CERIAS Tech Report 2001-101
A Profile of Information Security Training Needs on University Campuses
by Melissa Dark
Center for Education and Research
Information Assurance and Security
Purdue University, West Lafayette, IN 47907-2086

Information Security Training
Needs Assessment Study

Dr. Melissa Dark
CERIAS
Assistant Professor
Continuing Education Director

Executive Summary

Information security is considered to be a prevalent and growing concern in many organizations. According to some, "U.S. colleges and universities are ranked among the poorest protected systems because tightening security often means restricting access" (Information Security Magazine, 2000). In July, 2000 a needs assessment study was conducted to determine the information security training needs for professional staff on university campuses. A convenience sample was drawn from a sampling frame of professional staff at Purdue University. The survey consisted of 7 categories as follows: 1) Introduction to Information and Network Security Securing, 2) TCP/IP Networks, 3) Internet/Intranet Security, 4) Certificate Authority and PKI for Information Protection, 5) Performing a Security Forensics Review, 6) Application Specific Security Issues, and 7) Surveillance and Monitoring. Each category included 2-7 more specific topics for a total of 36 closed-ended items on the instrument. Respondents were asked to rate the importance of the topic to them in their job, as well as the perceived need for additional training/education on the topic. Data were analyzed using descriptive statistics and frequency counts. Major findings include:

Majority of respondents report the following topics as most important and also most needed:

- ✓ OS Security
- ✓ Fundamental Responsibilities in Information Security
- ✓ Fundamental Definitions in Information Security
- ✓ Organizing Your Network Security Program
- ✓ Operating Systems
- ✓ Web and Intranet Security
- ✓ Network Operating Systems
- ✓ Network Vulnerability and Auditing Tools
- ✓ TCP/IP Network Infrastructure

A smaller subset of respondents report the following topics as very important and needed:

- ✓ Identifying, Collecting, Processing, and Preserving Computer Evidence
- ✓ Detecting Computer Crime
- ✓ Investigating Computer Crime
- ✓ Preventing Computer Crime

Overview of Information Security Trends

Organizations are becoming increasingly reliant upon information technology in all aspects of the business enterprise. Many organizations, including colleges and universities, are counting on increased connectivity, availability of systems, and open environments for increased productivity, flexibility, and growth. However, computer systems are interdependent entities; this interdependence brings new security challenges, vulnerabilities, accidents, criminal behavior, and malicious activities.

The rapid expansions in the U.S. Information Technology sector has resulted in a corresponding increase in demand for information technology specialists in the national workforce, especially for specialists with technical skills in information/computer assurance and security. According to Vic Maconachy (2000) from the National Security Agency, many security tasks are not being adequately performed due to lack of personnel, training and tools. The pervasive nature of the problem is evidenced by several recent reports (U.S. Department of Commerce, Office of Technology Policy, 1999; Presidential Decision Directive 63, 1998; The White House, 2000; Critical Infrastructure Assurance Office, 2000), as well as by hiring projections issued by occupational analysts (Information Security, 2001).

Among the many different organizations faced with information security challenges, colleges and universities are especially vulnerable for various reasons. First, these institutions are not able to compete with industry on the wage scale. According to Atallah (2001), the average industry salary for information security skills is approximately 70% higher than the salary at academic institutions. Second, academic institutions are especially vulnerable to security breaches because their mindset and philosophy is one of openness and knowledge sharing in comparison to the proprietary mindset of business and industry. Third, academic institutions are especially attractive systems for hackers because they are comprised of relatively sophisticated, state of the art technology. The difficulty competing for a skilled workforce, the mindset of academic institutions, and the attractiveness of such systems to hackers create a unique security challenge for universities and colleges.

Needs Assessment Study

If colleges and universities are to be prepared to address this issue through the development of a training/educational program, it is necessary to determine the instructional needs. Needs assessments are conducted to determine if there is a need for instruction to be developed. In July, 2000 a needs assessment study was conducted to determine instructional needs of technical professional staff at colleges and universities.

Methods and Procedures

A convenience sample was drawn from a sampling frame of professional staff at Purdue University. An invitation to participate in the study was sent to 250 technical staff at Purdue University via email. The invitation included a hyperlink to the online survey. A copy of the survey can be found in Appendix A. The survey had seven main categories and each main

category had between 2-7 subcategories. Respondents rated the subcategories according to 1) the importance of the topic to them in their job, and 2) the need for professional development on the topic. Topics that are important to staff in their jobs might not necessarily require additional professional development. So, by asking respondents to rate both importance and need, we can be sure to provide professional development in topics that are both important and needed. The response rate was N = 71, which was a little over 28%.

