NOTE WHERE ANSWERS ARE WRITE-IN, THE DETAIL IS AT THE END OF THIS DOC.

Security SME Metrics

SurveyMonkey

1. Please use the following drop-down list to select your current field of employment:

	Response Percent	Response Count
Financial/Banking	**33.0%**	**36**
Insurance	3.7%	4
Public Accounting	1.8%	2
Transportation	0.0%	0
Aerospace	0.0%	0
Retail/Wholesale/Distribution	1.8%	2
Government/Military – National/State/Local	6.4%	7
Technology Service/Consulting	18.3%	20
Manufacturing/Engineering	2.8%	3
Telecommunications/Communications	5.5%	6
Mining/Construction/Petroleum/Agriculture	0.9%	1
Utilities	0.0%	0
Legal/Law/Real Estate	0.0%	0
Health Care/Medical	1.8%	2
Pharmaceutical	0.0%	0
Advertising/Marketing/Media	0.9%	1
Education/Student	14.7%	16
Other	8.3%	9
	If you chose OTHER, please specify:	8
	answered question	**109**

skipped question	**0**

2. Please use the following drop-down list to select your current professional activity:

	Response Percent	Response Count
CEO, President, Owner, General/Executive Manager	5.5%	6
CAE, General Auditor, Partner, Audit Head/VP/EVP	0.0%	0
CISO/CSO, Security Executive/VP/EVP	**23.9%**	**26**
CIO/CTO, Security Executive/VP/EVP	0.0%	0
CIO/CTO, Info Systems/Technology Executive/VP/EVP	5.5%	6
CFO/Controller, Treasurer, Finance Executive/VP/EVP	0.9%	1
Chief Compliance/Risk/Privacy officer, VP/EVP	0.9%	1
IT Audit Director/Manager/Consultant	3.7%	4
Security Director/Manager/Consultant	18.3%	20
IT Director/Manager/Consultant	2.8%	3
Compliance/Risk/Privacy Director/Manager/Consultant	2.8%	3
IT Senior Auditor (External/Internal)	0.0%	0
IT Auditor (External/Internal Staff)	0.0%	0
Non-IT Auditor (External/Internal)	0.0%	0
Security Staff	2.8%	3
IT Staff	5.5%	6

IT/IS Compliance/Risk/Control Staff	3.7%	4
Professor/Teacher	6.4%	7
Student	4.6%	5
Security Architect	4.6%	5
Other	8.3%	9
	If you chose OTHER, please specify:	10

answered question	**109**
skipped question	**0**

3. and 4. If you selected 'Security Architect' in response to question 2, please answer questions 3 and 4. Otherwise, please select the 'NEXT' button below. 3. On roughly how many projects did you have security architecture responsibilities?

	Response Count
	12

answered question	**12**
skipped question	**97**

4. What was the budget of the largest one?

	Response Count
	9

answered question	**9**
skipped question	**100**

5. Please use the following drop-down list to describe the size of your organization:

	Response Percent	Response Count
Not applicable	6.1%	6
Fewer than 50 employees	17.3%	17
50-499 employees	11.2%	11
500-4,999 employees	16.3%	16
5000-19,999 employees	13.3%	13
20,000-74,999 employees	13.3%	13
Over 75,000 employees	**22.4%**	**22**
	answered question	**98**
	skipped question	**11**

6. Please use the following drop-down list to describe the size of the IT audit staff:

	Response Percent	Response Count
Not applicable	22.4%	22
0 individuals	9.2%	9
1-10 individuals	26.5%	26
11-25 individuals	7.1%	7
Over 25 individuals	**34.7%**	**34**
	answered question	**98**
	skipped question	**11**

7. Please use the following drop-down list to describe the size of the security staff:

	Response Percent	Response Count
Not applicable	18.4%	18
0 individuals	3.1%	3
1-5 individuals	19.4%	19
6-10 individuals	10.2%	10
11-25 individuals	8.2%	8
Over 25 individuals	**40.8%**	**40**
	answered question	**98**
	skipped question	**11**

8. Please use the following drop-down list to describe the area of your professional interest:

	Response Percent	Response Count
Assurance/Audit	2.0%	2
Governance of Enterprise IT	4.1%	4
Information Security	**66.3%**	**65**
IT Compliance	1.0%	1
IT Control	1.0%	1
IT Value Delivery	5.1%	5
Risk Management	20.4%	20
	answered question	**98**
	skipped question	**11**

9. Please check all Professional Certifications you currently hold:

	Response Percent	Response Count
CISSP from ISC2	**61.7%**	**37**
CISM from ISACA	43.3%	26
CISA from ISACA	21.7%	13
GSEC from SANS	5.0%	3
GIAC from SANS	3.3%	2
Other, please specify certification and organization in the box below	40.0%	24
	answered question	**60**
	skipped question	**49**

10. Which of these or other professional security associations are you a member or officer?

	Member	Officer	Response Count
ASIS	**100.0% (3)**	0.0% (0)	3
CSI	**100.0% (5)**	0.0% (0)	5
ISACA	**91.4% (32)**	8.6% (3)	35
ICS2	**96.4% (27)**	3.6% (1)	28
ISF	**100.0% (7)**	0.0% (0)	7
ISSA	**86.4% (19)**	13.6% (3)	22
SANS	**75.0% (3)**	25.0% (1)	4
	Other, please specify membership and officer status		13

answered question	**54**
skipped question	**55**

11. Education (select all that apply):

	Response Percent	Response Count
High School	**51.1%**	**46**
Bachelor’s Degree in Science or Engineering	43.3%	39
Bachelor’s Degree Social Science or Humanities	12.2%	11
Other Bachelor’s Degree	13.3%	12
Masters Degree in Science or Engineering	33.3%	30
Masters Degree Social Science or Humanities	6.7%	6
Masters Degree not in Science, Engineering, Social Science or Humanities	20.0%	18
PhD in technical field	11.1%	10
PhD non-technical field	2.2%	2
	answered question	**90**
	skipped question	**19**

12. Enter the number of years in security (if any):

	Response Count
	86
answered question	**86**
skipped question	**23**

13. Number of years in a technology-related field (if any):

	Response Count
	87
answered question	87
skipped question	22

14. Enter the total number of years of work experience:

	Response Count
	91
answered question	91
skipped question	18

15. If you have current responsibilities with respect to security architecture, how would you describe them (please check all that apply and add any significant others):

	Response Percent	Response Count
Consulting	**65.8%**	**50**
Requirements	55.3%	42
Design	42.1%	32
Manufacture	1.3%	1
Implementation	28.9%	22
Integration	21.1%	16
Test	22.4%	17
Operate	14.5%	11
Evaluate	44.7%	34
Recommend	55.3%	42
Approve	38.2%	29
Purchase	22.4%	17
Sell	9.2%	7
Management Oversight	44.7%	34
Audit	17.1%	13
Sign-off on requirements	31.6%	24
Sign-off on design	26.3%	20
Sign-off on implementation strategy	26.3%	20
Sign-off on production operation	15.8%	12
Other (please specify in the box below)	11.8%	9
	answered question	**76**

skipped question	33

16. Please provide your definitions of the word “measurement,” the word “metrics,” and the phrase “security metrics” in general, without reference to security, by completing the following sentences: The word “measurement” means:

	Response Count
	71
answered question	71
skipped question	38

17. The word “metrics” means:

	Response Count
	71
answered question	71
skipped question	38

18. The phrase “security metrics” means:

	Response Count
	71
answered question	71
skipped question	38

19. In your opinion, are the best security metrics (please choose from the following drop-down list):

	Response Percent	Response Count
Nominal	5.6%	4
Ordinal	11.3%	8
Interval	2.8%	2
Ratio	16.9%	12
These terms are unfamiliar to me	25.4%	18
Other	**38.0%**	**27**
If you chose OTHER, please describe and explain why in the box below.		29
answered question		**71**
skipped question		**38**

20. Please explain the reasoning behind your answer to Question 19:

	Response Count
	71
answered question	**71**
skipped question	**38**

21. Please rate the following list of activities on a scale from 0 to 5, where the number indicates the contribution of the activity to an organization's ability to maintain its security. Each activity must be assigned its own number, but the number can be zero:

	0	1	2	3	4	5	Rating Average	Response Count
Articulate, maintain, and monitor system mission	0.0% (0)	8.1% (5)	11.3% (7)	22.6% (14)	16.1% (10)	**41.9% (26)**	3.73	62
Certification, accreditation, and security assessments	3.2% (2)	9.7% (6)	17.7% (11)	**30.6% (19)**	19.4% (12)	19.4% (12)	3.11	62
Use security standards as system requirements	4.8% (3)	4.8% (3)	14.5% (9)	**29.0% (18)**	**29.0% (18)**	17.7% (11)	3.26	62
System-level risk assessment	1.6% (1)	0.0% (0)	8.1% (5)	21.0% (13)	**43.5% (27)**	25.8% (16)	3.82	62
Infrastructure risk assessment	1.6% (1)	4.8% (3)	8.1% (5)	19.4% (12)	**43.5% (27)**	22.6% (14)	3.66	62
Identify security features that correspond to system functions	1.6% (1)	4.8% (3)	8.1% (5)	**32.3% (20)**	30.6% (19)	22.6% (14)	3.53	62
Due diligence in system and services acquisition	1.6% (1)	1.6% (1)	16.1% (10)	**29.0% (18)**	27.4% (17)	24.2% (15)	3.52	62
Security awareness	1.6% (1)	1.6% (1)	11.3% (7)	19.4% (12)	25.8% (16)	**40.3% (25)**	3.87	62
System and software change control	4.8% (3)	0.0% (0)	11.3% (7)	27.4% (17)	**29.0% (18)**	27.4% (17)	3.58	62
System recovery planning	4.8% (3)	0.0% (0)	9.7% (6)	21.0% (13)	**33.9% (21)**	30.6% (19)	3.71	62
Incident detection and response	3.2% (2)	3.2% (2)	4.8% (3)	14.5% (9)	29.0% (18)	**45.2% (28)**	3.98	62
Oversight of vendor maintenance	0.0% (0)	8.1% (5)	12.9% (8)	30.6% (19)	**35.5% (22)**	12.9% (8)	3.32	62
Control over removable media	4.8% (3)	9.7% (6)	12.9% (8)	19.4% (12)	**30.6% (19)**	22.6% (14)	3.29	62
Physical and environmental protection	3.2% (2)	8.1% (5)	9.7% (6)	24.2% (15)	21.0% (13)	**33.9% (21)**	3.53	62

Personnel screening and supervision	3.2% (2)	6.5% (4)	12.9% (8)	17.7% (11)	27.4% (17)	**32.3% (20)**	3.56	62
Software integrity preservation	3.2% (2)	0.0% (0)	16.1% (10)	24.2% (15)	**30.6% (19)**	25.8% (16)	3.56	62
Identify security features required to maintain integrity over system interfaces	1.6% (1)	8.1% (5)	8.1% (5)	17.7% (11)	**35.5% (22)**	29.0% (18)	3.65	62
Segregate users into groups or roles for access control	1.6% (1)	8.1% (5)	6.5% (4)	24.2% (15)	**33.9% (21)**	25.8% (16)	3.58	62
Maintain audit trails on use of system functions	1.6% (1)	3.3% (2)	16.4% (10)	18.0% (11)	**36.1% (22)**	24.6% (15)	3.57	61
User identification and authentication	3.2% (2)	0.0% (0)	3.2% (2)	4.8% (3)	29.0% (18)	**59.7% (37)**	4.35	62
Maintain values of standard security variables in system technical configuration	6.5% (4)	1.6% (1)	19.4% (12)	22.6% (14)	**38.7% (24)**	11.3% (7)	3.19	62
Quantify the value of assets at risk in system operation	1.6% (1)	4.8% (3)	17.7% (11)	21.0% (13)	**35.5% (22)**	19.4% (12)	3.42	62
Quantify probability of system security threats	4.8% (3)	8.1% (5)	19.4% (12)	**30.6% (19)**	17.7% (11)	19.4% (12)	3.06	62
Quantify potential organizational damage from system security threats	1.6% (1)	1.6% (1)	19.4% (12)	**30.6% (19)**	21.0% (13)	25.8% (16)	3.45	62
Evaluate the extent to which systems are protected from known threats	0.0% (0)	3.2% (2)	11.3% (7)	16.1% (10)	33.9% (21)	**35.5% (22)**	3.87	62
Other, if applicable	38.9% (7)	0.0% (0)	5.6% (1)	0.0% (0)	5.6% (1)	**50.0% (9)**	2.83	18
						If you chose OTHER, please specify:		13

answered question	**62**
skipped question	**47**

22. Please answer this question from the perspective of the highest level of management in your organization (e.g. CEO or President), as you perceive them to think about security. That is, how would your management rate, on a scale of 1 to 5, where 5 is the highest indicator that an organization which performs these activities is secure and is the lowest or least significant indicator of organizational security: (If not applicable please skip to the next question)

