Information Systems Security, 16:100–108, 2007

ISSN: 1065-898X print/1934-869X online
DOI: 10.1080/10658980701260579

Taylor & Francis
Taylor & Francis Group

Do Information Security Professionals and Business Managers View Information Security Issues Differently?

R. Kelly Rainer, Jr. and Thomas E. Marshall
Department of Management,
College of Business,
Auburn University,
Auburn, AL, USA

Kenneth J. Knapp
Air Force Academy,
Colorado Springs, CO, USA

Gina H. Montgomery
College of Business,
Auburn University,
Auburn, AL, USA

INTRODUCTION

Organizations today know that information technology is essential not only for daily operations but also for gaining strategic advantage in the marketplace. The importance of information technology means that information security has also become important. Breaches in information security can result in litigation, financial losses, damage to brands, loss of customer confidence, loss of business partner confidence, and can even cause the organization to go out of business.

A recent study (Knapp, Marshall, Rainer, & Morrow 2006) surveyed 874 certified information system security professionals (CISSPs) to determine and rank the top 25 information security issues. Of the 18 highest-ranked issues, 10 were more managerial in nature rather than technical. Table 1 shows these ten issues with their ranks in parentheses.

As we consider these ten issues as a whole, we see how critically important it is for information security professionals to have strong business, management, and organizational skills. As we look at each issue individually, we see a list of specific areas where information security professionals should have competence in order to effectively operate in an organizational context. The list of issues in Table 1 represents the issues with which information security professionals often have the most difficulty addressing. For example, three of these issues emphasize the need for excellent communication between information security professionals and business managers. The issues of "top management support," "low funding and inadequate budgets," and "justifying security expenditures" are closely related. The support of organizational executives is clearly needed to obtain the necessary funding for the information security function. To obtain this funding, information security professionals must present a coherent business case for information security needs.

Information security professionals must also communicate with the entire user community to raise their awareness of information security issues through training and education, thereby promoting an organizational culture attuned to information security. Information security professionals must also work with business managers and the user community during the risk

Address correspondence to
R. Kelly Rainer, Jr., Ph.D.,
George Phillips Privett Professor
of Management Information Systems
at Auburn University,
Auburn, Alabama.
E-mail: rainerk@auburn.edu

TABLE 1 Top 10 Managerial Information Security Issues (Knapp et al., 2006)

Top management support (1)
User awareness training and education (2)
Vulnerability and risk management (5)
Policy related issues (e.g., enforcement) (6)
Organizational culture (7)
Business continuity and disaster preparation (10)
Low funding and inadequate budgets (11)
Justifying security expenditures (15)
Governance (17)
Legal and regulatory issues (18)

management process in planning for business continuity in the event of a disaster, in addressing policy related issues in information security, and in the governance of information security. Information security professionals must also take the lead in explaining legal and regulatory issues as they relate to information security requirements for the organization.

These issues can place a burden on many information security professionals, who typically have technical backgrounds. In fact, information security is arguably more of a people problem than a technological problem. Therefore, information security professionals must understand the business side of the equation and work closely with executives, business managers, and the user community to adequately protect the information assets of their organizations.

Despite their technical backgrounds, information security professionals placed 10 managerial issues among their top 18 information security issues. Consequently, it would be interesting to see if business managers agree with them. Accordingly, the purpose of this study is to examine the differences, if any, between information security professionals and business managers in the relative importance of a number of information security issues.

THE STUDY

The study used an online survey answered by a convenience sample of 23 business managers and 46 information security professionals. The business managers represented a variety of functional areas in their respective organizations: information technology (six), accounting/finance (six), marketing (five), operations (four), and general management (two). All information security professionals were CISSPs. The industries represented in the study included manufacturing (six), financial services (five), healthcare (three), insurance (three), transportation (three), and retail (three).