Results of the needs assessment survey are attached in the appendices. Appendix B shows the importance results and appendix C has the needs results. Within each appendix, there are four tables of data presenting responses regarding the importance of various topics and four tables of data presenting the responses regarding the need for professional development on the various topics. The first table is sorted in descending order by VALUE POINTS. Value points were calculated by multiplying the N * Mean (for example n = 71 * 4.26 = 302.46). Value points reflect topics that were important/needed by the largest amount of people. The second table is sorted by Mean.

There is a shift in rank order from the important topics to needed topics. This is primarily due to certain topics being very important to a subset of respondents. The third table is sorted by frequency count; specifically the primary sort is in descending order by the number of respondents who rated the item strongly agree, with a secondary sort in descending order by the number of respondents who rated the item agree. Finally, the last table is sorted by N.

Conclusion

CERIAS has used this information to plan a series of training workshops for university technical staff. The value of this information for others most likely lies in: 1) understanding the process for gathering data about training needs, and/or 2) using the data to make inferences about Information Security training needs on your college or university campus.

Appendix A

Information Assurance and Security Professional Development Needs Assessment

The purpose of this survey is to determine the continuing education needs of information technology professionals in the areas of information assurance and security. This survey includes the following six categories:

1. Introduction to Information and Network Security
2. Securing TCP/IP Networks
3. Internet/Intranet Security
4. Certificate Authority and PKI for Information Protection
5. Performing a Security Forensics Review
6. Application Specific Security Issues

Each category has 2-7 topics listed. Please indicate the **Importance** of this topic to you in your job and the **Need** you have for additional education on this topic. If you have no knowledge of the topic, leave it blank.

Please indicate your current job position by checking all that apply in columns one and two	
Database	User
System	Administrator
Program	Manager
Network	Officer
Web	Engineer
Security	

1 = Not at all 2 = Very little 3 = Somewhat 4 = Fairly 5 = Extremely

Introduction to Information and Network Security	**Importance**	**Need**
Fundamental Definitions in Information Security	1 2 3 4 5	1 2 3 4 5
• Trust management: software vendors, software quality, colleagues, keys, etc. • Risk Analysis: identifying threats, types of threats, and tools/techniques for examining your computing environment's security • Commercial and Freeware Information Security: supplemental access control, authentication, audit and intrusion detection tools • Contingency Planning: business impact and cost/benefit analysis, formulating and testing your plan, software products • Detecting Computer Crime: recognizing computer crime, gathering and protecting evidence • Legislation and Standards: privacy protection laws, encryption export controversy, anti-hacker legislation, emerging international standards, Common criteria ISO/IEC 15408 and individual protection profiles		
Fundamental Responsibilities in Information Security	1 2 3 4 5	1 2 3 4 5
• Information Security Concepts: confidentiality, integrity, availability, accountability and audit ability • Infosec Policy: examining your business environment, examining your computing environment, creating appropriate policy. • Common Computer Vulnerabilities: stand-alone systems, Intranets, the Internet and Web, e-mail, fax and phone • Threats from Malicious Software: prevention, detection and elimination of viruses, worms, email bombs, etc. • Information Security and Training: benefits of awareness training, training methods and gaining management support		
Organizing your Network Security Program	1 2 3 4 5	1 2 3 4 5
• CERT, CIAC and other network security resources • Developing a network security strategy • Risk assessment techniques • Applying security tools • Physical security consideration		

	Importance					Need				
OS Security	1	2	3	4	5	1	2	3	4	5
• Server threats, vulnerabilities, and control issues • NOS Platform specific issues • Server security design requirements • Add-on products: password management, inactivity timeouts, privileged user controls, security audit tools, web server security threats and countermeasures • Workstation threats, vulnerabilities and control challenges • Tools and techniques for desktop and portable workstation system: access control, anti-theft, encryption, anti-virus, browser enhancements, desktop security suites • Web browser security threats and countermeasures: Java, ActiveX, Javascript, Trojan Horses • Methods for auditing security										
Perimeter Security	1	2	3	4	5	1	2	3	4	5
• Internet work security strategies • Remote access security • Warning banners • Network firewalls and proxy servers • Intrusion detection systems										
Authentication and Encryption	1	2	3	4	5	1	2	3	4	5
• Network users authentication: tokens, smart cards, biometrics, one-time passwords • Single sign-on alternatives: trusted hosts, trusted domains, Scripting, Kerberos, DCE • Cryptography and PKI • Virtual private networks										
Network Vulnerability and Auditing Tools/Techniques	1	2	3	4	5	1	2	3	4	5
• Network discovery tools and port scanners • Network security sweeps • Locating unauthorized modems, wargame dialers and other techniques										

