan?	9
Question 16: Which of the following (from a list) would you consider to be an actual or imminent threat to your organization?	9
Question 17: Which for the following (from a list) would you consider to be a potential impact of an OPSEC compromise?.....	9
Question 18: Has your organization implemented any countermeasures in order to address OPSEC-related risks or concerns?	10

OSPA 2009 State Of OPSEC Survey

Question 19: Do you feel that your organization would benefit from free or subsidized OPSEC instruction? 10

Question 20: Do you feel that your organization would benefit from external OPSEC support, such as guidance, awareness material or Subject Matter Expert availability?..... 10

OSPA 2009 State Of OPSEC Survey

2009 State of OPSEC Survey

4th Quarter 2009

EXECUTIVE SUMMARY

The Operations Security Professional's Association (OSPA) conducted the first annual State of OPSEC Survey (SOS). The objective of this multinational survey was to provide information and trend analysis for OPSEC professionals and other security positions. OSPA has made this information available to enable organizations, institutions and other entities to consider current trends, and develop and promote internal policy and strategies accordingly.

OSPA compiled the data for this effort over an approximately 30 day period, from December 1, 2009 to December 31, 2009, with the intent of establishing an initial baseline, upon which future survey data may be compared. It is anticipated, however, that subsequent SOS efforts shall expand in scope, resulting in a more comprehensive data set.

The SOS is a voluntary Cross-Sectional survey with measures taken to ensure randomness through representative sampling. OSPA conducted a 20-question survey that was made available on the website, as well as via telephonic interview, targeting security, management and other personnel at all levels across multiple industries and geographic locations. In order to better obtain a representative sample, industries that were not represented were randomly contacted via telephone to obtain a more accurate sample base.

In total, 126 responses were obtained from across sixteen industries. Representative industries are:

- Construction (3)
- Consulting, Non-Government (2)
- Education (5)
- Finance (6)
- Government (64)
 - Includes State Government, Federal Government, Government Agencies, Military and Government Contractors/Consultants
- Health Care (8)
- Information Technology (1)
- Law Enforcement (9)
- Manufacturing (2)
- Maritime (2)
- News/Journalism (3)
- Real Estate (2)
- Research and Development (4)
- Security and Investigations (4)
- Social Work (3)
- Software (2)
- Telecommunications (3)

OSPA 2009 State Of OPSEC Survey

- Self-Employed, Other (3)
 - Includes Trade Associations, Retired, Neighborhood Watch, etc

The strength of this survey is the ability to examine patterns by company size and industry. In order to eliminate statistical bias, a wide selection of resources were culled in such a way as to reach a varied sample, to include LinkedIn, Facebook, and multiple security related newsgroups and forums. All responses were collected on an anonymous basis, with original responses not retained for purposes other than data aggregation. This was done to eliminate any possibility of organizational-specific information being used for purposes outside of the scope of this survey.

SURVEY QUESTIONS

The following questions were asked of each survey respondent:

1. What is your industry/enterprise?
2. What is the size of your organization?
3. In which country is your organization based (or international)?
4. Does your organization have a formal OPSEC program?
5. Are employees required to receive OPSEC instruction and agree to policies as a requirement for employment?
6. How many personnel in your organization are primarily to OPSEC duties?
7. If personnel are assigned OPSEC as a secondary duty, what is their primary job function?
8. How much funding does your organization allocate to OPSEC?
9. How would you rate your organization's understanding and implementation of OPSEC?
10. Has your organization experienced a security breach of any type or magnitude within the last year, and in which OPSEC was determined to be a factor? (either where better OPSEC practices could have prevented the breach, or OPSEC-related concepts contributed to the breach)
11. Do you feel that your customers, clients or stakeholders are confident in your ability to protect their information or data?
12. Do you feel that your customers, clients or stakeholders are confident in your ability to protect your own information or data?
13. Has your organization completed a formal OPSEC survey within the last year?
14. Does your organization have a security plan that addresses personal electronic devices?
15. Does your organization have an OPSEC plan?
16. Which of the following (from a list) would you consider to be an actual or imminent threat to your organization?
17. Which for the following (from a list) would you consider to be a potential impact of an OPSEC compromise?
18. Has your organization implemented any countermeasures in order to address OPSEC-related risks or concerns?
19. Do you feel that your organization would benefit from free or subsidized OPSEC instruction?
20. Do you feel that your organization would benefit from external OPSEC support, such as guidance, awareness material or Subject Matter Expert availability?