	1	2	3	4	5	Rating Average	Response Count
Articulate, maintain, and monitor system mission	2.2% (1)	13.0% (6)	21.7% (10)	28.3% (13)	**34.8% (16)**	3.80	46
Certification, accreditation, and security assessments	8.5% (4)	23.4% (11)	25.5% (12)	**31.9% (15)**	10.6% (5)	3.13	47
Use security standards as system requirements	8.5% (4)	19.1% (9)	25.5% (12)	**34.0% (16)**	12.8% (6)	3.23	47
System-level risk assessment	2.1% (1)	25.5% (12)	29.8% (14)	**36.2% (17)**	6.4% (3)	3.19	47
Identify security features that correspond to system functions	6.5% (3)	28.3% (13)	**45.7% (21)**	15.2% (7)	4.3% (2)	2.83	46
Due diligence in system and services acquisition	2.1% (1)	14.9% (7)	27.7% (13)	**36.2% (17)**	19.1% (9)	3.55	47
Security awareness	4.3% (2)	6.4% (3)	**31.9% (15)**	29.8% (14)	27.7% (13)	3.70	47
System and software change control	0.0% (0)	25.5% (12)	**29.8% (14)**	23.4% (11)	21.3% (10)	3.40	47
System recovery planning	2.1% (1)	17.0% (8)	21.3% (10)	**40.4% (19)**	19.1% (9)	3.57	47
Incident detection and response	0.0% (0)	19.1% (9)	19.1% (9)	**36.2% (17)**	25.5% (12)	3.68	47
Oversight of vendor maintenance	4.3% (2)	21.3% (10)	**34.0% (16)**	27.7% (13)	12.8% (6)	3.23	47
Control over removable media	17.0% (8)	**29.8% (14)**	14.9% (7)	**29.8% (14)**	8.5% (4)	2.83	47
Physical and environmental protection	0.0% (0)	23.4% (11)	17.0% (8)	**38.3% (18)**	21.3% (10)	3.57	47

Personnel screening and supervision	0.0% (0)	14.9% (7)	19.1% (9)	**42.6% (20)**	23.4% (11)	3.74	47
Software integrity preservation	8.5% (4)	27.7% (13)	**29.8% (14)**	25.5% (12)	8.5% (4)	2.98	47
Identify security features required to maintain integrity over system interfaces	10.6% (5)	**38.3% (18)**	23.4% (11)	23.4% (11)	4.3% (2)	2.72	47
Segregate users into groups or roles for access control	10.9% (5)	15.2% (7)	28.3% (13)	**30.4% (14)**	15.2% (7)	3.24	46
Maintain audit trails on use of system functions	4.3% (2)	27.7% (13)	21.3% (10)	**34.0% (16)**	12.8% (6)	3.23	47
User identification and authentication	0.0% (0)	8.5% (4)	27.7% (13)	**34.0% (16)**	29.8% (14)	3.85	47
Maintain standard security variables in system technical configuration	10.6% (5)	**34.0% (16)**	31.9% (15)	17.0% (8)	6.4% (3)	2.74	47
Quantify the value of assets at risk in system operation	4.3% (2)	12.8% (6)	**38.3% (18)**	17.0% (8)	27.7% (13)	3.51	47
Quantify probability of system security threats	4.3% (2)	21.3% (10)	**34.0% (16)**	23.4% (11)	17.0% (8)	3.28	47
Quantify potential organizational damage from system security threats	2.1% (1)	17.0% (8)	27.7% (13)	**29.8% (14)**	23.4% (11)	3.55	47
Evaluate the extent to which systems are protected from known threats	2.1% (1)	14.9% (7)	27.7% (13)	**31.9% (15)**	23.4% (11)	3.60	47
Other, if applicable	**30.8% (4)**	0.0% (0)	15.4% (2)	23.1% (3)	**30.8% (4)**	3.23	13

If you chose OTHER, please specify: 6

answered question	**47**
skipped question	**62**

23. Please select the sentence fragments that complete the stem sentence and make it true (select all that apply): System security verification requires

	Response Percent	Response Count
... finite, cost-effective verification techniques	52.5%	32
... clear articulation of system mission and/or purpose	67.2%	41
... quantification of system assets	42.6%	26
... quantification of system threat environment	47.5%	29
... quantification of impact of system vulnerability exploit	52.5%	32
... technical analysis of security features	70.5%	43
... specification of security functional requirements	**72.1%**	**44**
Other (please specify in the box below)	8.2%	5
	answered question	**61**
	skipped question	**48**

24. Please rate the following system abilities on a scale of 1 to 5, where 5 is the highest indicator that a system which exhibits these attributes is secure and 1 is the lowest or least significant indicator that the system exhibits security.

	1	2	3	4	5	Rating Average	Response Count
pass regulatory audit	26.2% (16)	23.0% (14)	**31.1% (19)**	8.2% (5)	11.5% (7)	2.56	61
pass security audit	6.6% (4)	11.5% (7)	32.8% (20)	**34.4% (21)**	14.8% (9)	3.39	61
pass internal security review	4.9% (3)	8.2% (5)	**36.1% (22)**	26.2% (16)	24.6% (15)	3.57	61
withstand targeted penetration attacks by skilled attack teams	1.6% (1)	6.6% (4)	9.8% (6)	37.7% (23)	**44.3% (27)**	4.16	61
deliver on service level agreements despite damage to functional components	8.2% (5)	21.3% (13)	24.6% (15)	**36.1% (22)**	9.8% (6)	3.18	61
trace software provenance	9.8% (6)	21.3% (13)	**49.2% (30)**	11.5% (7)	8.2% (5)	2.87	61
maintain integrity of interfaces through system development lifecycle	9.8% (6)	14.8% (9)	**31.1% (19)**	29.5% (18)	14.8% (9)	3.25	61
fail in denial of service mode	21.3% (13)	**27.9% (17)**	23.0% (14)	13.1% (8)	14.8% (9)	2.72	61
Other, if applicable	25.0% (2)	0.0% (0)	12.5% (1)	0.0% (0)	**62.5% (5)**	3.75	8
					If you chose OTHER, please specify:		7

answered question	**61**
skipped question	**48**

25. Please rate the following types of measurement on a scale of 1 to 5, where 5 is the highest indicator that a measurement of the given type is useful in measuring system security and 1 is the lowest or least significant indicator that measurement of the given type is useful in measuring system security.

	1	2	3	4	5	Rating Average	Response Count
Number of resources consumed in system security-related tasks	**30.4% (17)**	23.2% (13)	28.6% (16)	14.3% (8)	3.6% (2)	2.38	56
Percentage of systems or components that have passed security configuration tests	3.6% (2)	19.6% (11)	21.4% (12)	**42.9% (24)**	12.5% (7)	3.41	56
Progress in a management plan to secure system	3.6% (2)	12.5% (7)	**35.7% (20)**	30.4% (17)	17.9% (10)	3.46	56
Logs that verify that process designed to secure system is followed	3.6% (2)	5.4% (3)	28.6% (16)	**42.9% (24)**	19.6% (11)	3.70	56
Successful execution of business continuity procedures	1.8% (1)	7.1% (4)	32.1% (18)	**42.9% (24)**	16.1% (9)	3.64	56
System performance measures in changing threat environment	1.8% (1)	21.4% (12)	23.2% (13)	**33.9% (19)**	19.6% (11)	3.48	56
Other, if applicable	22.2% (2)	0.0% (0)	11.1% (1)	11.1% (1)	**55.6% (5)**	3.78	9
					If you chose OTHER, please specify:		6

answered question	**56**
skipped question	**53**

26. Please rate following system characteristics on a scale of 1 to 5, where 5 is the highest indicator that system security requirements should be easy to identify and gather, and 1 is the lowest or least significant indicator that system security requirements should be easy to identify and gather.

	1	2	3	4	5	Rating Average	Response Count
System is comprised of independently operating functional components	10.7% (6)	19.6% (11)	23.2% (13)	**33.9% (19)**	12.5% (7)	3.18	56
System follows a commonly used architecture pattern	1.8% (1)	12.5% (7)	25.0% (14)	**46.4% (26)**	14.3% (8)	3.59	56
System uses off-the-shelf security software	14.3% (8)	21.4% (12)	**35.7% (20)**	12.5% (7)	16.1% (9)	2.95	56
System interfaces accept only valid input	1.8% (1)	5.4% (3)	16.1% (9)	33.9% (19)	**42.9% (24)**	4.11	56
System output conforms to well-defined specifications	5.4% (3)	5.4% (3)	21.4% (12)	**42.9% (24)**	25.0% (14)	3.77	56
Other, if applicable	33.3% (2)	0.0% (0)	16.7% (1)	0.0% (0)	**50.0% (3)**	3.33	6
					If you chose OTHER, please specify:		4

answered question	**56**
skipped question	**53**

27. Assume you are using a system to maintain critical industrial control operations. Please rate following security features on a scale of 1 to 5, where 5 is the highest indicator that the critical industrial control operation system requires implementation of this feature to be considered secure, and 1 is the lowest or least significant indicator that including of this item as a system security feature is required to be considered secure

	1	2	3	4	5	Rating Average	Response Count
Role-based identification	5.5% (3)	3.6% (2)	23.6% (13)	29.1% (16)	**38.2% (21)**	3.91	55
Access control	0.0% (0)	0.0% (0)	9.1% (5)	18.2% (10)	**72.7% (40)**	4.64	55
Non-repudiation	5.5% (3)	12.7% (7)	21.8% (12)	**30.9% (17)**	29.1% (16)	3.65	55
Data confidentiality	10.9% (6)	7.3% (4)	12.7% (7)	27.3% (15)	**41.8% (23)**	3.82	55
Data integrity	0.0% (0)	0.0% (0)	3.6% (2)	27.3% (15)	**69.1% (38)**	4.65	55
Communication security	1.8% (1)	1.8% (1)	10.9% (6)	25.5% (14)	**60.0% (33)**	4.40	55
Software integrity	0.0% (0)	1.8% (1)	7.3% (4)	21.8% (12)	**69.1% (38)**	4.58	55
Interface integrity	0.0% (0)	1.8% (1)	14.5% (8)	23.6% (13)	**60.0% (33)**	4.42	55
Compartmentalization	1.8% (1)	7.3% (4)	29.1% (16)	**30.9% (17)**	**30.9% (17)**	3.82	55
Resistance to DDOS	1.8% (1)	9.1% (5)	20.0% (11)	**36.4% (20)**	32.7% (18)	3.89	55
Resistance to Botnet activities	3.6% (2)	7.3% (4)	18.2% (10)	30.9% (17)	**40.0% (22)**	3.96	55
					answered question		**55**
					skipped question		**54**

28. Assume you are using a system to maintain a corporate network. Please rate following security features on a scale of 1 to 5, where 5 is the highest indicator that a corporate network requires implementation of this feature to be considered secure, and 1 is the lowest or least significant indicator that this corporate network security feature is required to be considered secure.

	1	2	3	4	5	Rating Average	Response Count
Role-based identification	5.5% (3)	5.5% (3)	16.4% (9)	32.7% (18)	**40.0% (22)**	3.96	55
Access control	0.0% (0)	0.0% (0)	5.5% (3)	23.6% (13)	**70.9% (39)**	4.65	55
Non-repudiation	7.3% (4)	12.7% (7)	18.2% (10)	**36.4% (20)**	25.5% (14)	3.60	55
Data confidentiality	0.0% (0)	1.8% (1)	18.2% (10)	25.5% (14)	**54.5% (30)**	4.33	55
Data integrity	0.0% (0)	0.0% (0)	14.5% (8)	29.1% (16)	**56.4% (31)**	4.42	55
Communication security	0.0% (0)	0.0% (0)	9.1% (5)	32.7% (18)	**58.2% (32)**	4.49	55
Interface integrity	1.8% (1)	3.6% (2)	25.5% (14)	27.3% (15)	**41.8% (23)**	4.04	55
Compartmentalization	3.6% (2)	3.6% (2)	**34.5% (19)**	30.9% (17)	27.3% (15)	3.75	55
System availability	0.0% (0)	7.3% (4)	21.8% (12)	34.5% (19)	**36.4% (20)**	4.00	55
Resistance to DDOS	1.8% (1)	3.6% (2)	27.3% (15)	**40.0% (22)**	27.3% (15)	3.87	55
Resistance to Botnet activities	1.8% (1)	3.6% (2)	18.2% (10)	32.7% (18)	**43.6% (24)**	4.13	55
					answered question		**55**
					skipped question		**54**

29. Please rate the following attributes of metrics data on a scale of 1 to 5, where 5 is the highest indicator that metrics data which exhibits these attributes provides a good measure of security and 1 is the lowest or least significant indicator of metrics data that contributes to good security metrics.