Securing TCP/IP Networks	**Importance**					**Need**				
Risks of TCP/IP Networks	1	2	3	4	5	1	2	3	4	5
• Packet sniffing • Source routing • Attacks on routing protocols • IP spoofing • Sequence number prediction • Session hijacking • Back-door attacks; reverse connections and ICMP tunnels • Denial of service attacks										
TCP/IP Network Infrastructure	1	2	3	4	5	1	2	3	4	5
• Examining your connections to external networks • Using tools to discover applications running on TCP/IP • Networks • Using tools to discover hosts on TCP/IP networks • Host name and IP addresses databases • Internetworking device security concerns: hubs, bridges and routers • Securely configuring and managing network devices • IP routing protocols security concerns										
TCP/IP Application Security	1	2	3	4	5	1	2	3	4	5
• Identifying TCP/IP-based Trojan horses • Port redirectors • Netcat and other tools • TCP/IP application risks • How hackers break into applications • Authentication in TCP/IP applications • Authorization of TCP/IP sessions: privileged network services • Authentication and authorizations of distributed components • Logging application usage • Vulnerability analysis tools										
Securing Network Connections	1	2	3	4	5	1	2	3	4	5
• Network segmentation using switching hubs • Detecting packet sniffers on networks • Adding authentication and encryption in the TCP/IP layers • PPP security: PAP and CHAP authentication • L2F and L2TP protocols • IPsec • PPTP • SSH-based VPNs • Tunneling										

Firewalls	Importance					Need				
	1	2	3	4	5	1	2	3	4	5
• Firewall fundamentals • Firewall configuration guidelines • Firewall designs • Packet filters • Application level firewalls • Proxy servers • Content filtering and intrusion detection • Securing connections • Securing the host • Auditing firewalls										

Internet/Intranet	**Importance**					**Need**				
Web and Intranet Security	1	2	3	4	5	1	2	3	4	5
• Main threats and vulnerabilities of Web servers and browsers • Web and TCP/IP-based attacks • Security concerns of e-mail, FTP, news and other intranet services • Security features of common Web servers • Server privileges – active pages, scripting, protecting the document root, and user authentication • Security configuration settings for Netscape and Internet Explorer Web browsers • Security problems of active content, including Java, JavaScript, ActiveX, plug-ins • Virus protection • Security concerns of Web-enabling technologies – CGI, Server Side Includes, Active Server Pages, and cookies • Security concerns of various scripting languages – C, C++, Perl, PHP, and Unix shell scripts • Securing the host server operating system • Security implications of Web proxy servers and caching proxy servers										
Web Server and Browser Auditing	1	2	3	4	5	1	2	3	4	5
• Auditing web content • CGI and back-end scripts • Web server log files - detecting suspicious activity, log file • Filter tools, web traffic analysis tools										

Using Certificate Authority and Public Key Infrastructure to Protect Your Information	**Importance**	**Need**
Cryptography	1 2 3 4 5	1 2 3 4 5
• PKI Technology Review: directory centric, PKI centric • Definitions • Algorithms • Symmetric key encryption • Asymmetric key encryption • Public key cryptography strengths and weaknesses • Dual key pair systems • Modern asymmetric key encryption		
PKI	1 2 3 4 5	1 2 3 4 5
• Elements • Applications • PKI deployment		
Certificates and Signatures	1 2 3 4 5	1 2 3 4 5
• Encryption and privacy • Authentication • Access control • Integrity • Non-repudiation • Digital signatures: how they work and their applications • Signatures vs. certificates • PGP, how and why to use it		
Certification Authorities and Directories	1 2 3 4 5	1 2 3 4 5
• Registration and certification process • Directories • Certificate management • Certificate value • Cross certification • Key recovery • Commercial and internal authorities • SSL and secure Web transactions		

