

IT Security in Higher Education, 2006 Survey Questionnaire

Thank you for your participation in the EDUCAUSE Center for Applied Research (ECAR) study on IT security in higher education. The study covers the security of networks and computing systems, including data, application, service, and operating systems. This Web-based survey is a critical component of the study. Our testing suggests that it will require approximately 35 to 45 minutes to complete. If you wish to print a copy of the survey before completing it online, a .pdf version is available from the header of the online survey and at http://www.educause.edu/ir/library/pdf/ecar_so/ers/si/esi05g.pdf.

Our survey software now has some features that address requests from our constituency:

- **Printing.** *To print a blank copy of the survey before completing it*, click “Printable version of this survey” in the header. *To print your responses after completing the survey* (recommended), select the “Review” button at the end of the survey.
- **Saving partially completed surveys.** The survey need not be completed at a single sitting. To save and return to a partially completed survey, set a Favorite (Bookmark) for the survey and then click the SAVE button. If cookies are enabled, when you return to the survey you will be taken to the place you left off.
- **Reviewing, revising, and saving responses.** You may review your answers before clicking the “Finish” button to submit your response. Click the “Review” button to review, print, and save responses.

Please complete this survey by Tuesday, November 29, 2005. As thanks for your time and valuable input, each participant is entitled to receive a summary of key findings from the study. In addition, three survey respondents will be selected at random to receive a complimentary copy of the final report or, for ECAR subscribers, one complimentary admission to an ECAR Research Symposium.

We appreciate your time and participation. If you have any questions or concerns, please e-mail ecar@educause.edu.

Click the Next button to begin the survey. Once again, thank you for your input!

Section 1: About You

1.1 Survey ID (Required) _____

1.2 Your Name (Required) _____

1.3 Your Title

- | | |
|--|--|
| <input type="checkbox"/> chancellor/president/provost | <input type="checkbox"/> director of networking |
| <input type="checkbox"/> CIO (or equivalent) | <input type="checkbox"/> auditor |
| <input type="checkbox"/> vice president/vice provost (non-CIO) | <input type="checkbox"/> other IT management |
| <input type="checkbox"/> IT security officer (or equivalent) | <input type="checkbox"/> other IT non-management |
| <input type="checkbox"/> director of administrative computing | <input type="checkbox"/> other administrative management |
| <input type="checkbox"/> director of academic computing | <input type="checkbox"/> other academic management |

1.4 How many years have you been professionally involved with IT security? <Drop-down list including none at all, less than 1 year, 1-20 years (in one-year intervals), and over 20 years>

Section 2: Staffing

2.1 What is the title of the position that has been assigned day-to-day management responsibility for central IT security?

- chancellor/president/provost
- CIO (or equivalent)
- vice president/vice provost (non-CIO)
- IT security officer (or equivalent)
- director of administrative computing
- director of academic computing
- director of networking
- auditor
- other IT management
- other IT non-management
- other administrative management
- other academic management

2.2 Does the person in this position focus on IT security full time?

- No
- Yes

2.3 What is this person's salary range?

- \$150,000+
- \$125,000–\$149,999
- \$100,000–\$124,999
- \$75,000–\$99,999
- \$50,000–\$74,999
- \$30,000–\$49,999
- Under \$30,000

2.4 The person in this position reports to

- chancellor/president/provost
- CIO (or equivalent)
- vice president/vice provost (non-CIO)
- IT security officer (or equivalent)
- director of administrative computing
- director of academic computing
- director of networking
- auditor
- other IT management
- other IT non-management
- other administrative management
- other academic management

2.5 Has your institution formally designated an individual as its information security officer (ISO)? (Required)

- No (Proceed to 2.7_2.11)
- Yes (Proceed to 2.6)
- Don't know (Proceed to 2.7_2.11)

2.6 When did your institution first designate this ISO position?

- 2005
- 2004
- 2003
- 2002
- 2001
- 2000
- 1997–1999
- 1994–1996
- Pre-1994
- Don't know

2.7_2.11 Does the person assigned day-to-day management responsibility for central IT security have any of the following security certifications?

| | No | Yes | Don't know |
|---|----|-----|------------|
| 2.7 Certified Information Systems Auditor (CISA) | | | |
| 2.8 Certified Information Systems Security Professional (CISSP) | | | |
| 2.9 Global Information Assurance Certification (GIAC) | | | |
| 2.10 Certified Information Security Manager (CISM) | | | |
| 2.11 Other security certifications | | | |