	1	2	3	4	5	Rating Average	Response Count
Valid: data supports a hypothesis that system is secure	3.8% (2)	5.7% (3)	22.6% (12)	32.1% (17)	**35.8% (19)**	3.91	53
Accurate: data reflects the content of measurement as it was envisioned	1.9% (1)	1.9% (1)	13.2% (7)	**56.6% (30)**	26.4% (14)	4.04	53
Numeric: data can be precisely quantified	9.4% (5)	13.2% (7)	20.8% (11)	**37.7% (20)**	18.9% (10)	3.43	53
Verifiable: data can be verified to conform to a given syntax	1.9% (1)	7.5% (4)	26.4% (14)	**39.6% (21)**	24.5% (13)	3.77	53
Correct: data is collected according to specifications	3.8% (2)	3.8% (2)	30.2% (16)	26.4% (14)	**35.8% (19)**	3.87	53
Consistent: measure is independent of measurer	1.9% (1)	1.9% (1)	17.0% (9)	30.2% (16)	**49.1% (26)**	4.23	53
Time-based: there is a fixed reference point of data collection	1.9% (1)	13.2% (7)	24.5% (13)	**30.2% (16)**	**30.2% (16)**	3.74	53
Replicable: measurement repeated in same manner in same environment yields same result	1.9% (1)	3.8% (2)	24.5% (13)	24.5% (13)	**45.3% (24)**	4.08	53
Unit-based: data may be expressed in terms of a unit	7.5% (4)	17.0% (9)	22.6% (12)	**26.4% (14)**	**26.4% (14)**	3.47	53
Informative: data provides information without reference to a specific situation or incident	11.3% (6)	3.8% (2)	22.6% (12)	**35.8% (19)**	26.4% (14)	3.62	53
					answered question		**53**
					skipped question		**56**

30. Please rate the following attributes of metrics on a scale of 1 to 5, where 5 is the highest indicator that metrics which exhibit these attributes provide a valid measure of security and 1 is the lowest or least significant indicator of metrics that provide a valid measure of security.

	1	2	3	4	5	Rating Average	Response Count
easy to connect to concept of security	1.9% (1)	3.8% (2)	26.4% (14)	30.2% (16)	**37.7% (20)**	3.98	53
transparent data gathering process	1.9% (1)	7.5% (4)	32.1% (17)	**39.6% (21)**	18.9% (10)	3.66	53
supports security decision-making	1.9% (1)	1.9% (1)	11.3% (6)	28.3% (15)	**56.6% (30)**	4.36	53
mathematical modeling of security management processes	11.3% (6)	26.4% (14)	**43.4% (23)**	13.2% (7)	5.7% (3)	2.75	53
weighting network forensics evidence to increase probabilities of conviction	22.6% (12)	24.5% (13)	**32.1% (17)**	17.0% (9)	3.8% (2)	2.55	53
quantifies threat surface	9.4% (5)	5.7% (3)	**43.4% (23)**	26.4% (14)	15.1% (8)	3.32	53
usies game theory to determine security investment strategies	32.1% (17)	22.6% (12)	**34.0% (18)**	11.3% (6)	0.0% (0)	2.25	53
complex mathematical models for assessing software security	**37.7% (20)**	24.5% (13)	28.3% (15)	7.5% (4)	1.9% (1)	2.11	53
					answered question		**53**
					skipped question		**56**

31. The following standards have been used as a basis for security metrics. Please rate the extent to which you are familiar with each standard, on a scale of 1 to 5, where 5 indicates that you are very experienced with the standard and 1 indicates that you have never heard of the standard.

	1	2	3	4	5	Rating Average	Response Count
Common Criteria for Information Technology Security Evaluation	20.8% (11)	15.1% (8)	**34.0% (18)**	18.9% (10)	11.3% (6)	2.85	53
ISO 27001, 27002 on Security Management (heritage BS7799 and ISO17799)	13.2% (7)	7.5% (4)	24.5% (13)	22.6% (12)	**32.1% (17)**	3.53	53
National Vulnerability Database Common Vulnerability Enumerations (CVE)	11.3% (6)	9.4% (5)	28.3% (15)	**32.1% (17)**	18.9% (10)	3.38	53
National Vulnerability Database Common Weakness Enumerations (CWE, which includes OWASP top 25)	15.1% (8)	13.2% (7)	22.6% (12)	**24.5% (13)**	**24.5% (13)**	3.30	53
Payment Card Industry Data Security Standard (PCI DSS)	11.3% (6)	9.4% (5)	28.3% (15)	20.8% (11)	**30.2% (16)**	3.49	53
Recommended Security Controls for Federal Information Systems (NIST SP800-53)	11.3% (6)	13.2% (7)	**30.2% (16)**	**30.2% (16)**	15.1% (8)	3.25	53
Systems Security Engineering Capability Maturity Model®, Version 3.0, SSE-CMM®, 2003.	30.2% (16)	13.2% (7)	**32.1% (17)**	15.1% (8)	9.4% (5)	2.60	53
Technical Specification for the Security Content Automation Protocol (SCAP - NIST SP800-126)	**32.1% (17)**	20.8% (11)	30.2% (16)	9.4% (5)	7.5% (4)	2.40	53
ISACA Control Objectives for Information Technology (COBIT)	9.4% (5)	17.0% (9)	26.4% (14)	18.9% (10)	**28.3% (15)**	3.40	53
Trusted Computer System Evaluation Criteria (The Orange Book)	18.9% (10)	17.0% (9)	**24.5% (13)**	20.8% (11)	18.9% (10)	3.04	53
Underlying Technical Models for Information Technology Security (NIST SP800-33)	**32.1% (17)**	15.1% (8)	30.2% (16)	17.0% (9)	5.7% (3)	2.49	53

answered question	53
skipped question	56

32. The following standards have been used as a basis for security metrics. For each standard on the list for which you answered 2 or higher in the previous question, please rate its utility in providing good security metrics, on a scale of 1 to 5, where 5 indicates that metrics based on the standard provide a good measure of security and 1 indicates that metrics based on the standard do not provide any measurement of security.

	1	2	3	4	5	Rating Average	Response Count
Common Criteria for Information Technology Security Evaluation	22.6% (12)	24.5% (13)	**41.5% (22)**	9.4% (5)	1.9% (1)	2.43	53
ISO 27001, 27002 on Security Management (heritage BS7799 and ISO17799)	13.2% (7)	11.3% (6)	**34.0% (18)**	28.3% (15)	13.2% (7)	3.17	53
National Vulnerability Database Common Vulnerability Enumerations (CVE)	18.9% (10)	9.4% (5)	**37.7% (20)**	17.0% (9)	17.0% (9)	3.04	53
National Vulnerability Database Common Weakness Enumerations (CWE, which includes OWASP top 25)	18.9% (10)	11.3% (6)	**34.0% (18)**	17.0% (9)	18.9% (10)	3.06	53
Payment Card Industry Data Security Standard (PCI DSS)	11.3% (6)	15.1% (8)	**39.6% (21)**	24.5% (13)	9.4% (5)	3.06	53
Recommended Security Controls for Federal Information Systems (NIST SP800-53)	17.0% (9)	5.7% (3)	**45.3% (24)**	20.8% (11)	11.3% (6)	3.04	53
Systems Security Engineering Capability Maturity Model®, Version 3.0, SSE-CMM®, 2003.	**32.1% (17)**	15.1% (8)	**32.1% (17)**	18.9% (10)	1.9% (1)	2.43	53
Technical Specification for the Security Content Automation Protocol (SCAP - NIST SP800-126)	30.2% (16)	11.3% (6)	**34.0% (18)**	15.1% (8)	9.4% (5)	2.62	53
ISACA Control Objectives for Information Technology (COBIT)	7.5% (4)	13.2% (7)	**45.3% (24)**	18.9% (10)	15.1% (8)	3.21	53

Trusted Computer System Evaluation Criteria (The Orange Book)	26.4% (14)	15.1% (8)	**41.5% (22)**	13.2% (7)	3.8% (2)	2.53	53
Underlying Technical Models for Information Technology Security (NIST SP800-33)	34.0% (18)	9.4% (5)	**43.4% (23)**	13.2% (7)	0.0% (0)	2.36	53
					answered question		**53**
					skipped question		**56**

33. The National Institute of Standards and Technology has published Performance Measurement Guide for Information Security (NIST SP800-55, original 2003 updated 2008). Please select the response from the following drop-down list that most closely describes your experience with that document:

		Response Percent	Response Count
I am not familiar with NIST SP800-55		26.4%	14
I am familiar with NIST SP800-55 but I have not read it		18.9%	10
I have read NIST SP800-55 but I do not recall details		**32.1%**	**17**
I have read NIST SP800-55 and I agree with most of what it recommends		11.3%	6
I have read NIST SP800-55 and I do not agree with most of what it recommends		1.9%	1
I have read NIST SP 800-55, but neither agree nor disagree with what it recommends		5.7%	3
Please provide an explanation of your response, and/or comments on NIST SP800-55.		3.8%	2
	Please provide an explanation of your response, and/or comments on NIST SP800-55.		15
		answered question	**53**

skipped question	**56**

34. We ask you to identify yourself for three reasons: • Someone may one day want to verify the integrity of the data collected by this survey. • We may wish to interview you on the topic of your answers. • You might be interested in receiving a copy of the survey results. If you agree to be identified for the purposes of potential follow up questions, please provide your name, affiliation, and email address:

		Response Percent	Response Count
Name		**100.0%**	**37**
Affiliation		83.8%	31
Address		70.3%	26
City		73.0%	27
State		75.7%	28
Email		**100.0%**	**37**
		answered question	**37**
		skipped question	**72**

35. Please indicate whether you would be willing to be interviewed, or just to verify the results, check all that apply: If you would rather not be identified but would like to get a copy of the survey results, you may do so by registering at securitymetrics.org, as the results will be posted to that mail list.

	Response Percent	Response Count
Verify	48.8%	20
Interview	46.3%	19
Receive results	**90.2%**	**37**
	answered question	**41**
	skipped question	**68**

Page 1, Q1. Please use the following drop-down list to select your current field of employment:

1	Federal Research Contractor	May 18, 2011 1:52 PM
2	eCommerce	May 13, 2011 5:07 PM
3	Computer industry	Mar 23, 2011 12:45 PM
4	not for profit	Mar 22, 2011 4:28 PM
5	Consumer products	Mar 21, 2011 12:18 AM
6	Security Consulting	Mar 19, 2011 5:52 PM
7	Consultant	Feb 14, 2011 10:45 PM
8	Research institute	Feb 14, 2011 1:01 PM

Page 1, Q2. Please use the following drop-down list to select your current professional activity:

1	Director of Research and Development	May 18, 2011 1:52 PM
2	Digital Forensic Analyst	May 16, 2011 10:36 AM
3	Forensic Analyst/Investigator	May 16, 2011 12:15 AM
4	security consultant	May 15, 2011 4:47 PM
5	Title is Director of Security and Compliance. Department of one. Have full range of tactical, operational, and strategic responsibilities; including architecture.	May 14, 2011 4:14 PM
6	Principal investigator, security R&D	May 13, 2011 9:29 AM
7	Applied Research	Mar 31, 2011 11:51 AM
8	Retired security consultant	Mar 20, 2011 9:51 PM
9	Researcher	Feb 14, 2011 1:01 PM
10	Product Manager for online banking security	Feb 14, 2011 9:54 AM

Page 1, Q3. and 4. If you selected 'Security Architect' in response to question 2, please answer questions 3 and 4. Otherwise, please select the 'NEXT' button below.