Performing a Security Forensics Review	**Importance**	**Need**
Basics	1 2 3 4 5	1 2 3 4 5
• Definitions • Types of computer crimes • Criminal motivators • Key targets for computer fraud • Techniques used to commit computer crimes		
Detecting Computer Crime	1 2 3 4 5	1 2 3 4 5
• Symptoms of computer fraud • Factors affecting detection • Detection tools for investigative forensics teams • Forensics specialties: preserving evidence, Trojan Horse programs, file slack, data-hiding techniques, text search techniques, fuzzy logic tools, identifying and detecting Internet abuse, boot process and memory programs.		
Investigating Computer Crime	1 2 3 4 5	1 2 3 4 5
• Investigation basics: objectives, organization, case management and suspects • Modifying the operating system • Password recovery and encrypted files • Identifying compressed files • Restoring erased files through cluster chaining • Operating dual function programs ties to security issues • Using automated fuzzy logic utilities to locate evidence		
Identifying, Collecting, Processing and Preserving Evidence	1 2 3 4 5	1 2 3 4 5
• Rules of evidence • Definition of evidence: private, proprietary and intrusive • Areas of evidence identification • Tools for recovering and documenting evidence		
Preventing Computer Crime	1 2 3 4 5	1 2 3 4 5
• Areas that require protection • What to protect against • Who to protect against • System vulnerabilities • Control techniques • Designing systems to prevent fraud		

Application Specific Security Issues	**Importance**	**Need**
Database Products	1 2 3 4 5	1 2 3 4 5
Operating Systems	1 2 3 4 5	1 2 3 4 5
Network Operating Systems	1 2 3 4 5	1 2 3 4 5
Application Programs	1 2 3 4 5	1 2 3 4 5
Mail Packages	1 2 3 4 5	1 2 3 4 5
Enterprise Resource Packages	1 2 3 4 5	1 2 3 4 5

Appendix B

Importance Sorted by Value Points	N	Mean	1	2	3	4	5	Value Points
OS Security	71	4.26	1	3	9	21	37	302.46
Fundamental responsibilities in information security	70	4.21		4	12	19	35	294.7
Fundamental definitions in information security	70	4	1	1	17	22	29	280
Operating Systems	65	4.26	2	3	6	19	35	276.9
Organizing your network security program	71	3.8	4	6	15	21	25	269.8
Network Operating Systems	64	4.12	2	5	8	17	32	263.68
Web and Intranet Security	65	4	2	4	13	19	27	260
Perimeter security	67	3.68	4	7	14	23	19	246.56
Risks of TCP/IP Networks	67	3.68	4	7	14	23	19	246.56
Network vulnerability and auditing tools	66	3.72	4	7	16	15	24	245.52
TCP/IP Application Security	66	3.72	4	7	16	15	24	245.52
Authentication and encryption	67	3.55	5	10	13	21	18	237.85
TCP/IP Network Infrastructure	67	3.55	5	10	13	21	18	237.85
Application Programs	64	3.7	4	5	18	16	21	236.8
Mail Packages	63	3.68	5	6	13	19	20	231.84
Database Products	64	3.59	6	8	14	14	22	229.76
Securing Network Connections	65	3.43	4	7	16	15	24	222.95
Web server and browser auditing	65	3.3	10	8	13	20	14	214.5
Certification Authorities and Directories	63	3.38	5	13	13	17	15	212.94
Firewalls	67	3.1	12	11	15	16	13	207.7
Certificates and Signatures	62	3.33	4	13	18	12	15	206.46
Clearer policies about surveillance practices	64	3.03	15	11	11	11	16	193.92
Cryptography	63	3.01	9	14	13	21	6	189.63
Enterprise Resource Packages	62	2.96	9	12	19	16	6	183.52
Surveillance to increase information security	64	2.81	15	11	18	11	9	179.84
Training about unexpected negative effects of surveillance	61	2.73	21	11	6	9	14	166.53
PKI	58	2.81	14	9	17	10	8	162.98
More control of surveillance practices	63	2.52	20	15	9	13	6	158.76
Identifying, Collecting, Processing and Preserving Evidence	35	4.34		2	3	11	19	151.9
Basics	35	4.17	1		8	9	17	145.95
Detecting Computer Crime	35	4.12		3	6	9	17	144.2
Investigating Computer Crime	35	3.91	2	3	5	11	14	136.85
Preventing Computer Crime	34	4		1	9	13	11	136
Surveillance to monitor Internet use	61	2.09	29	9	13	8	2	127.49
Surveillance to increase motivation to do better work	63	1.73	38	13	5	5	2	108.99
Surveillance to increase motivation to do more work	63	1.61	41	12	5	3	2	101.43