The survey for the business managers asked this question: Which of the following information security issues do you feel are the **most important for you to know something about** as you make decisions regarding the level of information security you need? The survey for the information security professionals asked this question: Which of the following information security issues do you feel are **the most important for your business managers to know about or be aware of**?

The survey contained 142 items concerning all aspects of information security in an organization (see Appendix). The items were derived from a review of the information security literature. Respondents were asked to add any items they thought necessary. None of the 69 respondents added any items, so we concluded that our list was reasonably inclusive. Respondents answered each item on 5-point scales, ranging from "very important" to "very unimportant."

The Appendix shows each information security item, and the average importance rating given to that item by information security professionals and by business managers. The items in the Appendix are ranked in descending order according to the information security professionals' average ratings.

ANALYSIS OF RESULTS

We first examined the ten most important items according to the information security professionals, and the ten most important items according to the business managers. Table 2 shows the issues for both groups.

The two groups have four items in common: confidentiality of information, integrity of information, availability of information, and backup and recovery. The first three of these items form the confidentiality, integrity, and availability (CIA) triad of information security and indicate that both groups realize the overall importance of information to the organization. Also, events such as the September 11 terrorist

TABLE 2 The Top 10 Items for Each Group

Information Security Professionals	Managers
1. Confidentiality of information	Confidentiality of information
2. Integrity of information	Backup and recovery
3. Firewalls	Business continuity planning
4. Layered defense	Access controls
5. Risk mitigation	Integrity of information
6. Availability of information	Availability of information
7. Backup and recovery	Physical security
8. Defense in depth	Incident detection
9. Demilitarized zone	ID theft
10. Risk management	Virus attacks

attacks and Hurricane Katrina have mandated the importance of backup and recovery.

Five of the remaining six items for the information security professionals are primarily technical in nature: firewalls, layered defense, risk mitigation, defense in depth, and demilitarized zone. These are "behind the scenes" technical issues that are relatively invisible to business managers. Information security professionals also rate risk management high, an issue with both technical and managerial aspects.

Interestingly, four of the remaining six items for the business managers are also technical in nature: access controls, physical security, incident detection, and virus attacks. These are technical issues that are more visible to managers than the technical issues considered important by many information security professionals. Managers deal with access controls and physical security every day, and security incidents and viruses are constantly in the news. The other two items that business managers consider important are more managerial in nature: business continuity planning and ID theft. Business continuity planning relates directly to backup and recovery, and ID theft has high visibility in the media.

We examined those items that were ranked higher by information security professionals than by business managers. This process revealed those items that information security professionals thought were more important for their business managers to know about than business managers thought they themselves should know about. As illustrated in Table 3, all ten items, with the exception of dumpster diving, are technical issues.

TABLE 3 Items More Important to Information Security Professionals

Issue	Mean Information Scurity Professional	Mean Business Manager	Difference
Scripts	3.76	3.04	0.72
Eavesdropping	3.73	3.04	0.69
Vulnerability scanners	3.98	3.35	0.63
Tunneling	4.24	3.65	0.59
Iris scans	3.24	2.65	0.59
Steganography	2.89	2.30	0.59
Dumpster diving	3.33	2.74	0.59
Browsing	3.41	2.83	0.58
Proxy server	4.35	3.78	0.57
TEMPEST attack	3.00	2.43	0.57

We then examined those items that were rated higher by business managers than by information security professionals. This process revealed those items that business managers thought were more important to know about than the information security professionals thought the managers should know about. As provided in Table 4, these ten items demonstrate a managerial orientation.