3. On roughly how many projects did you have security architecture responsibilities?

1	6	May 14, 2011 8:50 PM
2	100	May 14, 2011 4:14 PM
3	3	May 13, 2011 1:40 PM
4	5	Apr 25, 2011 6:01 AM
5	10	Apr 22, 2011 8:39 AM
6	0	Apr 22, 2011 8:39 AM
7	5	Mar 21, 2011 2:01 PM
8	2	Mar 21, 2011 5:34 AM
9	2	Mar 19, 2011 5:03 PM
10	10	Mar 9, 2011 6:45 AM
11	20	Feb 14, 2011 10:45 PM
12	1	Feb 14, 2011 1:15 PM

Page 1, Q4. What was the budget of the largest one?		
1	1000000	May 14, 2011 8:50 PM
2	1000000	May 14, 2011 4:14 PM
3	1000000	May 13, 2011 1:40 PM
4	4000000	Apr 25, 2011 6:01 AM
5	40000000	Apr 22, 2011 8:39 AM
6	1500000	Mar 19, 2011 5:03 PM
7	2000000	Mar 9, 2011 6:45 AM
8	10000000	Feb 14, 2011 10:45 PM
9	100000	Feb 14, 2011 1:15 PM

Page 3, Q9. Please check all Professional Certifications you currently hold:		
1	EnCE, CEH, CHFI	May 16, 2011 10:42 AM
2	EnCE, SCERS, CEH	May 16, 2011 12:20 AM
3	MCSE	May 14, 2011 4:19 PM
4	cgeit, cpa	May 13, 2011 10:03 AM
5	CCM from AFP; AAP from NACHA	May 13, 2011 9:26 AM
6	CGEIT	May 13, 2011 9:23 AM
7	CGEIT	May 3, 2011 8:12 AM
8	CGEIT	Apr 27, 2011 6:50 PM
9	CSSLP	Apr 22, 2011 11:12 PM
10	In process of getting CISSP	Apr 22, 2011 9:14 AM
11	CGEIT	Apr 22, 2011 8:56 AM
12	CISSLP	Apr 22, 2011 8:55 AM
13	CSSLP from ISC2	Apr 14, 2011 7:26 AM
14	Other real qualifications e.g. C.Eng, C.Sci, FBCS	Mar 23, 2011 12:54 PM
15	CCM - NSA; CEE - NSA	Mar 21, 2011 8:37 AM
16	CIPP, CGEIT	Mar 21, 2011 12:20 AM
17	CSSLP - ISC2	Mar 20, 2011 7:45 PM
18	CRISC from ISACA, Professional Engineer - State of CA	Mar 19, 2011 10:10 PM
19	GCIH from SANS	Mar 19, 2011 7:04 PM
20	PMP from PMI	Mar 14, 2011 8:35 PM
21	Security+	Mar 10, 2011 11:49 PM
22	CGEIT	Mar 9, 2011 6:56 AM
23	Technical Diploma	Mar 9, 2011 6:48 AM
24	ITIL Foundation, FAIR Analyst	Feb 14, 2011 8:13 PM

Page 3, Q10. Which of these or other professional security associations are you a member or officer?		
1	IIA member	Jun 6, 2011 9:23 PM
2	ACM and IEEE	May 16, 2011 4:27 PM
3	Member IEEE, ACM	May 13, 2011 12:10 PM
4	LOMA CISO Council, currently chairman	May 13, 2011 10:05 AM
5	OWASP	Apr 25, 2011 6:36 AM
6	none	Apr 23, 2011 6:40 PM
7	FSSCC Financial Services Sector	Apr 1, 2011 8:29 AM
8	Center for Internet Security - Board	Mar 23, 2011 12:54 PM
9	InfraGard, former Board of Directors	Mar 22, 2011 9:25 AM
10	IAPP	Mar 21, 2011 12:20 AM
11	ISA, IEEE, CIGRE, NERC	Mar 19, 2011 10:10 PM
12	Gesellschaft für Informatik	Mar 10, 2011 11:49 PM
13	IEEE	Feb 14, 2011 10:47 PM

Page 3, Q12. Enter the number of years in security (if any):		
1	20	Jun 6, 2011 9:23 PM
2	15	Jun 2, 2011 6:21 AM
3	26	May 20, 2011 10:58 AM
4	10	May 18, 2011 1:54 PM
5	11	May 16, 2011 10:58 PM
6	12	May 16, 2011 4:27 PM
7	4	May 16, 2011 12:38 PM
8	4	May 16, 2011 10:42 AM
9	14	May 16, 2011 7:09 AM
10	2	May 16, 2011 1:10 AM
11	25	May 16, 2011 12:49 AM
12	2	May 16, 2011 12:20 AM
13	5	May 15, 2011 7:33 PM
14	20	May 15, 2011 6:12 PM
15	4	May 15, 2011 4:56 PM
16	30	May 15, 2011 1:17 PM
17	16	May 14, 2011 8:50 PM
18	14	May 14, 2011 4:19 PM
19	40	May 13, 2011 5:17 PM
20	4	May 13, 2011 1:43 PM
21	15	May 13, 2011 12:10 PM
22	8	May 13, 2011 10:05 AM
23	17	May 13, 2011 9:45 AM
24	19	May 13, 2011 9:31 AM
25	5	May 13, 2011 9:26 AM
26	12	May 13, 2011 9:23 AM
27	27	May 3, 2011 8:12 AM
28	20	Apr 27, 2011 6:50 PM
29	11	Apr 25, 2011 10:13 AM

Page 3, Q12. Enter the number of years in security (if any):		
30	20	Apr 25, 2011 8:34 AM
31	7	Apr 25, 2011 6:36 AM
32	10	Apr 25, 2011 6:03 AM
33	11	Apr 23, 2011 6:40 PM
34	25	Apr 23, 2011 4:38 AM
35	44	Apr 22, 2011 11:12 PM
36	30	Apr 22, 2011 9:16 AM
37	15	Apr 22, 2011 9:14 AM
38	21	Apr 22, 2011 8:56 AM
39	9	Apr 22, 2011 8:55 AM
40	19	Apr 22, 2011 8:44 AM
41	16	Apr 22, 2011 8:42 AM
42	20	Apr 22, 2011 8:41 AM
43	20	Apr 19, 2011 4:42 AM
44	6	Apr 18, 2011 5:34 PM
45	29	Apr 14, 2011 7:26 AM
46	25	Apr 7, 2011 1:23 PM
47	16	Apr 5, 2011 8:39 AM
48	7	Apr 3, 2011 10:31 AM
49	20	Apr 1, 2011 8:29 AM
50	14	Mar 27, 2011 4:22 AM
51	20	Mar 23, 2011 12:54 PM
52	27	Mar 22, 2011 4:30 PM
53	14	Mar 22, 2011 9:25 AM
54	12	Mar 21, 2011 2:23 PM
55	20	Mar 21, 2011 2:03 PM
56	30	Mar 21, 2011 11:38 AM
57	13	Mar 21, 2011 10:37 AM
58	43	Mar 21, 2011 8:37 AM

Page 3, Q12. Enter the number of years in security (if any):		
59	7	Mar 21, 2011 6:16 AM
60	13	Mar 21, 2011 6:00 AM
61	15	Mar 21, 2011 5:43 AM
62	13	Mar 21, 2011 12:20 AM
63	40	Mar 20, 2011 9:54 PM
64	16	Mar 20, 2011 7:45 PM
65	25	Mar 20, 2011 7:56 AM
66	11	Mar 19, 2011 10:10 PM
67	10	Mar 19, 2011 7:04 PM
68	11	Mar 19, 2011 6:45 PM
69	40	Mar 19, 2011 5:55 PM
70	10	Mar 19, 2011 5:04 PM
71	5	Mar 14, 2011 8:35 PM
72	13	Mar 11, 2011 11:31 AM
73	11	Mar 10, 2011 11:49 PM
74	10	Mar 10, 2011 7:24 AM
75	18	Mar 9, 2011 3:27 PM
76	10	Mar 9, 2011 6:56 AM
77	10	Mar 9, 2011 6:48 AM
78	19	Feb 22, 2011 3:55 PM
79	3	Feb 17, 2011 1:07 PM
80	19	Feb 15, 2011 9:46 AM
81	35	Feb 14, 2011 10:47 PM
82	20	Feb 14, 2011 8:13 PM
83	5	Feb 14, 2011 5:16 PM
84	4	Feb 14, 2011 1:17 PM
85	3	Feb 14, 2011 9:58 AM
86	10	Feb 14, 2011 8:33 AM

Page 3, Q13. Number of years in a technology-related field (if any):		
1	25	Jun 6, 2011 9:23 PM
2	15	Jun 2, 2011 6:21 AM
3	27	May 20, 2011 10:58 AM
4	12	May 18, 2011 1:54 PM
5	17	May 16, 2011 10:58 PM
6	15	May 16, 2011 4:27 PM
7	20	May 16, 2011 12:38 PM
8	10	May 16, 2011 10:42 AM
9	21	May 16, 2011 7:09 AM
10	2	May 16, 2011 1:10 AM
11	30	May 16, 2011 12:49 AM
12	8	May 16, 2011 12:20 AM
13	25	May 15, 2011 7:33 PM
14	30	May 15, 2011 6:12 PM
15	20	May 15, 2011 5:53 PM
16	10	May 15, 2011 4:56 PM
17	35	May 15, 2011 1:17 PM
18	19	May 14, 2011 8:50 PM
19	19	May 14, 2011 4:19 PM
20	30	May 13, 2011 5:17 PM
21	15	May 13, 2011 1:43 PM
22	40	May 13, 2011 12:10 PM
23	34	May 13, 2011 10:05 AM
24	20	May 13, 2011 10:03 AM
25	27	May 13, 2011 9:45 AM
26	19	May 13, 2011 9:31 AM
27	30	May 13, 2011 9:26 AM
28	20	May 13, 2011 9:23 AM
29	20	May 3, 2011 8:12 AM

Page 3, Q13. Number of years in a technology-related field (if any):		
30	25	Apr 27, 2011 6:50 PM
31	26	Apr 25, 2011 10:13 AM
32	30	Apr 25, 2011 8:34 AM
33	16	Apr 25, 2011 6:36 AM
34	15	Apr 25, 2011 6:03 AM
35	20	Apr 23, 2011 6:40 PM
36	40	Apr 23, 2011 4:38 AM
37	25	Apr 22, 2011 11:12 PM
38	30	Apr 22, 2011 9:16 AM
39	29	Apr 22, 2011 9:14 AM
40	24	Apr 22, 2011 8:56 AM
41	24	Apr 22, 2011 8:55 AM
42	20	Apr 22, 2011 8:44 AM
43	30	Apr 22, 2011 8:42 AM
44	25	Apr 22, 2011 8:41 AM
45	24	Apr 19, 2011 4:42 AM
46	25	Apr 18, 2011 5:34 PM
47	1	Apr 14, 2011 7:26 AM
48	45	Apr 7, 2011 1:23 PM
49	11	Apr 5, 2011 8:39 AM
50	12	Apr 3, 2011 10:31 AM
51	22	Apr 1, 2011 8:29 AM
52	20	Mar 27, 2011 4:22 AM
53	25	Mar 23, 2011 12:54 PM
54	18	Mar 22, 2011 9:25 AM
55	35	Mar 21, 2011 2:23 PM
56	40	Mar 21, 2011 2:03 PM
57	10	Mar 21, 2011 11:38 AM
58	16	Mar 21, 2011 10:37 AM

Page 3, Q13. Number of years in a technology-related field (if any):		
59	45	Mar 21, 2011 8:37 AM
60	13	Mar 21, 2011 6:16 AM
61	21	Mar 21, 2011 6:00 AM
62	23	Mar 21, 2011 5:43 AM
63	56	Mar 20, 2011 9:54 PM
64	37	Mar 20, 2011 7:45 PM
65	37	Mar 20, 2011 7:56 AM
66	40	Mar 20, 2011 6:35 AM
67	39	Mar 19, 2011 10:10 PM
68	12	Mar 19, 2011 7:04 PM
69	11	Mar 19, 2011 6:45 PM
70	50	Mar 19, 2011 5:55 PM
71	20	Mar 19, 2011 5:04 PM
72	15	Mar 14, 2011 8:35 PM
73	13	Mar 11, 2011 11:31 AM
74	16	Mar 10, 2011 11:49 PM
75	20	Mar 10, 2011 7:24 AM
76	35	Mar 9, 2011 3:27 PM
77	25	Mar 9, 2011 6:56 AM
78	20	Mar 9, 2011 6:48 AM
79	20	Feb 22, 2011 3:55 PM
80	10	Feb 17, 2011 1:07 PM
81	14	Feb 15, 2011 9:46 AM
82	35	Feb 14, 2011 10:47 PM
83	20	Feb 14, 2011 8:13 PM
84	15	Feb 14, 2011 5:16 PM
85	5	Feb 14, 2011 1:17 PM
86	7	Feb 14, 2011 9:58 AM
87	17	Feb 14, 2011 8:33 AM

Page 3, Q14. Enter the total number of years of work experience:		
1	21	Jun 6, 2011 9:23 PM
2	30	Jun 2, 2011 6:21 AM
3	27	May 20, 2011 10:58 AM
4	16	May 18, 2011 1:54 PM
5	20	May 16, 2011 10:58 PM
6	15	May 16, 2011 4:27 PM
7	20	May 16, 2011 12:38 PM
8	14	May 16, 2011 10:42 AM
9	21	May 16, 2011 7:09 AM
10	2	May 16, 2011 1:10 AM
11	30	May 16, 2011 12:49 AM
12	10	May 16, 2011 12:20 AM
13	25	May 15, 2011 7:33 PM
14	30	May 15, 2011 6:12 PM
15	48	May 15, 2011 5:53 PM
16	10	May 15, 2011 4:56 PM
17	2	May 15, 2011 4:53 PM
18	35	May 15, 2011 1:17 PM
19	19	May 14, 2011 8:50 PM
20	19	May 14, 2011 4:19 PM
21	50	May 13, 2011 5:17 PM
22	18	May 13, 2011 1:43 PM
23	40	May 13, 2011 12:10 PM
24	34	May 13, 2011 10:05 AM
25	28	May 13, 2011 10:03 AM
26	33	May 13, 2011 9:45 AM
27	28	May 13, 2011 9:31 AM
28	35	May 13, 2011 9:26 AM
29	28	May 13, 2011 9:23 AM