Importance Sorted by Mean	N	Mean	1	2	3	4	5
Identifying, Collecting, Processing and Preserving Evidence	35	4.34		2	3	11	19
OS Security	71	4.26	1	3	9	21	37
Operating Systems	65	4.26	2	3	6	19	35
Fundamental responsibilities in information security	70	4.21		4	12	19	35
Basics	35	4.17	1		8	9	17
Network Operating Systems	64	4.12	2	5	8	17	32
Detecting Computer Crime	35	4.12		3	6	9	17
Fundamental definitions in information security	70	4	1	1	17	22	29
Web and Intranet Security	65	4	2	4	13	19	27
Preventing Computer Crime	34	4		1	9	13	11
Investigating Computer Crime	35	3.91	2	3	5	11	14
Organizing your network security program	71	3.8	4	6	15	21	25
Network vulnerability and auditing tools	66	3.72	4	7	16	15	24
TCP/IP Application Security	66	3.72	4	7	16	15	24
Application Programs	64	3.7	4	5	18	16	21
Perimeter security	67	3.68	4	7	14	23	19
Risks of TCP/IP Networks	67	3.68	4	7	14	23	19
Mail Packages	63	3.68	5	6	13	19	20
Database Products	64	3.59	6	8	14	14	22
Authentication and encryption	67	3.55	5	10	13	21	18
TCP/IP Network Infrastructure	67	3.55	5	10	13	21	18
Securing Network Connections	65	3.43	4	7	16	15	24
Certification Authorities and Directories	63	3.38	5	13	13	17	15
Certificates and Signatures	62	3.33	4	13	18	12	15
Web server and browser auditing	65	3.3	10	8	13	20	14
Firewalls	67	3.1	12	11	15	16	13
Clearer policies about surveillance practices	64	3.03	15	11	11	11	16
Cryptography	63	3.01	9	14	13	21	6
Enterprise Resource Packages	62	2.96	9	12	19	16	6
Surveillance to increase information security	64	2.81	15	11	18	11	9
PKI	58	2.81	14	9	17	10	8
Training about unexpected negative effects of surveillance	61	2.73	21	11	6	9	14
More control of surveillance practices	63	2.52	20	15	9	13	6
Surveillance to monitor Internet use	61	2.09	29	9	13	8	2
Surveillance to increase motivation to do better work	63	1.73	38	13	5	5	2
Surveillance to increase motivation to do more work	63	1.61	41	12	5	3	2

Importance Sorted by Frequency	N	Mean	1	2	3	4	5
OS Security	71	4.26	1	3	9	21	37
Fundamental responsibilities in information security	70	4.21		4	12	19	35
Operating Systems	65	4.26	2	3	6	19	35
Network Operating Systems	64	4.12	2	5	8	17	32
Fundamental definitions in information security	70	4	1	1	17	22	29
Web and Intranet Security	65	4	2	4	13	19	27
Organizing your network security program	71	3.8	4	6	15	21	25

Network vulnerability and auditing tools	66	3.72	4	7	16	15	24
TCP/IP Application Security	66	3.72	4	7	16	15	24
Securing Network Connections	65	3.43	4	7	16	15	24
Database Products	64	3.59	6	8	14	14	22
Application Programs	64	3.7	4	5	18	16	21
Mail Packages	63	3.68	5	6	13	19	20
Perimeter security	67	3.68	4	7	14	23	19
Risks of TCP/IP Networks	67	3.68	4	7	14	23	19
Identifying, Collecting, Processing and Preserving Evidence	35	4.34		2	3	11	19
Authentication and encryption	67	3.55	5	10	13	21	18
TCP/IP Network Infrastructure	67	3.55	5	10	13	21	18
Basics	35	4.17	1		8	9	17
Detecting Computer Crime	35	4.12		3	6	9	17
Clearer policies about surveillance practices	64	3.03	15	11	11	11	16
Certification Authorities and Directories	63	3.38	5	13	13	17	15
Certificates and Signatures	62	3.33	4	13	18	12	15
Web server and browser auditing	65	3.3	10	8	13	20	14
Investigating Computer Crime	35	3.91	2	3	5	11	14
Training about unexpected negative effects of surveillance	61	2.73	21	11	6	9	14
Firewalls	67	3.1	12	11	15	16	13
Preventing Computer Crime	34	4		1	9	13	11
Surveillance to increase information security	64	2.81	15	11	18	11	9
PKI	58	2.81	14	9	17	10	8
Cryptography	63	3.01	9	14	13	21	6
Enterprise Resource Packages	62	2.96	9	12	19	16	6
More control of surveillance practices	63	2.52	20	15	9	13	6
Surveillance to monitor Internet use	61	2.09	29	9	13	8	2
Surveillance to increase motivation to do better work	63	1.73	38	13	5	5	2
Surveillance to increase motivation to do more work	63	1.61	41	12	5	3	2