OSPA 2009 State Of OPSEC Survey

KEY FINDINGS:

Security Breaches in which OPSEC was a factor

Multiple respondents reported that they had experienced a security breach in the previous year which could be attributed to an OPSEC lapse of any magnitude.

Of the responses:

- 33% reported that a such a breach had occurred
- 58% reported that no such breach had occurred
- 8% did not know if such a breach had occurred

Affect of security breaches on customer, client and stakeholder confidence

A greater number of respondents reported a lack of customer, client or stakeholder (CCS) confidence when they had experienced an OPSEC-related security breach within the last year than those that had not experienced such a brief. It could therefore be concluded that a security breach gravely impacts the CCS perception of Critical Information protection capabilities.

Specifically:

- Of those that reported a breach, 43% reported a loss of CCS confidence in the ability to protect *both* CCS and their own data
- Of those that reported a breach, 50% reported a loss of CCS confidence in the ability to protect *either* CCS or their own data
- Of those that reported a breach, 19% “didn’t know” how the brief affected CCS perception of one of the two categories

Conversely, of those that did not report a breach, only 3% reported a loss of CCS confidence in the ability to protect *both* CCS and their own data, 9% reported a loss of CCS confidence in the ability to protect *either* CCS or their own data and 14% “didn’t know” how the brief affected CCS perception of one of the two categories.

Request for assistance

Most respondents (60%) indicated that they felt that their organizations would benefit from either free/subsidized OPSEC training or external OPSEC support, such as guidance, awareness material or SME availability.

47% of respondents either already receive some form of support, or “didn’t know” if they would, or how they would, benefit from support.

3% of respondents did not feel that they would benefit from external assistance or support.

OSPA 2009 State Of OPSEC Survey

Given the diverse nature of the State of OPSEC Survey, it may be concluded that the “Non-OPSEC” personnel (IT, IA, etc) reached with this survey are not aware of, or not utilizing, available OPSEC support.

Availability of OPSEC personnel

Approximately half of respondents reported that their organization did not have a dedicated position for OPSEC.

Findings include:

- 49% reported that there were “0” dedicated OPSEC positions in their organization.
- Of those organizations that had no OPSEC personnel, 39% did not have individual(s) to fill the role as a secondary duty.
- Of those organizations that had no OPSEC personnel as either a primary or secondary duty, 100% felt that their organizational understanding and implementation of OPSEC was either “Failing”, “Poor” or “Needs improvement”. Some respondents reported their understanding or implementation as “N/A” or “Don’t know”.
- Of those organizations that had no OPSEC personnel in a primary role, but did have one or more personnel performing OPSEC as a secondary duty, 50% reported their understanding and implementation of OPSEC as either “Average”, “Very Good” or “Excellent”.
- Of those organizations that had one or more dedicated OPSEC positions, 67% felt that their organizational understanding and implementation of OPSEC was either “Average”, “Very Good” or “Excellent”.

A correlation exists between the availability of OPSEC personnel and the reported organizational understanding of OPSEC implementation.

OSPA 2009 State Of OPSEC Survey

DATA COLLECTION METHODOLOGY

OSPA began survey creation and coordination in September of 2009. This lead time was established in order to allow for question creation and testing, as well as subject coordination.

Pilot Test. The research team conducted a pretest of the contact procedures and the questionnaire. The contact procedures were pre-tested to insure that they allowed us to determine the correct respondent quickly, to exclude online based interviews. During the administration of the pre-test questionnaire, if the respondent hesitated when responding, we asked the respondent to explain the difficulty he or she was having answering the question. We also asked respondents follow-up questions, such as if they had difficulty understanding certain terms, if any of the questions did not apply to them and why, and if there was something we did not ask but should have in order to better understand the organizational perspective. Once the pilot interviews were completed, we determined that the questionnaire required minimal modification.

Advance Letter. An introductory letter was provided to or read to all respondents. For online respondents, this information was presented in the form of a “splash screen”, which required acknowledgement prior to continuation. The purpose of this letter was to introduce the study, emphasize confidentiality and to explain respondent’s rights.

Question Selection. Survey questions were selected based on the relevance to an initial baseline and likelihood of positive or negative change over time. It is anticipated that this probability of change shall allow for the determination of methodology or implementation change based on multiple factors, to include funding, personnel allocation, organizational understanding and implementation and Customer, Client and Stakeholder (CCS) confidence.