Page 3, Q14. Enter the total number of years of work experience:		
30	32	May 3, 2011 8:12 AM
31	25	Apr 27, 2011 6:50 PM
32	26	Apr 25, 2011 10:13 AM
33	30	Apr 25, 2011 8:34 AM
34	19	Apr 25, 2011 6:36 AM
35	15	Apr 25, 2011 6:03 AM
36	20	Apr 23, 2011 6:40 PM
37	40	Apr 23, 2011 4:38 AM
38	46	Apr 22, 2011 11:12 PM
39	15	Apr 22, 2011 9:24 AM
40	30	Apr 22, 2011 9:16 AM
41	29	Apr 22, 2011 9:14 AM
42	24	Apr 22, 2011 8:56 AM
43	26	Apr 22, 2011 8:55 AM
44	20	Apr 22, 2011 8:44 AM
45	30	Apr 22, 2011 8:42 AM
46	25	Apr 22, 2011 8:41 AM
47	24	Apr 19, 2011 4:42 AM
48	25	Apr 18, 2011 5:34 PM
49	30	Apr 14, 2011 7:26 AM
50	45	Apr 7, 2011 1:23 PM
51	29	Apr 5, 2011 8:39 AM
52	12	Apr 3, 2011 10:31 AM
53	22	Apr 1, 2011 8:29 AM
54	15	Mar 27, 2011 4:22 AM
55	25	Mar 23, 2011 12:54 PM
56	30	Mar 22, 2011 4:30 PM
57	18	Mar 22, 2011 9:25 AM
58	38	Mar 21, 2011 2:23 PM

Page 3, Q14. Enter the total number of years of work experience:		
59	40	Mar 21, 2011 2:03 PM
60	40	Mar 21, 2011 11:38 AM
61	16	Mar 21, 2011 10:37 AM
62	45	Mar 21, 2011 8:37 AM
63	13	Mar 21, 2011 6:16 AM
64	21	Mar 21, 2011 6:00 AM
65	23	Mar 21, 2011 5:43 AM
66	18	Mar 21, 2011 12:20 AM
67	60	Mar 20, 2011 9:54 PM
68	43	Mar 20, 2011 7:45 PM
69	37	Mar 20, 2011 7:56 AM
70	40	Mar 20, 2011 6:35 AM
71	39	Mar 19, 2011 10:10 PM
72	12	Mar 19, 2011 7:04 PM
73	11	Mar 19, 2011 6:45 PM
74	55	Mar 19, 2011 5:55 PM
75	20	Mar 19, 2011 5:04 PM
76	22	Mar 14, 2011 8:35 PM
77	18	Mar 11, 2011 11:31 AM
78	16	Mar 10, 2011 11:49 PM
79	20	Mar 10, 2011 7:24 AM
80	39	Mar 9, 2011 3:27 PM
81	25	Mar 9, 2011 6:56 AM
82	20	Mar 9, 2011 6:48 AM
83	20	Feb 22, 2011 3:55 PM
84	18	Feb 17, 2011 1:07 PM
85	19	Feb 15, 2011 9:46 AM
86	35	Feb 14, 2011 10:47 PM
87	40	Feb 14, 2011 8:13 PM

Page 3, Q14. Enter the total number of years of work experience:		
88	15	Feb 14, 2011 5:16 PM
89	7	Feb 14, 2011 1:17 PM
90	0	Feb 14, 2011 9:58 AM
91	17	Feb 14, 2011 8:33 AM

Page 3, Q15. If you have current responsibilities with respect to security architecture, how would you describe them (please check all that apply and add any significant others):		
1	R&D, Education	May 15, 2011 1:17 PM
2	AS CISO, Security Architecture reports to me...	May 13, 2011 5:17 PM
3	Build	May 13, 2011 1:43 PM
4	Project sponsor and business owner	May 13, 2011 10:05 AM
5	M&A due diligence, Vendor/Customer due diligence	Apr 25, 2011 6:36 AM
6	Help the Infrastructure and Application Development/Operate teams to understand corporate and Industry control requirements and policies, and provide recommendations to ensure compliance with these policies and standards.	Apr 23, 2011 6:40 PM
7	Research	Apr 7, 2011 1:23 PM
8	Represent firm in FS Sector Critical Infrastructure Forums	Apr 1, 2011 8:29 AM
9	Project management.	Feb 17, 2011 1:07 PM

Page 4, Q16. Please provide your definitions of the word “measurement,” the word “metrics,” and the phrase “security metrics” in general, without reference to security, by completing the following sentences:

The word “measurement” means:

1	The data that results from measuring something	Jun 6, 2011 9:57 PM
2	A count of arbitrary units. For example, "Alice is 4'2" tall" is a measurement.	May 21, 2011 10:16 AM
3	numeric assessment	May 20, 2011 10:59 AM
4	A means of determining the size or amount of an item	May 18, 2011 1:57 PM
5	a unit or system of measurement	May 16, 2011 10:59 PM
6	To assess something against an established standard.	May 16, 2011 12:41 PM
7	Single point in time view of a security factor. This is objective and based on raw data.	May 16, 2011 11:03 AM
8	Quantification of state.	May 16, 2011 7:11 AM
9	Quantifying something	May 16, 2011 12:24 AM
10	Both the operation of qualitatively assessing some measurable value, and the result of that assessment.	May 15, 2011 6:17 PM
11	Observing something - counts of events, rates, ...	May 15, 2011 5:57 PM
12	a number or amount obtained from measuring physical, informational, or other processes	May 15, 2011 1:26 PM
13	the process or the result of determining the magnitude of a quantity,	May 14, 2011 8:52 PM
14	The act of measuring.	May 13, 2011 5:43 PM
15	The process of comparing an entity or occurance to a given standard	May 13, 2011 1:49 PM
16	the act of determining or assessing specific characteristics of an object, entity, system or process	May 13, 2011 12:18 PM
17	a quantitative or qualitative attribute to allow comparisons among like things	May 13, 2011 10:17 AM
18	quantication	May 13, 2011 10:05 AM
19	generally a quantifiable assessment of a characteristic	May 13, 2011 10:03 AM
20	Identify control weakness, adherence to regulatory requirements, allow management to monitor individual key performance indicators, demonstrate the continuing value of Information Security and bring transparency to the organization's technology risk posture and the state of information security in the organization.	May 13, 2011 9:54 AM
21	Collecting feedback to determine if policy goals are achieved.	May 13, 2011 9:50 AM
22	Defining a quantity in terms of units.	May 13, 2011 9:34 AM

Page 4, Q16. Please provide your definitions of the word “measurement,” the word “metrics,” and the phrase “security metrics” in general, without reference to security, by completing the following sentences:

The word “measurement” means:

23	relative to a standard unit of measurement	May 3, 2011 8:23 AM
24	Quantification.	Apr 27, 2011 6:51 PM
25	ascertain size	Apr 25, 2011 10:33 AM
26	the ability to instrument a process	Apr 25, 2011 8:37 AM
27	repeatable objective method of determining the quantity of an object or group of objects at a given point in time	Apr 25, 2011 7:18 AM
28	I default to Hubbard's definition, something like an observable quantity that reduces uncertainty	Apr 25, 2011 6:08 AM
29	amount or size obtained by comparing it to some standard or etalon	Apr 23, 2011 7:18 PM
30	applying a scale to an unknown	Apr 23, 2011 4:41 AM
31	A number that reflects activity based on data with which is collected.	Apr 22, 2011 11:18 PM
32	Extent, quantiity or size	Apr 22, 2011 9:34 AM
33	The quantification of some item's characteristics	Apr 22, 2011 9:25 AM
34	application of a discrete numerical representation of an attribute or characteristic of something	Apr 22, 2011 9:21 AM
35	Map from empirical world to formal, relational world.	Apr 22, 2011 9:00 AM
36	to measure	Apr 22, 2011 8:59 AM
37	a value to describe quantity	Apr 19, 2011 4:47 AM
38	The capture or generation of a value associated with a metric.	Apr 18, 2011 5:41 PM
39	repeatable observations	Apr 14, 2011 7:31 AM
40	Observations of a system or phenomonon that are quantified in a manner that is useful to a community of people with concerns related to the system or phenomenon	Apr 7, 2011 1:53 PM
41	The action of measuring something	Apr 5, 2011 9:14 AM
42	The extent, quantity, amount, or degree of something, as determined by standard	Apr 4, 2011 6:24 AM
43	A set of observations that reduce uncertainty where the result is expressed as a quantity	Apr 1, 2011 9:13 AM
44	A means to assist the organization make informed decisions about the design of systems, selection of controls, and efficiency of security operations	Mar 28, 2011 8:17 AM

Page 4, Q16. Please provide your definitions of the word “measurement,” the word “metrics,” and the phrase “security metrics” in general, without reference to security, by completing the following sentences:

The word “measurement” means:

45	A scientific count of some factor in comparison to a baseline.	Mar 27, 2011 4:30 AM
46	Objectively quantify.	Mar 23, 2011 12:55 PM
47	determination of the size or extent of something	Mar 22, 2011 4:37 PM
48	Quantification of one or more traits such that they can be tracked, compared, normalized, baselined, etc.	Mar 22, 2011 9:34 AM
49	the process or the result of a process to determine a specific attribute (quantity or quality) of something using a defined standard of measure	Mar 22, 2011 7:05 AM
50	obtaining a quantitative number or defined unambigious, repeatable qualitative term	Mar 21, 2011 2:07 PM
51	The ability to determine a meaning relationship between reality and imagination.	Mar 21, 2011 8:41 AM
52	An objective quantitative value associated with an observation.	Mar 21, 2011 6:18 AM
53	determining the size of something relative to an agreed and acceptable, repeatable, verifiable unit.	Mar 21, 2011 6:03 AM
54	Quantitative depiction.	Mar 21, 2011 12:22 AM
55	specification	Mar 20, 2011 9:56 PM
56	The ability and tools used to collect information about a process	Mar 20, 2011 7:58 PM
57	Establishing a specific, verifiable quantity of something.	Mar 20, 2011 8:13 AM
58	statistic (number or descriptive term such as high, medium, low) used to represent the relative size of something in relation to an established scale or unit of measure	Mar 20, 2011 7:06 AM
59	making an objective observation.	Mar 19, 2011 10:13 PM
60	The method to determine a quantity or magnitude.	Mar 19, 2011 7:15 PM
61	The act or result of measuring.	Mar 19, 2011 6:01 PM
62	n/a	Mar 19, 2011 5:06 PM
63	to compare something to a known standard	Mar 11, 2011 11:39 AM
64	the process of gathering meaningful data about a process or technology in an effort to determine its state, health, etc.	Mar 10, 2011 7:35 AM
65	a point in time representation of the value, size etc of some concept/item	Mar 9, 2011 3:43 PM
66	*	Mar 9, 2011 2:18 PM

Page 4, Q16. Please provide your definitions of the word “measurement,” the word “metrics,” and the phrase “security metrics” in general, without reference to security, by completing the following sentences:

The word “measurement” means:

67	Being able to numerically determine a value or quantity of something	Mar 9, 2011 6:59 AM
68	Measurement theory incorporates the scale of nominal, ordinal, interval, ratio, and absolute. These scales are used to measure something, with the output being data. In essence, it is something you know.	Feb 15, 2011 9:50 AM
69	the result of an act of measuring	Feb 14, 2011 10:49 PM
70	A measurement is something that "ascertains the dimensions, quantity, or capacity" of something - an object, a process - anything, really. Measurements have at least these three qualities: validity, reproducibility, appropriate level of detail	Feb 14, 2011 8:23 PM
71	Measuring a process using UCL or LCL (or targets, goals and thresholds)	Feb 14, 2011 5:17 PM

Page 4, Q17. The word “metrics” means:

1	A unit of measure	Jun 6, 2011 9:57 PM
2	The comparison of one or more measurements for the purpose of drawing a conclusion. For example, Alice is 4'2" tall compared to an average height of 5'6" tall allows us to conclude that Alice is short.	May 21, 2011 10:16 AM
3	scale for numeric assessment	May 20, 2011 10:59 AM
4	The general comparison of sizes / amounts of multiple related items	May 18, 2011 1:57 PM
5	a method of measuring something	May 16, 2011 10:59 PM
6	Bullet points in an established standard to be used as guidelines for measurement.	May 16, 2011 12:41 PM
7	Comparing two or more security measurements over time and comparing them to a known standard. This is subjective to sine extent as it involves analysis of a series of measurements.	May 16, 2011 11:03 AM
8	Set of measurements meaningful to tracking success/failure of an activity.	May 16, 2011 7:11 AM
9	The specific units of measurement used to quantify something	May 16, 2011 12:24 AM
10	A set of measurements applied over a domain, such as time, space, or other variable basis.	May 15, 2011 6:17 PM
11	A formally defined analysis of typically a series of measurements - often compared to a standard.	May 15, 2011 5:57 PM
12	recording and analyzing measurements, usually with an eye towards determining system norms or progress towards a goal	May 15, 2011 1:26 PM
13	measure of an organization's activities and performance.	May 14, 2011 8:52 PM
14	the art of measurement	May 13, 2011 5:43 PM
15	a predefined measurement that is usually repeated over time to show how a given process or item is performing (usually over time).	May 13, 2011 1:49 PM
16	the results of measurement exercises	May 13, 2011 12:18 PM
17	quantitative or qualitative grouping or ranking - what you get after you correlate your measurements	May 13, 2011 10:17 AM
18	statistics used to monitor something	May 13, 2011 10:05 AM
19	the dimensions or attributes used to measure	May 13, 2011 10:03 AM
20	Meaningful and balanced measurements aligned with business goals and objective to identify and measure the effectiveness of controls against some meaningful criteria.	May 13, 2011 9:54 AM
21	A discrete and measurable parameter	May 13, 2011 9:50 AM