Importance Sorted by N	**N**	**Mean**	**1**	**2**	**3**	**4**	**5**
OS Security	71	4.26	1	3	9	21	37
Organizing your network security program	71	3.8	4	6	15	21	25
Fundamental responsibilities in information security	70	4.21		4	12	19	35
Fundamental definitions in information security	70	4	1	1	17	22	29
Perimeter security	67	3.68	4	7	14	23	19
Risks of TCP/IP Networks	67	3.68	4	7	14	23	19
Authentication and encryption	67	3.55	5	10	13	21	18
TCP/IP Network Infrastructure	67	3.55	5	10	13	21	18
Firewalls	67	3.1	12	11	15	16	13
Network vulnerability and auditing tools	66	3.72	4	7	16	15	24
TCP/IP Application Security	66	3.72	4	7	16	15	24
Operating Systems	65	4.26	2	3	6	19	35
Web and Intranet Security	65	4	2	4	13	19	27
Securing Network Connections	65	3.43	4	7	16	15	24
Web server and browser auditing	65	3.3	10	8	13	20	14
Network Operating Systems	64	4.12	2	5	8	17	32

Application Programs	64	3.7	4	5	18	16	21
Database Products	64	3.59	6	8	14	14	22
Clearer policies about surveillance practices	64	3.03	15	11	11	11	16
Surveillance to increase information security	64	2.81	15	11	18	11	9
Mail Packages	63	3.68	5	6	13	19	20
Certification Authorities and Directories	63	3.38	5	13	13	17	15
Cryptography	63	3.01	9	14	13	21	6
More control of surveillance practices	63	2.52	20	15	9	13	6
Surveillance to increase motivation to do better work	63	1.73	38	13	5	5	2
Surveillance to increase motivation to do more work	63	1.61	41	12	5	3	2
Certificates and Signatures	62	3.33	4	13	18	12	15
Enterprise Resource Packages	62	2.96	9	12	19	16	6
Training about unexpected negative effects of surveillance	61	2.73	21	11	6	9	14
Surveillance to monitor Internet use	61	2.09	29	9	13	8	2
PKI	58	2.81	14	9	17	10	8
Identifying, Collecting, Processing and Preserving Evidence	35	4.34		2	3	11	19
Basics	35	4.17	1		8	9	17
Detecting Computer Crime	35	4.12		3	6	9	17
Investigating Computer Crime	35	3.91	2	3	5	11	14
Preventing Computer Crime	34	4		1	9	13	11

Appendix C

Need Sorted by Value Points	N	Mean	1	2	3	4	5	Value Points
OS Security	70	4.1	2	5	9	22	32	287
Fundamental definitions in information security	70	3.88	3	4	11	32	20	271.6
Fundamental responsibilities in information security	69	3.92	1	7	12	25	24	270.48
Organizing your network security program	71	3.74	5	3	19	22	22	265.54
Operating Systems	64	4.03	3	5	9	17	30	257.92
Web and Intranet Security	64	3.93	2	7	8	23	24	251.52
Network Operating Systems	64	3.9	4	5	11	17	27	249.6
Network vulnerability and auditing tools	66	3.66	5	9	14	13	25	241.56
TCP/IP Network Infrastructure	66	3.66	5	9	14	13	25	241.56
Perimeter security	67	3.59	4	9	15	21	18	240.53
TCP/IP Application Security	67	3.59	4	9	15	21	18	240.53
Authentication and encryption	67	3.43	5	12	14	21	15	229.81
Risks of TCP/IP Networks	67	3.43	5	12	14	21	15	229.81
Database Products	64	3.56	7	9	10	17	21	227.84
Securing Network Connections	66	3.42	5	9	14	13	25	225.72
Firewalls	66	3.39	6	8	22	14	16	223.74
Application Programs	64	3.46	6	7	18	17	16	221.44
Certificates and Signatures	64	3.4	4	10	19	18	13	217.6
Certification Authorities and Directories	64	3.39	5	9	20	16	14	216.96
Web server and browser auditing	65	3.33	8	7	17	21	12	216.45
Mail Packages	63	3.39	9	7	13	18	16	213.57
Clearer policies about surveillance practices	64	3.1	18	4	13	11	18	198.4
Cryptography	62	3.16	8	13	13	17	11	195.92
Enterprise Resource Packages	62	2.93	9	15	16	15	7	181.66
Training about unexpected negative effects of surveillance	62	2.93	19	7	10	11	15	181.66
Surveillance to increase information security	63	2.87	17	6	18	12	10	180.81
PKI	59	3	11	10	16	12	10	177
More control of surveillance practices	62	2.7	21	8	11	12	10	167.4
Identifying, Collecting, Processing and Preserving Evidence	34	4.14	2	2	2	11	17	140.76
Basics	35	3.97	1	2	5	16	11	138.95
Detecting Computer Crime	35	3.94		5	4	14	12	137.9
Surveillance to monitor Internet use	60	2.26	28	9	9	7	7	135.6
Investigating Computer Crime	35	3.82	2	2	8	11	12	133.7
Preventing Computer Crime	34	3.76	2	2	6	16	8	127.84
Surveillance to increase motivation to do better work	62	1.83	36	13	4	5	4	113.46
Surveillance to increase motivation to do more work	61	1.73	38	11	5	4	3	105.53