Section 4: Current Environment

4.1 Is IT security an integral part of either your campus or IT strategic plan?

- Do not have either a campus or IT strategic plan
- Not a part of our campus or IT strategic plan
- Is a part of our campus or IT strategic plan
- Don't know

4.2 At what stage is your institution's IT security plan?

- Comprehensive plan in place
- Partial plan in place (or some units have plan)
- Neither a comprehensive nor partial plan in place
- Don't know

4.3_ 4.18 Describe your institution's current IT security approaches.

| | Already implemented | Implementation in progress | Will implement within 12 months | Not planning to implement within 12 months | Don't know |
|---|---------------------|----------------------------|---------------------------------|--|------------|
| 4.3 Network firewalls (perimeter) | | | | | |
| 4.4 Network firewalls (interior) | | | | | |
| 4.5 Application layer firewalls (e.g., Web server firewall) | | | | | |
| 4.6 Enterprise directory | | | | | |
| 4.7 Electronic signature | | | | | |
| 4.8 Shibboleth | | | | | |
| 4.9 Encryption—transmission | | | | | |
| 4.10 Encryption—data storage | | | | | |
| 4.11 Centralized data backup system | | | | | |
| 4.12 Virtual private network (VPN) for remote access | | | | | |
| 4.13 Security standards for application or system development | | | | | |
| 4.14 Intrusion detection | | | | | |
| 4.15 Intrusion prevention | | | | | |
| 4.16 Active filtering | | | | | |
| 4.17 Security event management (centralization of logging, collection, and monitoring of various IT events) | | | | | |
| 4.18 Digital certificates | | | | | |

4.19_4.29 What wireless security protections has your institution implemented?

| | Already implemented | Implementation in progress | Will implement within 12 months | Not planning to implement within 12 months | Don't know |
|--|---------------------|----------------------------|---------------------------------|--|------------|
| 4.19 40-bit Wired Equivalent Privacy (WEP) | | | | | |
| 4.20 128-bit Wired Equivalent Privacy (WEP) | | | | | |
| 4.21 Extensible Authentication Protocol (EAP) | | | | | |
| 4.22 Internet Protocol Virtual Private Network (IP VPN) | | | | | |
| 4.23 Firewall | | | | | |
| 4.24 Kerberos | | | | | |
| 4.25 Remote authentication dial-in user service (RADIUS) | | | | | |
| 4.26 Advanced Encryption Standard (AES) | | | | | |
| 4.27 Wireless-vendor-supplied proprietary solution | | | | | |
| 4.28 Registration of MAC | | | | | |
| 4.29 Other | | | | | |

Section 5: Awareness and Training

5.1_5.4 Please give us your opinion about the following statements:

| | Strongly disagree | Disagree | Neutral | Agree | Strongly agree | Don't know |
|---|-------------------|----------|---------|-------|----------------|------------|
| 5.1 IT security is one of the three top IT issues confronting my institution today. | | | | | | |
| 5.2 IT security practices are woven into the fabric of my institution's business operations. | | | | | | |
| 5.3 IT security is now a part of our institutional employee culture. | | | | | | |
| 5.4 My institution communicates IT security awareness issues to its faculty, students, and staff regularly. | | | | | | |

5.5_5.7 What type of formal IT security awareness programs does your institution have?

| | Mandatory | Voluntary | No awareness program |
|------------------|-----------|-----------|----------------------|
| 5.5 For students | | | |
| 5.6 For faculty | | | |
| 5.7 For staff | | | |

5.8_5.10 My institution's IT security awareness programs have been effective for our

| | Strongly disagree | Disagree | Neutral | Agree | Strongly agree | Don't know |
|--------------|-------------------|----------|---------|-------|----------------|------------|
| 5.8 Students | | | | | | |
| 5.9 Faculty | | | | | | |
| 5.10 Staff | | | | | | |

5.11 How often does the IT security organization (IT security officer or CIO) make a report to senior management on IT security issues?