Finally, we examined those items that were rated nearly equally by both business managers and by information security professionals. This process revealed items that business managers and

TABLE 4 Items More Important to Business Managers

Issue	Mean Information Scurity Professional	Mean Business Manager	Difference
ID theft	3.85	4.30	–0.45
Relationship between infosec and employee productivity	3.54	3.96	–0.42
Warm site	3.41	3.74	–0.33
Competitive intelligence	3.46	3.70	–0.24
Cold site	3.30	3.52	–0.22
Hot site	3.74	3.96	–0.22
Theft	3.83	4.04	–0.21
Backup and recovery	4.43	4.61	–0.18
Access controls	4.30	4.48	–0.18
Authorization	4.04	4.22	–0.18

TABLE 5 Items in Basic Agreement Between the Two Groups

Issue	Mean Information Scurity Professional	Mean Business Manager	Difference
Tokens	3.54	3.57	–0.03
Dumb ID cards	3.16	3.19	–0.03
Cyberterrorism	3.50	3.52	–0.02
Incident containment	4.20	4.22	–0.02
Spyware	3.96	3.96	0
Pharming attack	3.70	3.70	0
Repudiation	3.89	3.87	0.02
Virus attacks	4.28	4.26	0.02
Availability of information	4.46	4.43	0.03
Incident recovery	4.16	4.13	0.03
Weak passwords	4.07	4.04	0.03

information security professionals considered to be equally important to know about. We found 11 items where the ratings of the two groups had a difference of less than .04, indicating basic agreement. Table 5 shows these 11 issues.

DISCUSSION

Our findings can be visualized as a continuum, which we illustrate in Figure 1. Business managers are at one end and are generally concerned with managerial aspects of information security. At the other end, information security professionals are mainly concerned with the more technical aspects of information security.

Tables 2, 3, and 4 provide support for this continuum. In general, information security professionals consider technical issues as more important than managers do (e.g., various encryption issues, network attacks, and certificate issues). Also, managers place greater emphasis on managerial issues than the information security professionals do. However, there are interesting areas of agreement and disagreement between the two groups.

- The two groups agree on the importance of systems that provide information confidentiality, integrity, and availability.
- The two groups place similar importance on backup and recovery. However, business managers place greater emphasis on five related issues: backup and recovery, business continuity planning, and hot, warm, and cold sites. Backup and recovery and business continuity planning made the managers' top 10 list, and managers rated the three types of backup sites higher than information security professionals did.
- Of the seven risk-related issues in our study, information security professionals rated six of the issues higher than business managers did, and the seventh, risk transference, was rated almost equally by the two groups. This finding points out that the entire risk management process is a major function of information security professionals.
- The three issues of competitive intelligence, disclosure threats, and information leaks, are closely related. All three are rated higher by business managers than by information security professionals. Business managers value competitive intelligence, while at the same time do not want to inadvertently disclose information to competitors also seeking competitive intelligence.
- The largest difference in rankings between the two groups is the issue of scripts. This finding may in part result from the fact that the issue is highly technical and many business managers may not understand vulnerabilities involving scripts.
- Business managers rated the issue of the relationship between information security and employee productivity more highly than the information security professionals did. In general, excessively rigorous information security measures can reduce employee productivity and can even decrease security. For example, requiring employees to memorize strong passwords for multiple applications can cause irritation and loss of productivity. Such a requirement will probably lead to employees writing down passwords, thus actually decreasing security.

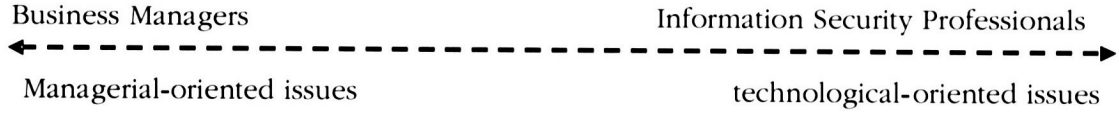

FIGURE 1 Continuum of Managerial and Technological Issues

- Business managers rated identity theft and social engineering as more important than information security professionals. These issues are closely related and result substantially from a lack of user awareness.
- Information security professionals rate technology to locate lost or stolen laptops more highly than business managers do. Considering the large number of laptops lost or stolen each year, it is surprising that managers did not rank this issue more highly.
- Managers place greater importance on spam and adware than information security professionals. Perhaps this is because these related issues are covered extensively in the media, thus influencing business managers more than technically well-informed information security professionals.
- Although the two groups agree on the importance of strong passwords, the information security professionals rated all issues regarding passwords and passphrases higher than managers did. This finding may come from information security professionals better realizing the dangers of weak passwords.