Need Sorted by Mean	N	Mean	1	2	3	4	5
Identifying, Collecting, Processing and Preserving Evidence	34	4.14	2	2	2	11	17
OS Security	70	4.1	2	5	9	22	32
Operating Systems	64	4.03	3	5	9	17	30
Basics	35	3.97	1	2	5	16	11

Detecting Computer Crime	35	3.94		5	4	14	12
Web and Intranet Security	64	3.93	2	7	8	23	24
Fundamental responsibilities in information security	69	3.92	1	7	12	25	24
Network Operating Systems	64	3.9	4	5	11	17	27
Fundamental definitions in information security	70	3.88	3	4	11	32	20
Investigating Computer Crime	35	3.82	2	2	8	11	12
Preventing Computer Crime	34	3.76	2	2	6	16	8
Organizing your network security program	71	3.74	5	3	19	22	22
Network vulnerability and auditing tools	66	3.66	5	9	14	13	25
TCP/IP Network Infrastructure	66	3.66	5	9	14	13	25
Perimeter security	67	3.59	4	9	15	21	18
TCP/IP Application Security	67	3.59	4	9	15	21	18
Database Products	64	3.56	7	9	10	17	21
Application Programs	64	3.46	6	7	18	17	16
Authentication and encryption	67	3.43	5	12	14	21	15
Risks of TCP/IP Networks	67	3.43	5	12	14	21	15
Securing Network Connections	66	3.42	5	9	14	13	25
Certificates and Signatures	64	3.4	4	10	19	18	13
Firewalls	66	3.39	6	8	22	14	16
Certification Authorities and Directories	64	3.39	5	9	20	16	14
Mail Packages	63	3.39	9	7	13	18	16
Web server and browser auditing	65	3.33	8	7	17	21	12
Cryptography	62	3.16	8	13	13	17	11
Clearer policies about surveillance practices	64	3.1	18	4	13	11	18
PKI	59	3	11	10	16	12	10
Enterprise Resource Packages	62	2.93	9	15	16	15	7
Training about unexpected negative effects of surveillance	62	2.93	19	7	10	11	15
Surveillance to increase information security	63	2.87	17	6	18	12	10
More control of surveillance practices	62	2.7	21	8	11	12	10
Surveillance to monitor Internet use	60	2.26	28	9	9	7	7
Surveillance to increase motivation to do better work	62	1.83	36	13	4	5	4
Surveillance to increase motivation to do more work	61	1.73	38	11	5	4	3

Need Sorted by Frequency	**N**	**Mean**	**1**	**2**	**3**	**4**	**5**
OS Security	70	4.1	2	5	9	22	32
Operating Systems	64	4.03	3	5	9	17	30
Network Operating Systems	64	3.9	4	5	11	17	27
Network vulnerability and auditing tools	66	3.66	5	9	14	13	25
TCP/IP Network Infrastructure	66	3.66	5	9	14	13	25
Securing Network Connections	66	3.42	5	9	14	13	25
Fundamental responsibilities in information security	69	3.92	1	7	12	25	24
Web and Intranet Security	64	3.93	2	7	8	23	24
Organizing your network security program	71	3.74	5	3	19	22	22
Database Products	64	3.56	7	9	10	17	21
Fundamental definitions in information security	70	3.88	3	4	11	32	20
Perimeter security	67	3.59	4	9	15	21	18
TCP/IP Application Security	67	3.59	4	9	15	21	18