Page 4, Q17. The word “metrics” means:

22	Measure of performance	May 13, 2011 9:34 AM
23	relative to a defined set of atributes	May 3, 2011 8:23 AM
24	Measurements.	Apr 27, 2011 6:51 PM
25	measurement of performance or progress	Apr 25, 2011 10:33 AM
26	a set of key processes and systems states to measure	Apr 25, 2011 8:37 AM
27	(my definition for business metric) - measurement of performance	Apr 25, 2011 7:18 AM
28	intuitively I'd say a measurement or set of measurements that provide feedback on previous decisions and therefor inform future decisions	Apr 25, 2011 6:08 AM
29	number of units of specific standard	Apr 23, 2011 7:18 PM
30	an agreed-upon scale	Apr 23, 2011 4:41 AM
31	Metrics is a measurement through which one can take actions based on the data collected that can cause change.	Apr 22, 2011 11:18 PM
32	Quantifiable measurement	Apr 22, 2011 9:34 AM
33	The definition of what is being measured, including the characteristic and the unit of measure	Apr 22, 2011 9:25 AM
34	methodology for measuring and tracking changes in the attributes or characteristics of something	Apr 22, 2011 9:21 AM
35	Measurements used for decision-making.	Apr 22, 2011 9:00 AM
36	results of measuring	Apr 22, 2011 8:59 AM
37	measures of a number of variables to discern information about a system	Apr 19, 2011 4:47 AM
38	A dimension of analysis used to quantify and understand performance of a thing or an activity	Apr 18, 2011 5:41 PM
39	repeatable measurements expressed as numeric values	Apr 14, 2011 7:31 AM
40	A means for converting a set of measurements into a quantity related to criteria that are helpful in decision-making regarding a system or phenomenon.	Apr 7, 2011 1:53 PM
41	Standards of measurement by which efficiency, performance, progress, or quality of a plan, process, or product can be assessed.	Apr 5, 2011 9:14 AM
42	measure scientifically and methodically	Apr 4, 2011 6:24 AM
43	Metrics describe a system of measurement that includes the item being measured, the unit of measurement, and the value of the unit	Apr 1, 2011 9:13 AM
44	Quantifiable measurement	Mar 28, 2011 8:17 AM

Page 4, Q17. The word “metrics” means:

45	A measure statistic	Mar 27, 2011 4:30 AM
46	A time series of measurement instances.	Mar 23, 2011 12:55 PM
47	the definition what is being measured	Mar 22, 2011 4:37 PM
48	A set of measurements as defined above that together help manage some business process/purpose	Mar 22, 2011 9:34 AM
49	A measure to assess performance using an agreed-upon standard	Mar 22, 2011 7:05 AM
50	define in measurable terms	Mar 21, 2011 2:07 PM
51	The ability to quantify what specific items you are trying to measure in a quantitative or qualitative manner.	Mar 21, 2011 8:41 AM
52	Comparing a measurement against a baseline or trend.	Mar 21, 2011 6:18 AM
53	a set of properties	Mar 21, 2011 6:03 AM
54	Collection of measurements to assist in making management decisions.	Mar 21, 2011 12:22 AM
55	measuring	Mar 20, 2011 9:56 PM
56	Meaningful information that gives insight into how a process is internally operating	Mar 20, 2011 7:58 PM
57	The set of objective, verifiable, repeatable relationships between quantities (larger vs smaller) as opposed to non-quantifiable relationships (better vs. worse).	Mar 20, 2011 8:13 AM
58	use of statistics to inform, educate and clarify useful information about subjects or items of interest in relation to a field of interest	Mar 20, 2011 7:06 AM
59	measurable properties	Mar 19, 2011 10:13 PM
60	A standard measurement.	Mar 19, 2011 7:15 PM
61	The standard by/against which one measures.	Mar 19, 2011 6:01 PM
62	n/a	Mar 19, 2011 5:06 PM
63	the rationalization of a lot measurements	Mar 11, 2011 11:39 AM
64	a unit of measurement deemed meaningful that used to provide feedback on a process or technology.	Mar 10, 2011 7:35 AM
65	A collection of measurements over thime that allow comparison and identification of patterns, changes or outliers	Mar 9, 2011 3:43 PM
66	*	Mar 9, 2011 2:18 PM
67	Metrics are a collection of measurements	Mar 9, 2011 6:59 AM

Page 4, Q17. The word “metrics” means:

68	Metrics however are about analysis and intelligent decision making. Metrics translate data into meaningful information which will support decision making. Information is something you use to make decisions.	Feb 15, 2011 9:50 AM
69	A set of mechanisms used for measurement	Feb 14, 2011 10:49 PM
70	Could mean the same as measurements. Or could be a specific set or collection of measurements designed or conceived to provide information about an object or a process	Feb 14, 2011 8:23 PM
71	Key Performance Indicators	Feb 14, 2011 5:17 PM

Page 4, Q18. The phrase “security metrics” means:		
1	A measuring system that reflects something related to the achievement of security goals	Jun 6, 2011 9:57 PM
2	A metric that allows one to draw a conclusion of some sort related to security.	May 21, 2011 10:16 AM
3	scale for measuring some protecion element	May 20, 2011 10:59 AM
4	Measurement of the security posture of a system, organization, etc.	May 18, 2011 1:57 PM
5	Metrics based on IT security performance goals and objectives	May 16, 2011 10:59 PM
6	Hybrid of metrics used as guidelines for assessing the baseline best practices with regards to preventing unauthorized access or asset loss.	May 16, 2011 12:41 PM
7	Analyzing measurements of security factors, such as those expressed in the McCumber Cube, and comparing system goals to actual outcomes/reality.	May 16, 2011 11:03 AM
8	Set of measurements meaningful to tracking level of provided security.	May 16, 2011 7:11 AM
9	Aspects of security used to quantify something in the field	May 16, 2011 12:24 AM
10	Metrics associated with security, such as costs or incidents per some period.	May 15, 2011 6:17 PM
11	Metrics applicable to IT security.	May 15, 2011 5:57 PM
12	metrics applied to security features such as confidentiality integrity and availability, or to security strategies for prevention, detection, and response	May 15, 2011 1:26 PM
13	measure of an organization's activities and performance around infosec	May 14, 2011 8:52 PM
14	measurements of security risk and effectiveness	May 13, 2011 5:43 PM
15	a predefined measurement that is usually repeated over time to show how a given security process, or tool is performing (usually over time).	May 13, 2011 1:49 PM
16	the results of measurement exercises that are related to physical and/or logical security	May 13, 2011 12:18 PM
17	applying grouping or ranking to information management practices to assess and improve maturity of practices	May 13, 2011 10:17 AM
18	security related statistics	May 13, 2011 10:05 AM
19	the set of attributes or security practices used to determine how secure something is. Often used in conjunction with an overarching framework like ISO 27002.	May 13, 2011 10:03 AM
20	Meaningful and balanced measures that bring/improve transparency of the organization's security posture, program / assurance / compliance / technology risk that are continuously re-evaluated and rebalanced to ensure effectiveness of risk identification and mitigation.	May 13, 2011 9:54 AM
21	Measurable feedback system related to established security goals.	May 13, 2011 9:50 AM
22	Measure of performance around protecting unauthorized or unintended use of systems.	May 13, 2011 9:34 AM

Page 4, Q18. The phrase “security metrics” means:		
23	those atributes/metrics that demonstrate the efficacy of security controls	May 3, 2011 8:23 AM
24	A migraine.	Apr 27, 2011 6:51 PM
25	measurement of performance, progress, or effectiveness of a variety of security controls or remedial activities	Apr 25, 2011 10:33 AM
26	the key security processses and systems states to measure	Apr 25, 2011 8:37 AM
27	measurement of performance or state in one aspect of security (CIA - or Hexad implied)	Apr 25, 2011 7:18 AM
28	metrics for information security	Apr 25, 2011 6:08 AM
29	threat levels	Apr 23, 2011 7:18 PM
30	decision support	Apr 23, 2011 4:41 AM
31	Metrics that are used to improve the security posture and risk.	Apr 22, 2011 11:18 PM
32	Overall program objectives and measurements	Apr 22, 2011 9:34 AM
33	Once the term "security" is defined, measuring how "secure" something is against some scale	Apr 22, 2011 9:25 AM
34	measuring and tracking changes in security posture.	Apr 22, 2011 9:21 AM
35	Metrics used to make security-related decisions.	Apr 22, 2011 9:00 AM
36	measures specific to security	Apr 22, 2011 8:59 AM
37	measures of values to discern information about the security posture of a system	Apr 19, 2011 4:47 AM
38	Those dimensions of analysis dealing with risk and vulnerability, and also efforts both preventative and reactive to mitigate consequences of exploits.	Apr 18, 2011 5:41 PM
39	repeatable security measurements expressed as numeric values	Apr 14, 2011 7:31 AM
40	A means for converting a set of measurements related to the assurance that a computer-based system can in some manner be disrupted, into a quantity related to criteria that are helpful in decision-making regarding that system.	Apr 7, 2011 1:53 PM
41	Standards of measurement by which efficiency, performance, progress, or quality of a security plan, process, or product can be assessed.	Apr 5, 2011 9:14 AM
42	Methodically measure the security posture of a define system or a set of systems.	Apr 4, 2011 6:24 AM
43	Security metrics are a series of key measurements that help quantify the amount of risk that exists in a given envrionment/situation	Apr 1, 2011 9:13 AM
44	Provide quantitative and objective basis for security operations	Mar 28, 2011 8:17 AM
45	A measure related to an aspect of security performance	Mar 27, 2011 4:30 AM
46	Metrics defined by each entities security program.	Mar 23, 2011 12:55 PM

Page 4, Q18. The phrase “security metrics” means:		
47	The definition of security measures	Mar 22, 2011 4:37 PM
48	A set of metrics as defined above that deal with security/risk/loss related aspects of a business process	Mar 22, 2011 9:34 AM
49	measurs to assess the performance or effectiveness of a security control or process	Mar 22, 2011 7:05 AM
50	define some aspect of security or security investment in measurable terms	Mar 21, 2011 2:07 PM
51	The ability to quantitative or qualitative present a true picture of the security posture of an organization to a variety of responsible parties.	Mar 21, 2011 8:41 AM
52	Comparing the effectiveness of security controls against an established goal in order to assess risk posture.	Mar 21, 2011 6:18 AM
53	whatever you want it to be	Mar 21, 2011 6:03 AM
54	Collection of measurements to assist in making management decisions related to security.	Mar 21, 2011 12:22 AM
55	mesuring security	Mar 20, 2011 9:56 PM
56	Meaningful information that gives insight into how security processes are internally operating	Mar 20, 2011 7:58 PM
57	A set of quantifiable relationships between measurable security attributes.	Mar 20, 2011 8:13 AM
58	use of statistics about security topics and conditions such as threats, security incidents, perpetrators, and controls	Mar 20, 2011 7:06 AM
59	measurable properties relevant to securing systems. In this case, industrial control systems.	Mar 19, 2011 10:13 PM
60	Standard measurements used to determine ranges of security.	Mar 19, 2011 7:15 PM
61	The standards by which one evaluates the state of or improvement in security.	Mar 19, 2011 6:01 PM
62	n/a	Mar 19, 2011 5:06 PM
63	metrics that directly or indirectly tie back to measurements of which there are security implications	Mar 11, 2011 11:39 AM
64	metrics that provides meaningful feedback on a security process or technology.	Mar 10, 2011 7:35 AM
65	applying the use of metrics to the security domain. representing activity, posture, evolution and variability	Mar 9, 2011 3:43 PM
66	*	Mar 9, 2011 2:18 PM
67	Security metrics are security related measurements that assist in highlighting a posture or position	Mar 9, 2011 6:59 AM
68	Security metrics are the meaningful measurements and metrics which support security decisions.	Feb 15, 2011 9:50 AM

Page 4, Q18. The phrase “security metrics” means:		
69	a set of mechanisms used for measuring security-related things	Feb 14, 2011 10:49 PM
70	Metrics that provide measurements about an aspect of security, or, more specifically in this context, information and IT security	Feb 14, 2011 8:23 PM
71	Measuring the success of Security Programs	Feb 14, 2011 5:17 PM