Overall, information security professionals rated 35 issues substantially higher than business managers, where the managers rated only two issues substantially higher than the information security professionals (see Appendix). These results may be because information security professionals have a stronger technical understanding of the many threats represented in these issues and thus rate them higher.

CONCLUSIONS

The important implication of our findings is that, for optimal organizational information security, business managers and information security professionals must move toward each other on the continuum. That is, business managers should have a basic knowledge of the more technical aspects of information security and information security professionals should have a better understanding of the managerial aspects of information security. Therefore, for information security professionals to move toward the center of the continuum, they must learn more about business functions such as accounting, finance, marketing, operations, human resources, organizational behavior, and project management.

By learning more about business administration, information security professionals will be better able to understand all aspects of information security in an organizational context. They will be able to discuss information security needs (e.g., budget requests) in terms of return on investment, employee productivity trade-offs, and metrics to measure the success of information security efforts. Further, a knowledge of business administration may provide information security professionals with several career benefits:

1. a better competitive position for promotion in their organizations,,
2. a better competitive position for management jobs in other functional areas of the organization,
3. positions in consulting firms, or
4. becoming an entrepreneur and starting a company.

In an ideal world, business managers would want to know more about the various technical aspects of information security, rather than relying totally on information security professionals. However, given the demanding workload and responsibilities of most business managers in today's competitive environment, it is unlikely that many managers will make the time to learn more about the technical side of information security. That being said, it is advisable that information security professionals take management and business classes to help them learn more about the organizational environment. If they do this, they will be more effective in addressing the top managerial issues, which in turn will lead to more effective information security programs.

REFERENCE

Knapp, K., Marshall, T.E., Rainer, R. Kelly, Jr., and Morrow, D. (2006). The Top Information Security Issues: What Can Government Do to Help? *Information Systems Security.* September/October, pp. 51–58.

APPENDIX

		Column			
		A	B	C	D
	Issue	Mean Information Security Professional*	Mean Business Manager	Difference (A-B)	See note†
1	Confidentiality of information	4.57	4.7	–0.13	
2	Integrity of information	4.54	4.48	0.06	
3	Firewalls	4.51	4.22	0.29	
4	Layered defense	4.48	4	0.48	▲
5	Risk mitigation	4.48	4	0.48	▲
6	Availability of information	4.46	4.43	0.03	
7	Backup and recovery	4.43	4.61	–0.18	
8	Defense in depth	4.41	3.96	0.45	▲
9	Demilitarized zone	4.37	4.17	0.2	
10	Risk management	4.37	4.22	0.15	
11	Virtual private networks	4.37	3.96	0.41	▲
12	Authentication	4.37	4.04	0.33	
13	Proxy server	4.35	3.78	0.57	▲
14	Business continuity planning	4.33	4.48	–0.15	
15	Risk analysis	4.33	4.13	0.2	
16	Trojan horse	4.3	4.04	0.26	
17	Access controls	4.3	4.48	–0.18	
18	Least privilege	4.28	4.04	0.24	
19	Virus attacks	4.28	4.26	0.02	
20	Intrusion detection system	4.26	4.09	0.17	
21	Risk planning	4.26	4.14	0.12	
22	Tunneling	4.24	3.65	0.59	▲
23	Worm attacks	4.22	4.04	0.18	
24	Internet protocol security (IPSec)	4.22	3.96	0.26	
25	Physical security	4.22	4.39	–0.17	
26	Incident reaction	4.2	4.09	0.11	
27	Incident containment	4.2	4.22	–0.02	
28	Strong passwords	4.2	4.04	0.16	
29	Passwords	4.2	3.91	0.29	
30	Incident detection	4.17	4.3	–0.13	
31	Encryption	4.17	4.09	0.08	
32	Digital certificate	4.17	3.74	0.43	▲
33	Privilege	4.17	4	0.17	
34	Incident recovery	4.16	4.13	0.03	
35	Incident classification	4.11	4	0.11	
36	Back door	4.11	3.83	0.28	
37	Denial-of-service attack	4.09	3.91	0.18	
38	information security legislation	4.09	4.04	0.05	
39	Weak passwords	4.07	4.04	0.03	
40	Risk avoidance	4.07	3.87	0.2	
41	Authorization	4.04	4.22	–0.18	