Clearer policies about surveillance practices	64	3.1	18	4	13	11	18
Identifying, Collecting, Processing and Preserving Evidence	34	4.14	2	2	2	11	17
Mail Packages	63	3.39	9	7	13	18	16
Application Programs	64	3.46	6	7	18	17	16
Firewalls	66	3.39	6	8	22	14	16
Authentication and encryption	67	3.43	5	12	14	21	15
Risks of TCP/IP Networks	67	3.43	5	12	14	21	15
Training about unexpected negative effects of surveillance	62	2.93	19	7	10	11	15
Certification Authorities and Directories	64	3.39	5	9	20	16	14
Certificates and Signatures	64	3.4	4	10	19	18	13
Web server and browser auditing	65	3.33	8	7	17	21	12
Detecting Computer Crime	35	3.94		5	4	14	12
Investigating Computer Crime	35	3.82	2	2	8	11	12
Cryptography	62	3.16	8	13	13	17	11
Basics	35	3.97	1	2	5	16	11
PKI	59	3	11	10	16	12	10
Surveillance to increase information security	63	2.87	17	6	18	12	10
More control of surveillance practices	62	2.7	21	8	11	12	10
Preventing Computer Crime	34	3.76	2	2	6	16	8
Enterprise Resource Packages	62	2.93	9	15	16	15	7
Surveillance to monitor Internet use	60	2.26	28	9	9	7	7
Surveillance to increase motivation to do better work	62	1.83	36	13	4	5	4
Surveillance to increase motivation to do more work	61	1.73	38	11	5	4	3

Need Sorted by N	**N**	**Mean**	**1**	**2**	**3**	**4**	**5**
Organizing your network security program	71	3.74	5	3	19	22	22
OS Security	70	4.1	2	5	9	22	32
Fundamental definitions in information security	70	3.88	3	4	11	32	20
Fundamental responsibilities in information security	69	3.92	1	7	12	25	24
Perimeter security	67	3.59	4	9	15	21	18
TCP/IP Application Security	67	3.59	4	9	15	21	18
Authentication and encryption	67	3.43	5	12	14	21	15
Risks of TCP/IP Networks	67	3.43	5	12	14	21	15
Network vulnerability and auditing tools	66	3.66	5	9	14	13	25
TCP/IP Network Infrastructure	66	3.66	5	9	14	13	25
Securing Network Connections	66	3.42	5	9	14	13	25
Firewalls	66	3.39	6	8	22	14	16
Web server and browser auditing	65	3.33	8	7	17	21	12
Operating Systems	64	4.03	3	5	9	17	30
Web and Intranet Security	64	3.93	2	7	8	23	24
Network Operating Systems	64	3.9	4	5	11	17	27
Database Products	64	3.56	7	9	10	17	21
Application Programs	64	3.46	6	7	18	17	16
Certificates and Signatures	64	3.4	4	10	19	18	13
Certification Authorities and Directories	64	3.39	5	9	20	16	14
Clearer policies about surveillance practices	64	3.1	18	4	13	11	18

Mail Packages	63	3.39	9	7	13	18	16
Surveillance to increase information security	63	2.87	17	6	18	12	10
Cryptography	62	3.16	8	13	13	17	11
Enterprise Resource Packages	62	2.93	9	15	16	15	7
Training about unexpected negative effects of surveillance	62	2.93	19	7	10	11	15
More control of surveillance practices	62	2.7	21	8	11	12	10
Surveillance to increase motivation to do better work	62	1.83	36	13	4	5	4
Surveillance to increase motivation to do more work	61	1.73	38	11	5	4	3
Surveillance to monitor Internet use	60	2.26	28	9	9	7	7
PKI	59	3	11	10	16	12	10
Basics	35	3.97	1	2	5	16	11
Detecting Computer Crime	35	3.94		5	4	14	12
Investigating Computer Crime	35	3.82	2	2	8	11	12
Identifying, Collecting, Processing and Preserving Evidence	34	4.14	2	2	2	11	17
Preventing Computer Crime	34	3.76	2	2	6	16	8