Survey Delivery. In order to achieve a true random sampling, wide dissemination of the survey link was crucial. The survey direct URL (http://www.opsecprofessionals.org/2009_OPSEC_Survey.html) was distributed to OSPA members, as well as shared on security-related websites, forums, chat rooms and messaging boards. No attempt was made to target a particular demographic in order to seek a wide sample. In certain cases, where a particular industry was not represented to any degree, multiple organizations within that industry were contacted via email or telephone on a strictly random basis with no regard to size or location.

RESULTS

The following tables document the question and subsequent responses. Note that for all entries, rounding shall allow for a statistical spread of $\pm 0.5\%$ per response:

Question 1: What is your industry/enterprise?		
Response	Number	Percent
Construction	3	2%
Consulting, Non-Government	2	2%
Education	5	4%
Finance	6	5%
Government (Includes State Government, Federal Government, Government Agencies, Military and Government Contractors/Consultants)	64	50%
Health Care	8	6%
Information Technology	1	1%

OSPA 2009 State Of OPSEC Survey

Law Enforcement	9	7%
Manufacturing	2	1%
Maritime	2	1%
News/Journalism	3	2%
Real Estate	2	1%
Research and Development	4	3%
Security and Investigations	4	4%
Social Work	3	2%
Software	2	1%
Telecommunications	3	2%
Self-Employed / Other (Includes Trade Associations, Retired, Neighborhood Watch, etc)	3	2%
Total Statistical Variance		4%

It is noted that Government respondents comprise the bulk of collected data. This is attributed to the prevalence and successful directives regarding OPSEC implementation within the Government sectors. It is hoped that future surveys will see an increased percentage of respondents from additional industries.

Question 2: What is the size of your organization?		
Response	Number	Percent
1-99	34	27%
100-499	28	22%
500-1,499	16	13%
1,500-9,999	28	22%
10,000-49,000	7	5%
50,000 or more	13	10%
Statistical Variance		1%

Question 3: In which country is your organization based (or international)?		
Response	Number	Percent
Australia	5	4%
Canada	8	6%
Germany	3	3%
International	9	7%
United Kingdom	4	3%
United States	97	77%
Total Statistical Variance		1%

Question 4: Does your organization have a formal OPSEC program?		
Response	Number	Percent
Yes	76	60%
No	35	28%
Don't Know	3	2%
Have an Informal Policy	6	5%
Policy Under Development	6	5%

OSPA 2009 State Of OPSEC Survey

Total Statistical Variance		0%
----------------------------	--	----

Question 5: Are employees required to receive OPSEC instruction and agree to policies as a requirement for employment?

Response	Number	Percent
Yes	68	54%
No	54	43%
Don't Know	4	3%
Total Statistical Variance		0%

Question 6: How many personnel in your organization are primarily dedicated to OPSEC duties?

Response	Number	Percent
0	62	49%
1-2	35	28%
2-5	7	6%
5+	22	17%
Total Statistical Variance		0%

Note that those reporting 5+ dedicated OPSEC personnel were largely Government personnel.

Question 7: If personnel are assigned OPSEC as a secondary duty, what is their primary job function?

Response	Number	Percent
None or NA	74	59%
Information Technology	14	11%
Information Security	20	16%
Physical Security	20	16%
Emergency Management	1	1%
Information Assurance	2	1%
Management	13	10%
Other Information Operations	5	4%
External (Law Enforcement, Security Company)	2	1%

Note that responses do not equal 100% due to multiple reporting options. Data collected represents the number of respondents that gave a particular answer.

Question 8: How much funding does your organization allocate to OPSEC?

Response	Number	Percent
Don't Know	33	26%
None	41	33%
\$1-1,000	27	21%
\$1,001-5,000	8	6%
\$5,001-10,000	2	1%
\$10,000+	15	12%
Total Statistical Variance		1%

OSPA 2009 State Of OPSEC Survey

Question 9: How would you rate your organization's understanding and implementation of OPSEC?		
Response	Number	Percent
NA	2	1%
Don't Know	5	4%
Failing	12	10%
Poor	15	12%
Needs Improvement	31	23%
Average	24	19%
Good	0	0%
Very Good	20	16%
Excellent	17	13%
Total Statistical Variance		2%

Not including those that rated themselves "NA" or "Don't Know", 45% of respondents rated themselves as "Needs Improvement" or below. 48% rated themselves as "Average" or above.