- | | |
|---------------------------------------|-------------------------------------|
| <input type="checkbox"/> Never | <input type="checkbox"/> Often |
| <input type="checkbox"/> Seldom | <input type="checkbox"/> Very often |
| <input type="checkbox"/> Occasionally | <input type="checkbox"/> Don't know |

Section 6: Enterprise Processes

6.1 Do you require that all new enterprise systems and applications be tested for IT security?

- No
- Yes
- Don't know

6.2 How often does your institution scan for vulnerabilities?

- Continuously
- Daily
- Weekly
- Monthly
- Quarterly
- Annually
- Other regular schedule
- Not regularly
- Don't scan

6.3 6.11 To reduce IT security vulnerability at your institution, what is the implementation status of each of the following?

| | Already implemented | Implementation in progress | Will implement within 12 months | Not planning to implement within 12 months | Don't know |
|--|---------------------|----------------------------|---------------------------------|--|------------|
| 6.3 Limiting the types of protocols allowed through the firewall/router | | | | | |
| 6.4 Limiting the URLs allowed through the firewall | | | | | |
| 6.5 Restricting and eliminating access to servers and applications | | | | | |
| 6.6 Timing-out access to specific applications after an idle period | | | | | |
| 6.7 Using security devices (cards, biometric scanners, etc.) for authentication | | | | | |
| 6.8 Installing a software inventory system to watch for malicious software or program changes | | | | | |
| 6.9 Installing closed desktop systems that don't allow user configuration changes | | | | | |
| 6.10 Instituting a recovery or back-up plan in the case of disasters caused by natural events or by human acts | | | | | |
| 6.11 Isolating or quarantining computers that do not meet minimum security requirements | | | | | |

6.12 How often are passwords for key enterprise systems (HR, student, and financial) required to be changed?

- Single use
- Every 30 days
- Every 60 days
- 60–180 days
- More than 180 days
- It varies
- No requirement
- Don't know

6.13_6.22 Which of the following does your institution use for authentication?

| | Already implemented | Implementation in progress | Will implement within 12 months | Not planning to implement within 12 months | Don't know |
|--|---------------------|----------------------------|---------------------------------|--|------------|
| 6.13 Conventional password/PIN | | | | | |
| 6.14 Strong password | | | | | |
| 6.15 Kerberos | | | | | |
| 6.16 PKI certificate (software) without PIN | | | | | |
| 6.17 PKI certificate (software) with PIN | | | | | |
| 6.18 PKI hardware token without PIN | | | | | |
| 6.19 PKI hardware token with PIN | | | | | |
| 6.20 Secure ID-style one-time password | | | | | |
| 6.21 Other multi-factor authentication methods | | | | | |
| 6.22 Biometric identification | | | | | |

Section 7: Incident Handling

Definition of an incident: Any action/event that takes place through, on, or involving information technology resources, whether accidental or purposeful, that has the potential to destabilize, violate, or damage the resources, services, policies, or data of the community or of individual members of the community. Such incidents may focus on or target individuals, systems/networks, or data resources and result in a policy, education, disciplinary, or technical action.

7.1 Do you have a formal IT security incident handling process? (Required)

- No (Proceed to 7.8_7.19)
- Yes (Proceed to 7.2_7.7)
- Don't know (Proceed to 7.8_7.19)

7.2_7.7 Does the incident-handling process include the following offices?

| | No | Yes | Don't know |
|---|----|-----|------------|
| 7.2 Police/Public Safety | | | |
| 7.3 Legal Counsel | | | |
| 7.4 Communications/Public Relations | | | |
| 7.5 Student Judicial Affairs/Dean of Students | | | |
| 7.6 Campus Human Resources office | | | |
| 7.7 Data stewards | | | |

7.8_7.19 What are the top three computer security concerns for your institution? (Select up to 3)

- 7.8 Computer virus, worm, or Trojan horse
- 7.9 Denial of service
- 7.10 Electronic vandalism or sabotage
- 7.11 Embezzlement
- 7.12 Fraud
- 7.13 Theft of intellectual property (copyrights, patents, trade secrets, trademarks)
- 7.14 Unlicensed use or copying (piracy) of digital products (software, music, motion pictures, etc.)
- 7.15 Theft of personal financial information (SSN, credit/debit/ATM card, account or PIN numbers, etc.)
- 7.16 Other computer security incidents (hacking, spoofing, sniffing, pinging, scanning, spyware, etc.)
- 7.17 Misuse of computers by employees (Internet, e-mail, etc.)
- 7.18 Breaches resulting from information obtained from stolen laptops
- 7.19 Other

9.2_9.5 How do you anticipate the following categories of central IT security expenditures to change over the next 12 months?

