The Operations Security Professional's Association (OSPA)

State Of OPSEC Survey

4th Quarter 2010

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

OSPA 2010 State Of OPSEC Survey

Table of Contents

OSPA 2010 State Of OPSEC Survey

List of Tables

2010 State of OPSEC Survey

4th Quarter 2010

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, 2010 to December 31, 2010, 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.

This is the second annual survey, with information from this instance being compared against the baseline collected in 2009.

In total, 572 responses were obtained from across sixteen self-identified industries. This is an increase in 446 respondents from 2009. Representative industries are:

- Construction (17)
- Consulting, Non-Government (6)
- Education (43)
- Finance (28)
- Government (175)
    - Includes State Government, Federal Government, Government Agencies, Military and Government Contractors/Consultants
- Health Care (16)
- Information Technology (56)
- Law Enforcement (44)
- Manufacturing (9)
- Maritime (7)
- News/Journalism (18)
- Real Estate (5)
- Research and Development (3)
- Security and Investigations (18)

- Software (5)
- Telecommunications (32)
- Travel (54)
- Self-Employed, Other (36)
    - 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, direct contact, print media 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.

The option of "decline to answer" was made available for certain questions. These responses did not represent a statistically significant portion of any response. In the rare case that this was selected, that answer was not counted towards the total.

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 2010 State Of OPSEC Survey

21. Does your organization make use of any of the named OPSEC tools?
22. Has your organization modified its OPSEC program or posture in response to the recent "WikiLeaks" incident?
23. Does your organization create its own OPSEC awareness materials, to include posters, labels, videos, etc?
24. Does your organization have a threat statement or other formal threat document?

OSPA 2010 State Of OPSEC Survey

KEY FINDINGS:

1. Increase in awareness of the threats related to international and domestic terrorism
When asked "Which of the following (from a list) would you consider to be an actual or imminent threat to your organization," an increased number of respondents indicated that both international and domestic terrorism were a significant concern.

Of 572 respondents:
215 (58%) indicated that International Terrorism was an actual or imminent threat, representing an increase of 42% from 2009.
122 (33%) indicated that Domestic Terrorism was an actual or imminent threat, representing an increase of 14% from 2009.

2. Utilization of free/subsidized OPSEC instruction and other methods of OPSEC support
When asked "Do you feel that your organization would benefit from free or subsidized OPSEC instruction" and "Do you feel that your organization would benefit from external OPSEC support, such as guidance, awareness material or Subject Matter Expert availability," an increased number of respondents indicated that they are now utilizing such resources. When clarification was volunteered by the respondent, sources included IOSS, OSPA, 1st IO and similar entities.

Of 572 respondents:
136 (37%) indicated that their organizations are currently benefiting from free or subsidized instruction, representing an increase of 13% from 2009.
136 (37%) also indicated that their organizations already benefit from external OPSEC support, such as guidance, awareness material or SME availability, representing an increase of 17% from 2009.

It is interesting to note that the responses to questions 19 and 20 were nearly identical, as they were in 2009.

3. Modification of OPSEC programs or postures in response to real-world threats
When asked "has your organization modified its OPSEC program or posture in response to the recent 'WikiLeaks' incident," 57% indicated that they had done so, while 23% indicated that they had not. This also corresponds to an increase in awareness of internal threats, where 68% of respondents indicated that this represented a threat to their organization.

OSPA 2010 State Of OPSEC Survey

Data Collection Methodology

OSPA began survey creation and coordination in October of 2010. 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/2010_OPSEC_Survey.html) was distributed to OSPA members, as well as shared on security-related websites, forums, chat rooms and messaging boards. Similarly, historically under-represented industries were directly and randomly contacted in order to ensure accuracy. 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 ±.5% per response. For that reason, totals may not equal 100%.

Question 1: What is your industry/enterprise?				
Response	**2009 number**	**2010 Number**	**2010 Percent**	**Change**
Construction	3	17	3%	+1%
Consulting, Non-Government	2	6	1%	-1%
Education	5	43	8%	+4%
Finance	6	28	5%	None
Government (Includes State Government, Federal Government, Government Agencies, Military and Government Contractors and	64	175	31%	-19%

Consultants)				
Health Care	8	16	3%	-3%
Information Technology	1	56	10%	+9%
Law Enforcement	9	44	8%	+1%
Manufacturing	2	9	2%	+1%
Maritime	2	7	1%	None
News/Journalism	3	18	3%	+1%
Real Estate	2	5	1%	None
Research and Development	4	3	1%	-2%
Security and Investigations	4	18	3%	-1%
Social Work	3	0	0%	-2%
Software	2	5	1%	None
Telecommunications	3	32	5%	+3%
Travel	0	54	10%	+10%
Self-Employed / Other (Includes Trade Associations, Retired, Neighborhood Watch, etc)	3	36	6%	+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. This is anticipated to be an enduring finding.