Question 10: Has your organization experienced a security breach of any type or magnitude within the last year, in which OPSEC was determined to be a factor? (either where better OPSEC practices could have prevented the breach, or OPSEC-related concepts contributed to the breach)		
Response	Number	Percent
Yes	42	33%
No	74	59%
Don't Know	10	8%
Total Statistical Variance		0%

Question 11: Do you feel that your customers, clients or stakeholders are confident in your ability to protect their information or data?		
Response	Number	Percent
Yes	81	64%
No	28	22%
Don't Know	17	13%
Total Statistical Variance		1%

Question 12: Do you feel that your customers, clients or stakeholders are confident in your ability to protect your own information or data?		
Response	Number	Percent
Yes	92	73%
No	21	17%
Don't Know	13	10%
Total Statistical Variance		0%

Question 13: Has your organization completed a formal OPSEC survey within the last year?		
Response	Number	Percent
Yes	36	29%
No	74	59%
Don't Know	16	13%

OSPA 2009 State Of OPSEC Survey

Total Statistical Variance		1%
----------------------------	--	----

Note that multiple respondents volunteered that they have completed an OPSEC survey, but not within the last year.

Question 14: Does your organization have a security plan that addresses personal electronic devices?		
Response	Number	Percent
Yes	95	75%
No	24	19%
Don't Know	7	5%
Total Statistical Variance		1%

Question 15: Does your organization have an OPSEC plan?		
Response	Number	Percent
Yes	68	54%
No	51	40%
Don't Know	7	5%
Total Statistical Variance		1%

Question 16: Which of the following (from a list) would you consider to be an actual or imminent threat to your organization?		
Response	Number	Percent
Internal Threats	51	40%
Foreign Intelligence Service (FIS)	38	30%
Hackers	57	45%
Corporate Espionage	26	20%
International Terrorism	20	16%
Domestic Terrorism	24	19%
Criminals	3	2%
Don't Know	1	1%

Note that responses do not equal 100% due to multiple reporting options. Data collected represents the number of respondents that gave a particular answer.

Question 17: Which of the following (from a list) would you consider to be a potential impact of an OPSEC compromise?		
Response	Number	Percent
Financial Loss	37	29%
Loss Of Personnel Safety	53	42%
Loss of Customer, Client or Stakeholder (CCS) Confidence	59	47%
Loss of Sensitive Records	10	8%
Loss of sensitive US Technology	1	1%
Compromise of Critical Information	1	1%
Ability to Accomplish Mission	17	13%

Note that responses do not equal 100% due to multiple reporting options. Data collected represents the number of respondents that gave a particular answer. It must be noted that a very small percentage (1% in

OSPA 2009 State Of OPSEC Survey

each case) felt that a loss of sensitive technology and Critical Information was a significant potential impact of an OPSEC compromise.

Question 18: Has your organization implemented any countermeasures in order to address OPSEC-related risks or concerns?

Response	Number	Percent
Don't Know	11	9%
Have Not attempted to identify OPSEC risks or concerns	7	6%
Have Not identified OPSEC risks or concerns	6	5%
Yes	84	67%
No	18	14%
Total Statistical Variance		1%

Question 19: Do you feel that your organization would benefit from free or subsidized OPSEC instruction?

Response	Number	Percent
Don't Know	20	16%
Already Have	30	24%
Yes	69	55%
No	7	6%
Total Statistical Variance		1%

Question 20: Do you feel that your organization would benefit from external OPSEC support, such as guidance, awareness material or Subject Matter Expert availability?

Response	Number	Percent
Don't Know	22	17%
Already Have	25	20%
Yes	67	53%
No	12	10%
Total Statistical Variance		0%

LIMITATIONS OF THE DATA

When delving deeper into specific issues, it will be important to consider the number of organizations that respond, and to take measures to increase responsiveness among Civilian-sector organizations. Furthermore, additional survey diversity shall be sought by increasing the evaluation sample size.

CONCLUSIONS

OPSEC is a critical addition to any organizational or individual security posture, and one that is being increasingly utilized by security personnel. However, based on the results of this SOS Survey, it is apparent that a compelling need exists for additional resources.

It is a rapidly expanding field, which is a requirement for the rapidly changing threats to personnel and organizations. Annually, additional SOS surveys will be conducted to track changes and expansion within the OPSEC discipline, with the intention of assisting in the allocation of resources and capabilities.