Page 4, Q19. In your opinion, are the best security metrics (please choose from the following drop-down list):		
1	The data set and desired conclusion dictate scale type, not the analyst's choice of favorites.	May 21, 2011 10:16 AM
2	It really depends on what specific factors of security are being measured. Some factors are best expressed in nominal metrics, and some in ordinal, interval or as ratios.	May 16, 2011 11:03 AM
3	The best metrics are domain- and availabiity-dependent.	May 15, 2011 1:26 PM
4	All are valid - just depends on what is trying to be shown.	May 13, 2011 1:49 PM
5	metrics incorporating value and uncertainty	May 13, 2011 12:18 PM
6	I do not think I can pick a "best"	May 13, 2011 10:17 AM
7	This question appears to be at the heart of your survey and I don't expect that you are getting meaningful responses. To do so, you should give the definitions you are using and examples.	May 13, 2011 10:03 AM
8	All those types have value depending on what you are trying to communicate/measure.	May 13, 2011 9:54 AM
9	Combination	May 13, 2011 9:50 AM
10	Security metrics can be expressed in several ways.	Apr 25, 2011 10:33 AM
11	It depends on the metrics, both ordinals and percentages / ratios a good methodologies depending on the specific metric	Apr 25, 2011 8:37 AM
12	those that have business correlation, and can be collected analyzed and communicated to support decisions (I assume your context implies that this capability exists, but in truth most organizations struggle reaching a minimal level of maturity) Your question brought to mind a similar question: "What is the best language?" My response to that has always been similar to the one above. Those with the ability to communicate in multiple languages have strong oppinions in this area, but if you ask a laguage professor they will often slap their foreheads and wish that their students knew how to communicate in any language. (My 2 cents from the soapbox)	Apr 25, 2011 7:18 AM
13	security metrics - should uniquely designed in each case based on some standard methods	Apr 23, 2011 7:18 PM
14	Nominal and actual	Apr 22, 2011 9:34 AM
15	Are of these metrics could be used to either measure specific activities or show how the certain attribues have changed over time.	Apr 22, 2011 9:21 AM
16	The best security metrics are key performance indicators that are defined by process owners used to determine the health of business processes with imbedded controls. The KPIs can be divided into implementation KPIs that represent work effort to implement controls and "run the business" KPIs that represents on-going processes.	Apr 22, 2011 8:59 AM

Page 4, Q19. In your opinion, are the best security metrics (please choose from the following drop-down list):		
17	Other. All can be useful. For example, for categorizing attack types, nominal is useful. For relating risk levels, ordinal can be useful. For evaluating security outcomes, such as number of attacks resulting in financial losses exceeding a specific value, interval can be useful. For evaluating the level of human effort that is spent on SW patching in a company from year to year, ratio can be useful.	Apr 7, 2011 1:53 PM
18	security Metrics should be used as transitory - they are not true representation of performance or status, but more a convenient means to define targets, benchmarks, status for the temporary time they remain relevant and are not gamed	Mar 27, 2011 4:30 AM
19	Depends on the context, the metric and the ultimate use.	Mar 23, 2011 12:55 PM
20	"It Depends": different numeric representations are appropriate for expressing and communicating different concepts. Ratios are extremely useful and well understood in many business contexts (by non-security and non-technical folk), but are often misused (intentionally and unintentionally). Ordinal scales are easy to understand and if used correctly can convey an enormous amount of information in a very compact format (i.e. a Class 1 Cleanroom) if the science is sufficiently mature to have such constructs (i.e. not information security!).	Mar 22, 2011 9:34 AM
21	It depends. I can foresee cases where each of these terms would be appropriate depending on what is being measured and how. Ordinal for how many repeat issues I have identified in a risk assessment. Ratio, for percentage of devices that are in compliance with control standards. Interval, the number of malicious packets detected per unit of time...	Mar 22, 2011 7:05 AM
22	I'm not sure that there is such a thing as a security metric.	Mar 20, 2011 8:13 AM
23	Ordinal is useful in some instances where perception is wanted (ie: asking for opinion on a scale of 1-5) but cardinal (actual count) seems most useful in IT Security (ie: # of intrusions by type; cost to remediate versus severity of threat, etc,	Mar 20, 2011 7:06 AM
24	I do not yet believe they exist for industrial control systems	Mar 19, 2011 10:13 PM
25	visualisations	Mar 19, 2011 5:06 PM
26	interesting question. I would error on the side of ratio but it depends on the purpose of the metric and what it is composed of.	Mar 11, 2011 11:39 AM
27	you need a combination of some, even all, of the above. It will depend on which aspect of security you are attempting to assess measurements from	Mar 9, 2011 3:43 PM
28	All the traditional scale measurement types are applicable in some manner. The key is to use them where they serve the necessary purpose (in support of making good decisions)	Feb 15, 2011 9:50 AM
29	As of today,m these are the best available in most cases.	Feb 14, 2011 10:49 PM

Page 4, Q20. Please explain the reasoning behind your answer to Question 19:		
1	In my work in the IT Controls Benchmarking work that spanned over 1000+ organizations, we were able to use units of measures using ratios, and there was a zero point. E.g., change success rate. But many of the metrics were Intervals e.g., Likert style questions about the perceived value and culture.	Jun 6, 2011 9:57 PM
2	For example, I'm currently using the following metrics in my work: Nominal - From a vulnerabiltiy scan, perform root cause analysis to determine _why_ the vuln was present. Categories include: "Base build design," "bad build execution," "bad configuration management," "bad patch management," and several others. By comparing the counts, we can draw conclusions about which root cause is the most important to address next. Ordinal - But, we might want to weight our nominal counts above based on the High/Medium/Low risk ranking of the vulnerabilities. Though, this becomes a problematic technique precisely because the values are ordinal and we seem to be attempting to use them as interval or ratio scale types. Interval - I might also want to track degree of deviation from a baseline (i.e. how far from the desired configuration is my current configuration) Ratio - and, if I'm ever compromised, how many consumers will I have to purchase identity monitoring for? There certainly is a problematic out there for scale types in security metrics. Mainly the issue is that most plausible risk measurements require the use of one or more metrics where the data only supports a nominal or ordinal data set but we're trying to perform analysis that can only be done with interval or ratio scale types. Unfortunately, you 'can't get there from here' without breaking some analytical rules.	May 21, 2011 10:16 AM
3	Based on operational experiences	May 20, 2011 10:59 AM
4	It's easier to explain a ratio to higher level management.	May 18, 2011 1:57 PM
5	My degree is in business, with another year in computer science courses, but not a lot of math.	May 16, 2011 10:59 PM
6	I am not familiar with the application of 'ordinal' and 'ratio' in the context of security metrics.	May 16, 2011 12:41 PM
7	I know you probably want a more detailed response, but I don't think any one level of measurement is optimal over the others for every security factor.	May 16, 2011 11:03 AM
8	Unfamiliar terms.	May 16, 2011 7:11 AM
9	I don't know	May 16, 2011 12:24 AM
10	I haven't run into those terms in a context that applies here.	May 15, 2011 6:17 PM
11	I'm familiar with "analytics", but not specifically in the security field - and don't recognize those terms.	May 15, 2011 5:57 PM
12	We dislike comparing apples and oranges, but at the same time cannot in the real world distill our measurements down to a common number (such as $). We use what we can gather, then focus on specific project domains where the measurements can still make some useful sense.	May 15, 2011 1:26 PM
13	??	May 14, 2011 8:52 PM

Page 4, Q20. Please explain the reasoning behind your answer to Question 19:		
14	security metrics should reflect risk - particularly residual risk and where possible be measured in dollars so they are most relevant to the business.	May 13, 2011 5:43 PM
15	I think metrics should be flexible to drive behavior in a desired direction. It doesn't so much matter what clothing you dress your data in - it matters that they are accurate enough to show where you are now and the direction you have come.	May 13, 2011 1:49 PM
16	Pure numeric metrics omit value and uncertainty characteristics that are important for decision making. Even ratios are not helpful unless put into an appropriate context expressed as value measures. Value measures are seldom precise so should be expressed in the form of probability distributions.	May 13, 2011 12:18 PM
17	My use of metrics is not particularly mature or consistent. I rely a great deal on the judgement and consensus of SMEs.	May 13, 2011 10:17 AM
18	these are unfamiliar to me	May 13, 2011 10:05 AM
19	see above	May 13, 2011 10:03 AM
20	All the types of metrics have value depending on what variables you are trying to measure and analyse. Patch status for example lends itself to be a ratio metric because you are trying to measure an absolute status. Some metrics require significant amounts of historical data to become meaningful. Nominal metrics, such as heat maps, are used to present high level status data in a visually easy to interpret form. So all metric types are valid depending on the data set and the analytical/audience objective.	May 13, 2011 9:54 AM
21	Depends on nature/purpose of measurement: compliance, comparison to external, comparison to past performance. I prefer nominal (binary) for Compliance issues. For comparative measurements with external models I prefer ordinal. For continuous improvement I prefer ratios, using prior performance as the non-arbitrary zero point.	May 13, 2011 9:50 AM
22	terms unfamiliar.	May 13, 2011 9:34 AM
23	It is all relative. There is no absolute in security.	May 3, 2011 8:23 AM
24	It's complicated.	Apr 27, 2011 6:51 PM
25	Not sure if there are "Best" security metrics. I think the best security metrics are "meaningful" security metrics within the context of the environment or organization.	Apr 25, 2011 10:33 AM
26	practical experience	Apr 25, 2011 8:37 AM

Page 4, Q20. Please explain the reasoning behind your answer to Question 19:		
27	(I assume your context implies that this capability exists, but in truth most organizations struggle reaching a minimal level of maturity) Your question brought to mind a similar question: "What is the best language?" My response to that has always been similar to the one above. Those with the ability to communicate in multiple languages have strong oppinions in this area, but if you ask a laguage professor they will often slap their foreheads and wish that their students knew how to communicate in any language. (My 2 cents from the soapbox)	Apr 25, 2011 7:18 AM
28	provides the most statistical manipulations and maps more to reality than others.	Apr 25, 2011 6:08 AM
29	personal experience	Apr 23, 2011 7:18 PM
30	nothing is stable enough to develop an actuarial tail	Apr 23, 2011 4:41 AM
31	I am not familiar with these terms in this context	Apr 22, 2011 11:18 PM
32	Need to set expectations and measure against achieving them.	Apr 22, 2011 9:34 AM
33	We don't have a number scale for measuring "security" so that rules out Interval and Ratio. But security can be relative (machine A is more secure than machine B based on measurements X and Y). Nominal makes no sense here.	Apr 22, 2011 9:25 AM
34	We may measure specific events, specific attributes or characteristics, specific changes in attributes over time or measurement one attribute with respect to another. Thus, all of the techniques have a place in the metrics behind security.	Apr 22, 2011 9:21 AM
35	The more quantitative, the more exact, the more useful in comparisons and trade-off decisions.	Apr 22, 2011 9:00 AM
36	Metrics are numbers and output- a broad definition. the best security metrics are measures of process health where controls are part of those processes	Apr 22, 2011 8:59 AM
37	Ordinal values based against historical trends to show increasing or decreasing values.	Apr 19, 2011 4:47 AM
38	I relied on Jennifer to answer these questions. LoL!	Apr 18, 2011 5:41 PM
39	Most security issues are best represented in a relative manner instead of absolutes, specific targets, or qualitative statements.	Apr 14, 2011 7:31 AM
40	The "best" metric depends on the questions being asked regarding assurance and the value of assurance, and the best questions are dependent on the issues under evaluation and their relationship to overall system objectives .	Apr 7, 2011 1:53 PM
41	Not sure most technology or security executives understand those terms - could just mean I'm a dork!	Apr 5, 2011 9:14 AM
42	N/A	Apr 4, 2011 6:24 AM
43	Includes an absolute zero point and allows more effective comparison of relative risk values	Apr 1, 2011 9:13 AM

Page 4, Q20. Please explain the reasoning behind your answer to Question 19:

44	We use metrics to show progression (or lack there of) over time.	Mar 28, 2011 8:17 AM
45	Like all metrics they become gamed unless reality is more difficult to achieve than the metric itself.	Mar 27, 2011 4:30 AM
46	Self explanatory.	Mar 23, 2011 12:55 PM
47	You benefit more from something that at least can be put into an order and not just named	Mar 22, 2011 4:37 PM
48	It's in the Other box.	Mar 22, 2011 9:34 AM
49	See response to 19	Mar 22, 2011 7:05 AM
50	best to measure in relative ranges as it is hard to nail down an absolute for security	Mar 21, 2011 2:07 PM
51	Try to show the good, bad and ugly side of things. Draw from history to show the bad side and tie it to cost and then deterministically show the present posture or potential for future if things are put into place.	Mar 21, 2011 8:41 AM
52	Ratio determines how close you are above/below the goal.	Mar 21, 2011 6:18 AM
53	It is a relatively new and unscientific field.	Mar 21, 2011 6:03 AM
54	We may use different terminology to explain the same things.	Mar 21, 2011 12:22 AM
55	Minimal valid data	Mar 20, 2011 9:56 PM
56	To have the ability to see how information is related to processing steps or rework steps tells us how well controlled a process is operating. Proportions of information that is constantly changing state (e.g. percentage of exceptions coming up for expiry) tells us how the processing related to closing exceptions is operating or not operating as intended.	Mar 20, 2011 7:58 PM
57	Security is an epiphenoninon, a second-order effect of a business process as implemented in a cultural context. As such it is difficult to define repeatable, comparable, quantifiable objective measures of security.	Mar 20, 2011 8:13 AM
58	personal preference when reading statistics in security research	Mar 20, 2011 7:06 AM
59	Relevant metrics unique to control system cyber security have not been established	Mar 19, 2011 10:13 PM
60	It allows for an absolute zero which allows for meaningful interpretation.	Mar 19, 2011 7:15 PM
61	Pass	Mar 19, 2011 6:01 PM
62	aggregation of security metrics is impossible	Mar 19, 2011 5:06 PM
63	e.g. a metric (or indicator) could be something like the amount of risk one has assumed. a ratio is probably a better value to present (ratio of assumed to total, or ration of assumed to establish limits..etc).	Mar 11, 2011 11:39 AM