		Column			
		A	B	C	D
	Issue	Mean Information Security Professional*	Mean Business Manager	Difference (A-B)	See note†
42	Certificate authority	4.04	3.65	0.39	
43	Risk assumption	4.04	3.87	0.17	
44	Distributed denial-of-service attack	4.02	3.91	0.11	
45	Incident indicators	4.02	3.91	0.11	
46	Secure sockets layer (SSL)	4.02	4.13	–0.11	
47	Private key	4	3.65	0.35	
48	Vulnerability scanners	3.98	3.35	0.63	▲
49	Digital signature	3.96	3.87	0.09	
50	Passphrases	3.96	3.59	0.37	
51	Spyware	3.96	3.96	0	
52	Public-key infrastructure	3.96	3.65	0.31	
53	Information leaks	3.96	4.04	–0.08	
54	Public key	3.93	3.65	0.28	
55	User names	3.93	3.7	0.23	
56	Hackers	3.93	3.61	0.32	
57	Asymmetric encryption	3.93	3.48	0.45	▲
58	Crackers	3.91	3.61	0.3	
59	Repudiation	3.89	3.87	0.02	
60	Trap door	3.87	3.57	0.3	
61	ID theft	3.85	4.3	–0.45	▼
62	Monitoring traffic	3.85	3.35	0.5	▲
63	Modification of message contents	3.85	3.35	0.5	▲
64	Theft	3.83	4.04	–0.21	
65	Sniffers	3.8	3.48	0.32	
66	Sabotage	3.8	3.7	0.1	
67	Phishing attack	3.78	3.83	–0.05	
68	Smart ID cards	3.78	3.74	0.04	
69	Virus hoax	3.78	3.48	0.3	
70	Downstream liability	3.78	3.61	0.17	
71	Masquerade	3.76	3.3	0.46	▲
72	Scripts	3.76	3.04	0.72	▲
73	Password crack	3.76	3.65	0.11	
74	Rogue access points	3.74	3.48	0.26	
75	Hot site	3.74	3.96	–0.22	
76	Buffer overflow	3.74	3.26	0.48	▲
77	First-function authentication	3.74	3.39	0.35	
78	One-time passwords	3.74	3.43	0.31	
79	Monitoring transmissions	3.73	3.22	0.51	▲
80	Eavesdropping	3.73	3.04	0.69	▲
81	Disclosure threats	3.72	3.83	–0.11	
82	Technology used to locate lost/stolen laptops	3.71	3.35	0.36	
83	Pharming attack	3.7	3.7	0	
84	Zombie	3.7	3.35	0.35	
85	Risk transference	3.7	3.78	–0.08	
86	Brute force attack	3.67	3.43	0.24	