| | Decrease more than 15% | -15% | -10% | -5% | 0% | +5% | +10% | +15% | Increase more than 15% |
|---------------------------------|------------------------|------|------|-----|----|-----|------|------|------------------------|
| 9.2 Security staffing | | | | | | | | | |
| 9.3 Security products | | | | | | | | | |
| 9.4 Security services | | | | | | | | | |
| 9.5 Security education/training | | | | | | | | | |

9.6 My institution has provided the needed resources to address the institution's IT security issues.

- | | |
|---|--------------------------------------|
| <input type="radio"/> Strongly disagree | <input type="radio"/> Agree |
| <input type="radio"/> Disagree | <input type="radio"/> Strongly agree |
| <input type="radio"/> Neutral | <input type="radio"/> Don't know |

9.7 What is the primary method your institution uses to justify central IT security expenditures?

- | | |
|---|---|
| <input type="radio"/> In reaction to major incident | <input type="radio"/> To meet federal and state compliance mandates |
| <input type="radio"/> By risk assessment | <input type="radio"/> None |
| <input type="radio"/> As a strategic investment in security | <input type="radio"/> Don't know |
| <input type="radio"/> As incident prevention | |

Section 10: Outcomes and Future Directions

10.1_10.6 Please give your opinion about the following statements.

| | Strongly disagree | Disagree | Neutral | Agree | Strongly agree | Not Applicable | Don't know |
|---|-------------------|----------|---------|-------|----------------|----------------|------------|
| 10.1 The IT security program at my institution is successful. | | | | | | | |
| 10.2 My institution today has gone beyond the federal and state government's recommendations for IT security. | | | | | | | |
| 10.3 The centrally controlled data, networks, and applications are secure. | | | | | | | |
| 10.4 The locally controlled data, networks, and applications are secure. | | | | | | | |
| 10.5 We have developed metrics to determine the effectiveness of our IT security activities. | | | | | | | |
| 10.6 I feel my institution is more secure today than it was two years ago. | | | | | | | |

10.7_10.17 What are the major barriers to IT security at your institution? (Select up to 3)

- | | |
|--|---|
| <input type="checkbox"/> 10.7 Technology issues | <input type="checkbox"/> 10.13 Academic culture that values openness and autonomy |
| <input type="checkbox"/> 10.8 Lack of resources | <input type="checkbox"/> 10.14 Culture of decentralization |
| <input type="checkbox"/> 10.9 Lack of awareness | <input type="checkbox"/> 10.15 Privacy of the individual |
| <input type="checkbox"/> 10.10 Absence of policies | <input type="checkbox"/> 10.16 Increased sophistication of threats |
| <input type="checkbox"/> 10.11 Lack of enforcement of policies | <input type="checkbox"/> 10.17 Other |
| <input type="checkbox"/> 10.12 Lack of senior management support | |

10.18_10.23 Please give us your opinion on the following statements about your institution.

| | Strongly disagree | Disagree | Neutral | Agree | Strongly agree | Don't know |
|---|-------------------|----------|---------|-------|----------------|------------|
| 10.18 Business requirements take precedence over IT security when there is a conflict. | | | | | | |
| 10.19 My institution's IT security architecture and implementation sacrifices some level of protection to ensure ease of use. | | | | | | |
| 10.20 IT security inhibits academic freedom. | | | | | | |
| 10.21 IT security compromises personal privacy. | | | | | | |
| 10.22 IT security unnecessarily limits user access to information. | | | | | | |
| 10.23 Individual behaviors have become more sensitive to security and privacy in the past two years. | | | | | | |

Section 11: Conclusion

11.1 EDUCAUSE plans to conduct telephone interviews with some institutions to probe further into IT security. Would you be willing to participate in such an interview?

- No
- Yes

11.2 If yes, what is your e-mail address? _____

11.3 If you have any other comments or insights about IT security in higher education, please share them with us. _____

11.4 We are committed to continually improving our surveys. All comments are welcome and will be considered. _____

You have reached the end of the survey. Thank you! Please submit this survey by clicking the "Finish" button now, or, if you wish to review, print, or save your responses, click "Review."

Full ECAR studies are available either through subscription or purchase at the ECAR Web site, <http://www.educause.edu/ecar/>. If you have any questions or concerns, please e-mail ecar@educause.edu.

– END SURVEY –