Page 4, Q20. Please explain the reasoning behind your answer to Question 19:		
64	I do not have a formal background in metrics development	Mar 10, 2011 7:35 AM
65	Some things in security are "countable" but others are only qualitatively assessable.	Mar 9, 2011 3:43 PM
66	*	Mar 9, 2011 2:18 PM
67	They need to be numerical in order to prevent any dispute	Mar 9, 2011 6:59 AM
68	All the traditional scale measurement types are applicable in some manner. The key is to use them where they serve the necessary purpose (in support of making good decisions)	Feb 15, 2011 9:50 AM
69	As of today,m these are the best available in most cases.	Feb 14, 2011 10:49 PM
70	ratio, or cardinal numbers can be manipulated in legitimate ways by arithmetic and statistics. Nominaland ordinal values can only be counted; performing other arithmetic operations on ordinal values is problematic.	Feb 14, 2011 8:23 PM
71	N/A	Feb 14, 2011 5:17 PM

Page 5, Q21. Please rate the following list of activities on a scale from 0 to 5, where the number indicates the contribution of the activity to an organization's ability to maintain its security. Each activity must be assigned its own number, but the number can be zero:

1	I'm assuming that zero means "zero contribution" and 5 means "max contribution"	Jun 6, 2011 10:01 PM
2	Jennifer - a note here. The answers to these questions vary depending on the organization. So, I chose my current org to use as a case study since I think what you are really interested in here is the differential between architect and management.	May 21, 2011 10:16 AM
3	Establish priority of security relative to other business functions.	May 16, 2011 7:17 AM
4	Support from the top. Effective enforcement of policy and standards.	May 13, 2011 12:23 PM
5	Quantify, as used above does not necessarily mean to assign a numeric value, rather, it means to be ale to "reason" about the value. Something can be recognized as critical to an organization without assigning a specific dollar value.	May 13, 2011 10:08 AM
6	analyze data from internal and external sources to understand user behavioral patterns to identify anomalies for trending analysis, new control requirements, incident response and forensic analysis.	Apr 22, 2011 9:19 AM
7	Question 21 was answered to indicate our ability/position to track metrics against each line item, not as a representation of our security health.	Mar 28, 2011 8:32 AM
8	Working with the vendors to understand what they feel is baseline security and what peers are doing to make security a reality. Operational security is significanlty different at times from theoretical. You need to implement and sometimes policy does not match reality.	Mar 21, 2011 8:48 AM
9	Segregation of duties	Mar 20, 2011 10:07 PM
10	Expert IT security staff with expert knowledge of systems, infrastructure, architecture, vendors, and the ability to influence, control, or better yet prevent anything that impacts on security.	Mar 20, 2011 7:59 AM
11	Assignment of duties and responsibility, supervision, variance detection (including incident detection), timely corrective action and remediation, safe defaults,	Mar 19, 2011 6:16 PM
12	Apply and maintain a fluid defense-in-depth strategy across the organization with the goal being 'optimal' security.	Feb 15, 2011 9:56 AM
13	The questions have different answers for different situations	Feb 14, 2011 10:52 PM

Page 5, Q22. Please answer this question from the perspective of the highest level of management in your organization (e.g. CEO or President), as you perceive them to think about security. That is, how would your management rate, on a scale of 1 to 5, where 5 is the highest indicator that an organization whi...

1	The CEO doesn't care. He hired me to do this for him and provide the security assurance the business needs. He wouldn't understand the implications of half of this. Just expects me to cost effectively assure security for our businesses.	May 13, 2011 5:58 PM
2	Protect company reputation. That is what (my) execs really care about from InfoSec.	May 13, 2011 10:25 AM
3	Ability to "pass" audit	Apr 25, 2011 7:25 AM
4	IT Security expertise, diligence and reliability on the part of employees given responsibility for security	Mar 20, 2011 7:59 AM
5	Express enterprise risk tolerance, assign responsibility for asset protection, require timely measurement and reporting.	Mar 19, 2011 6:16 PM
6	Different for different situations	Feb 14, 2011 10:52 PM

Page 6, Q23. Please select the sentence fragments that complete the stem sentence and make it true (select all that apply):

System security verification requires

1	...qualification of system assets, ...qualification of system threat environment, ...qualification of impact of system vulnerability exploit. (Quantification is not practicable in our real world.)	May 15, 2011 1:34 PM
2	I'm not comfortable with the use of "quantification" in the above. Probability for example is notoriously hard to assign.	May 13, 2011 10:32 AM
3	see previous comment about quantification - need enough information to "reason" about each topic	May 13, 2011 10:11 AM
4	An assessment of how the integrated security components combine to defend against, discover or respond to attacks.	Apr 7, 2011 2:06 PM
5	some verification technique (need not be cost-effective) nor the assets, threats, and vulnerabilities quantified although that would give best results for presentation /communication purposes	Mar 20, 2011 9:10 AM

Page 6, Q24. Please rate the following system abilities on a scale of 1 to 5, where 5 is the highest indicator that a system which exhibits these attributes is secure and 1 is the lowest or least significant indicator that the system exhibits security.

1	Threat modeling based external security assessment. Audit is this game where you define control objectives, controls, evidence sets, and check things off a list. Security is a different game where an adversary tries to defeat, in the most generic sense, your creativity. That's why you need the assessment to include external threat modeling (i.e. the creativity of other experts applied to your problem) which audit does, in theory, perfectly but, in practice, at best, poorly.	May 21, 2011 10:24 AM
2	We need to continue our mission while under attack, including partially successful attacks. This goes further than SLAs to include unwritten and assumptive mission needs.	May 15, 2011 1:34 PM
3	Assumption is that abilities applie to system confidentiality and integrity and not to availablility.	May 13, 2011 12:29 PM
4	Withstand targeted penetration attacks by skilled attack teams that are similar to expected threat actors: 5	Mar 22, 2011 9:41 AM
5	these generally do not apply to industrial control system cyber security	Mar 19, 2011 10:18 PM
6	Provide reliable control over and relative ease in demonstrating the behavior, use, and content of the system.	Mar 19, 2011 6:25 PM
7	The question is a poor one since the term "security" is poorly defined.	Feb 14, 2011 10:54 PM

Page 7, Q25. Please rate the following types of measurement on a scale of 1 to 5, where 5 is the highest indicator that a measurement of the given type is useful in measuring system security and 1 is the lowest or least significant indicator that measurement of the given type is useful in measuring system sec...

1	Please disregard score for "other" I had to check something to get the comment box. With regard to "performance" I assume you mean performance of security controls, not transaction throughput which may or may not be relevant.	May 21, 2011 10:39 AM
2	System security compared to what?	May 13, 2011 12:35 PM
3	Completeness of expected inventory vs. reality.	Mar 23, 2011 1:01 PM
4	I believe you need to know what the security, auditability and control basis and features that are part of a system to make an eduacated judgement call... What is the package including compensating controls that can be applied.	Mar 21, 2011 8:53 AM
5	metrics demonstrating most threats are routinely thwarted and anomolies are caught in system security set of controls as well as forward looking controls to handle zero day and other threats that can be anticipated but may not have occurred yet (not all orgs can support this but this is my ideal)	Mar 20, 2011 9:25 AM
6	Time to variance detection and corrective action.	Mar 19, 2011 6:32 PM

Page 7, Q26. Please rate following system characteristics on a scale of 1 to 5, where 5 is the highest indicator that system security requirements should be easy to identify and gather, and 1 is the lowest or least significant indicator that system security requirements should be easy to identify and gather.

1	Please disregard score for "other" I had to check something to get the comment box. Having seen your presentation at MMC, I know that the last two go to your thesis - which I'm not necessairilly a fan of (you've set up your problematic differently than I would have). But, with regard to this question, the first three are of one type and the last two are of another. They can't be compared this way. If I really want to know if a system is secure, I need to look at its inputs and outputs. To the degree that a system is comprised of other systems (i.e. COTS or functional components) then those become systems with their own I/O. At best these describe scope. In terms of measurement, one would use the concepts of the last two (i.e. I/O) to measure the first three and the first three are descriptive scopes by which you could compare between dispirate systems.	May 21, 2011 10:39 AM
2	Need to have set of best-of-breed, well-proven requirements rather than "commonly used" since the latter don't seem to be working.	May 13, 2011 12:35 PM
3	The environment requires easy to understand system documentation from inception to production with security being an identifiable component at all levels. As much detail as is needed to fully describe security related elements/functions is required and development phases are reviewed and accepted or rejected based on completeness and ease of understanding.	Mar 20, 2011 9:25 AM
4	Audit trail fixes accountability for all significant events.	Mar 19, 2011 6:32 PM

Page 9, Q33. The National Institute of Standards and Technology has published Performance Measurement Guide for Information Security (NIST SP800-55, original 2003 updated 2008). Please select the response from the following drop-down list that most closely describes your experience with that document:

1	I remember studying NIST 800-55, but could not readily differentiate it from the COBIT framework, so didn't refer to it afterwards. I thought it was valid, but remember thinking it needed more discussion of the context of which info sec operates in (e.g, appdev, IT operations, etc.)	Jun 6, 2011 10:17 PM
2	It is an approach. Certainly a practicioner who implemented it or portions of it would be far ahead of a practicioner that didn't and certainly, for example within the enormous community of federal departments and agencies, using a common standard, rather than rolling one's own, makes sense. But, in practice, I'll probably roll my own metrics based on what I'm trying to accomplish most of the time and I will only look to use a standard like this if I need to compare myself to others and if that comparison will be useful (i.e. they are my peers) and if the data exists where I can get to it. As for question 32, I couldn't proceed without checking something for the standards that I don't know well. So, on all of the ones where I checked "1" in question 31, I also checked "1" in 32. These responses should be translated into null.	May 21, 2011 10:59 AM
3	Seems like a good model, especially the way it develops foundation of management and builds metrics and quantifiable practices on top of this foundation.	May 16, 2011 11:40 AM
4	Not particularly applicable to an agile ecommerce environment	May 13, 2011 6:09 PM
5	SP800-55 categories are useful, but is too overly reliant on percentage measurements.	May 13, 2011 5:54 PM
6	I'm familiar with a number of the NIST SP 800 series and might refer to them from time-to-time, but do not look to them on a regular basis. Nor, do I think, do most infosec practitioners. You hardly eve see them referenced in conferences or in the commonly-used popular infosec press. I think that there is a general perception in the corporate world that NIST publications apply to government, not the private sector.	May 13, 2011 12:51 PM
7	I'm not familiar with this standard	Apr 23, 2011 7:43 PM
8	It's one approach	Apr 22, 2011 11:54 AM
9	It's been quite a few years since I read through it.	Apr 22, 2011 9:57 AM
10	It describe how to go about thinking about metrics in an educational manner.	Apr 22, 2011 9:13 AM
11	I have no reason in using this guide as part of my research, so while I read the guide for general value, I have no basis for sustaining detailed recollections regarding what was presented.	Apr 7, 2011 3:24 PM
12	I believe it needs a serious update in light of the world of mobile and idevices...	Mar 21, 2011 9:00 AM
13	I agree in part but what good is it to measure how many mobile devices use encryption when answers are not captured by sensitivity level /criticality of data? I prefer specific operational statistics to tell the security story rather than adherence to standards. For example: penetrations that result in sec incidents by root cause and severity /cost trended to show actual increase or decrease over time with mitigation/recovery costs also presented.	Mar 20, 2011 11:56 AM

Page 9, Q33. The National Institute of Standards and Technology has published Performance Measurement Guide for Information Security (NIST SP800-55, original 2003 updated 2008). Please select the response from the following drop-down list that most closely describes your experience with that document:		
14	Pass	Mar 19, 2011 6:40 PM
15	n/a	Mar 19, 2011 5:12 PM

THE REMAINDER OF THE SURVEY CONTAINED CONTACT INFORMATION WHICH HAS BEEN DELETED FROM THIS DOCUMENT.