		Column			
		A	B	C	D
	Issue	Mean Information Security Professional*	Mean Business Manager	Difference (A-B)	See note†
87	Social engineering	3.67	3.83	–0.16	
88	Second-function authentication	3.67	3.35	0.32	
89	IP spoofing	3.65	3.52	0.13	
90	Port scanning	3.63	3.09	0.54	▲
91	Man-in-the-middle	3.63	3.48	0.15	
92	Dictionary attack	3.63	3.35	0.28	
93	Software errors (bugs)	3.62	3.36	0.26	
94	Session hijacking	3.61	3.39	0.22	
95	Mail bombing	3.61	3.52	0.09	
96	Mail bombs	3.61	3.39	0.22	
97	Pretty good privacy (PGP)	3.6	3.09	0.51	▲
98	Spam	3.59	3.74	–0.15	
99	Information extortion	3.59	3.22	0.37	
100	Botnet	3.57	3.04	0.53	▲
101	Script kiddies	3.57	3.09	0.48	▲
102	Bot	3.54	3.09	0.45	▲
103	Tokens	3.54	3.57	–0.03	
104	Logic bombs	3.54	3.13	0.41	▲
105	Relationship between information security and employee productivity	3.54	3.96	–0.42	▼
106	Cyberterrorism	3.5	3.52	–0.02	
107	Adware	3.49	3.61	–0.12	
108	Proximity card reader	3.48	3.41	0.07	
109	Secure electronic transaction (SET)	3.48	3.39	0.09	
110	Replay	3.46	3.04	0.42	▲
111	Competitive intelligence	3.46	3.7	–0.24	
112	Biometrics	3.46	3.22	0.24	
113	Software piracy	3.44	3.48	–0.04	
114	Warm site	3.41	3.74	–0.33	
115	Browsing	3.41	2.83	0.58	▲
116	Cyberactivism	3.41	3.35	0.06	
117	Fingerprints	3.37	3.17	0.2	
118	Trap and trace	3.37	3.04	0.33	
119	Dumpster diving	3.33	2.74	0.59	▲
120	Cold site	3.3	3.52	–0.22	
121	Shoulder surfing	3.3	3.13	0.17	
122	Wire tapping	3.27	2.82	0.45	▲
123	Industrial espionage	3.26	3.13	0.13	
124	Iris scans	3.24	2.65	0.59	▲
125	Vandalism	3.22	3.35	–0.13	
126	Retinal scans	3.2	2.68	0.52	▲
127	Evil twins	3.17	2.74	0.43	▲
128	War driving	3.17	3	0.17	
129	Tailgating	3.17	3.13	0.04	

		Column			
		A	B	C	D
	Issue	Mean Information Security Professional*	Mean Business Manager	Difference (A-B)	See note†
130	Dumb ID cards	3.16	3.19	–0.03	
131	Footprinting	3.15	2.7	0.45	▲
132	Between the lines attack	3.13	2.65	0.48	▲
133	Back hack	3.11	2.7	0.41	▲
134	Fingerprinting	3.11	2.78	0.33	
135	War chalking	3.02	2.78	0.24	
136	TEMPEST attack	3	2.43	0.57	▲
137	Signature recognition	2.96	2.61	0.35	
138	Honeypots	2.93	2.78	0.15	
139	Honeynets	2.91	2.74	0.17	
140	Steganography	2.89	2.3	0.59	▲
141	Radio frequency jamming	2.89	2.48	0.41	▲
142	Voice recognition	2.74	2.48	0.26	
	Mean	3.77	3.57	0.20	
				Total	▲ = 35
				Total	▼ = 2

* Five-point scale, 5 = Very Important issue, 1 = very unimportant issue.

† ▲ = Issue rated at least .40 higher by Information Security Professionals than Business Managers.
▼ = Issue rated at least –.40 lower by Information Security Professionals than Business Managers.
.40 is twice the mean of column C.

BIOGRAPHIES

R. Kelly Rainer, Jr., Ph.D is George Phillips Privett Professor of Management Information Systems at Auburn University, Auburn, Alabama. He received his Ph.D from the University of Georgia in 1989.

Thomas E. Marshall, Ph.D is Associate Professor of Management Information Systems at Auburn University, Auburn, Alabama. His research interests include various aspects of information security and database technology.

Kenneth J. Knapp, Ph.D is Assistant Professor of Management Information Systems at the Air Force Academy, Colorado Springs, Colorado.

Gina H. Montgomery is a Ph.D student in Management Information Systems at Auburn University, Auburn, Alabama.