Question 2: What is the size of your organization?				
Response	**2009 Number**	**2010 Number**	**Percent**	**Change**
1-99	34	114	10%	-17%
100-499	28	74	13%	-9%
500-1,499	16	208	37%	+24%
1,500-9,999	28	56	10%	+12%
10,000-49,000	7	75	13%	+8%
50,000 or more	13	45	8%	-2%

Question 3: In which country is your organization based (or international)?				
Response	**2009 Number**	**2010 Number**	**Percent**	
Australia	5	3	1%	-1%
Canada	8	16	3%	-3%
Germany	3	24	4%	+1%
International	9	63	11%	-4%
Mexico	0	5	1%	+1%
United Kingdom	4	107	19%	+16%
United States	97	354	62%	-15%

Question 4: Does your organization have a formal OPSEC program?				
Response	**2009 Number**	**2010 Number**	**Percent**	**Change**
Yes	76	205	36%	-24%%
No	35	112	20%	-8%

Don't Know	3	33	6%	+4%
Have an Informal Policy	6	148	26%	+21%
Policy Under Development	6	74	13%	+8%

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

Response	2009 Number	2010 Number	Percent	Change
Yes	68	183	50%	-4%
No	54	146	40%	-3%
Don't Know	4	41	10%	+7%

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

Response	2009 Number	2010 Number	Percent	Change
0	62	187	51%	+2%
1-2	35	70	19%	-9%
2-5	7	41	11%	+5%
5+	22	73	20%	+3%

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

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

Response	2009 Number	2010 Number	Percent	Change
None or NA	74	92	21%	-31%
Information Technology	14	64	15%	-4%
Information Security	20	51	12%	-4%
Physical Security	20	76	18%	+2%
Emergency Management	1	0	0%	-1%
Information Assurance	2	32	7%	+6%
Management	13	79	18%	+8%
Other Information Operations	5	41	10%	+6%
External (Law Enforcement, Security Company)	2	0	0%	-1%

Note that responses exceed 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	2009 Number	2010 Number	Percent	Change
Don't Know	33	111	30%	+9%
None	41	131	35%	+25%
$1-1,000	27	51	14%	+2%
$1,001-5,000	8	62	17%	+1%
$5,001-10,000	2	2	<1%	0%
$10,000+	15	15	<1%	-7%

Question 9: How would you rate your organization's understanding and implementation of OPSEC?				
Response	**2009 Number**	**2010 Number**	**Percent**	**Change**
NA	2	0	0%	-1%
Don't Know	5	28	8%	+4%
Failing	12	38	10%	0%
Poor	15	51	14%	+2%
Needs Improvement	31	79	21%	-2%
Average	24	74	20%	+1%
Good	0	51	14%	+14%
Very Good	20	19	5%	-11%
Excellent	17	32	9%	-4%

Not including those that rated themselves "NA" or "Don't Know", 45% of respondents rated themselves as "Needs Improvement" or below. 47% 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	**2009 Number**	**2010 Number**	**Percent**	**Change**
Yes	42	82	22%	-9%
No	74	177	48%	-11%
Don't Know	10	113	30%	+22%

Question 11: Do you feel that your customers, clients or stakeholders are confident in your ability to protect their information or data?				
Response	**2009 Number**	**2010 Number**	**Percent**	**Change**
Yes	81	174	47%	-17%
No	28	80	22%	0%
Don't Know	17	118	32%	+22%

Question 12: Do you feel that your customers, clients or stakeholders are confident in your ability to protect *your own* information or data?				
Response	**2009 Number**	**2010 Number**	**Percent**	**Change**
Yes	92	177	48%	-25%
No	21	85	23%	+6%
Don't Know	13	109	30%	+20%

Question 13: Has your organization completed a formal OPSEC survey within the last year?				
Response	**2009 Number**	**2010 Number**	**Percent**	**Change**
Yes	36	143	38%	+9%
No	74	122	33%	-26%
Don't Know	16	107	29%	+16%

OSPA 2010 State Of OPSEC Survey

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	**2009 Number**	**2010 Number**	**Percent**	**Change**
Yes	95	321	86%	+15%
No	24	39	10%	-9%
Don't Know	7	12	3%	-2%

Question 15: Does your organization have an OPSEC plan?				
Response	**2009 Number**	**2010 Number**	**Percent**	**Change**
Yes	68	153	41%	-13%
No	51	126	34%	-6%
Don't Know	7	93	25%	+20%

Question 16: Which of the following (from a list) would you consider to be an actual or imminent threat to your organization?				
Response	**2009 Number**	**2010 Number**	**Percent**	**Change**
Internal Threats	51	251	68%	+28%
Foreign Intelligence Service (FIS)	38	86	23%	-7%
Hackers	57	103	28%	-17%
Corporate Espionage	26	51	14%	-6%
International Terrorism	20	215	58%	+42%
Domestic Terrorism	24	122	33%	+14%
Criminals	3	95	26%	+24%
Don't Know	1	4	1%	0%

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	**2009 Number**	**2010 Number**	**Percent**	**Change**
Financial Loss	37	109	29%	0%
Loss Of Personnel Safety	53	201	54%	+14%
Loss of Customer, Client or Stakeholder (CCS) Confidence	59	91	24%	-23%
Loss of Sensitive Records	10	101	27%	+19%
Loss of sensitive US Technology	1	32	9%	+8%
Compromise of Critical Information	1	212	57%	+56%
Ability to Accomplish Mission	17	119	32%	+19%

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

OSPA 2010 State Of OPSEC Survey

Question 18: Has your organization implemented any countermeasures in order to address OPSEC-related risks or concerns?				
Response	**2009 Number**	**2010 Number**	**Percent**	**Change**
Don't Know	11	15	4%	-5%
Have Not attempted to identify OPSEC risks or concerns	7	44	12%	+6%
Have Not identified OPSEC risks or concerns	6	9	3%	-2%
Yes	84	210	56%	-11%
No	18	94	25%	+15%

Question 19: Do you feel that your organization would benefit from free or subsidized OPSEC instruction?				
Response	**2009 Number**	**2010 Number**	**Percent**	**Change**
Don't Know	20	31	8%	-8%
Already Have	30	136	37%	+13%
Yes	69	173	47%	-8%
No	7	31	9%	+3%

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	**2009 Number**	**2010 Number**	**Percent**	**Change**
Don't Know	22	31	8%	-9%
Already Have	25	136	37%	+17%
Yes	67	174	47%	-8%
No	12	31	9%	-1%

21. Has your organization modified its OPSEC program or posture in response to the recent "WikiLeaks" incident?				
Response	**2009 Number**	**2010 Number**	**Percent**	**Change**
Yes		213	57%	
No		86	23%	
Don't know		73	20%	

22. Does your organization make use of any of the named OPSEC tools?				
Response	**2009 Number**	**2010 Number**	**Percent**	**Change**
IOSS Practitioners Toolbox 2.1		205	55%	
IOSS WWII retro OPSEC computer backgrounds and screensavers		176	47%	
IOSS CBT Resources		199	53%	
OSPA CIL Generator		212	56%	
OSPA OPSEC Correlation Analysis Tool (OCAT)		85	23%	
OSPA OSINT Tool		74	20%	
Other		299	80%	

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

23. Does your organization create its own OPSEC awareness material, to include posters, labels, videos, etc?				
Response	**2009 Number**	**2010 Number**	**Percent**	**Change**
Yes		117	31%	
No		158	42%	
Don't know		97	26%	

24. Does your organization have a Threat Statement or other formal threat document?				
Response	**2009 Number**	**2010 Number**	**Percent**	**Change**
Yes		102	27%	
No		143	38%	
Don't know		127	34%	

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 State of OPSEC Survey, it is apparent that a compelling need exists for additional resources as well as increased awareness. It's also encouraging to note that a greater percentage of respondents are taking advantage of existing resources. It is also encouraging to note that respondents are modifying their posture in response to threats or incidents.

It is a rapidly expanding field, which is a requirement for the rapidly changing threats to personnel and organizations. Additionally, fields which traditionally failed to adopt OPSEC measures or concepts are beginning to do so on some level. Annually, additional State of OPSEC 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.