

IT Security in Higher Education Survey Questionnaire

Thank you for your participation in the EDUCAUSE Center for Applied Research (ECAR) study on IT Security in Higher Education. The study will cover 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. It consists of 13 parts, and our testing suggests that it will require approximately 35 to 45 minutes to complete. If you wish to preview the survey questions, visit http://survey.educause.edu/survey/it-security_preview.html.

Please complete the survey by April 23, 2003. We appreciate your time and candor. The survey does not need to be completed at a single sitting. You can save your responses and return to it at times that are convenient for you. You may also wish to consult with colleagues about answers to particular questions, or if another person on your campus is better positioned to answer this survey, please forward this e-mail to that person. If at any point you wish to exit before submitting your final answers, click the Save button and follow the directions. To return to the survey, use the bookmark or favorite you saved when you exited the survey.

As thanks for your time and valuable input, every participant will receive a summary of key findings. In addition, three survey respondents will be selected at random to receive a complimentary copy of the final report or, for ECAR subscribers, one additional complimentary admission to the second annual ECAR Research Symposium, November 19-21, 2003, at San Diego's landmark Hotel Del Coronado. Full ECAR studies are available either through subscription or purchase at <http://www.educause.edu/ecar/>. If you have any questions or concerns, please e-mail ecar@educause.edu.

For purposes of this survey, IT security covers the security of networks and computing systems, including data, application, service and operating systems.

© 2003 EDUCAUSE. Reproduction by permission only.

EDUCAUSE CENTER FOR APPLIED RESEARCH

All data and information collected by the EDUCAUSE Center for Applied Research is used strictly for the purposes of research and analysis for the benefit of ECAR subscribers and EDUCAUSE members. EDUCAUSE does not make personally or institutionally identifiable information or data available to its members, sponsors, contractors, or others.

1 General Information - Institutional Profile

1.1 Survey ID:

1.2 Your Name:

1.3 Your Title:
(Single selection)

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

1.4 How many years have you been professionally involved with IT security?
(Single selection)

- Not at all
- Less than 1 year
- 1 year
- 2 years
- 3 years
- 4 years
- 5 years
- 6 years
- 7 years
- 8 years
- 9 years
- 10 years
- Over 10 years

1.5 How many devices are connected to your institution's networks?
(Single selection)

- Under 1,000
- 1,001 - 5,000
- 5,001 - 10,000
- 10,001 - 20,000
- 20,001 - 40,000
- 40,001 - 60,000
- 60,001 - 80,000
- 80,001 - 100,000
- Over 100,000

- Not centrally tracked
- Don't know

1.6 How many total users does your institution support?
(Single selection)

- Under 1,000
- 1,001 - 5,000
- 5,001 - 10,000
- 10,001 - 20,000
- 20,001 - 40,000
- 40,001 - 60,000
- 60,001 - 80,000
- 80,001 - 100,000
- Over 100,000
- Not centrally tracked
- Don't know

1.7 Does your institution have residence halls connected to its networks?

(Single selection) Yes No All Some None Don't know

1.8 Do your institution's enterprise systems reside in an on-site data center?

(Single selection) Yes No All Some None Don't know

1.9 Does your institution provide remote network access?

(Single selection) Yes No All Some None Don't know

If you answered "Yes" to 1.9, continue with 1.10

If you answered "No" or "Don't know" to 1.9, skip to 2.1

Indicate the ways in which your institution provides remote access.

- | | | | |
|---|-----|----|------------|
| 1.10 Campus modem pool | Yes | No | Don't know |
| 1.11 Outsourced modem pool | Yes | No | Don't know |
| 1.12 Institutionally arranged discount with ISP | Yes | No | Don't know |
| 1.13 Subsidized ISP accounts | Yes | No | Don't know |

1.14 Other (please specify):

2. Staffing

2.1 What is the title of the position with day-to-day management responsibility for IT security? (Single selection)

- CIO (or equivalent)
- vice president / vice provost (Non-CIO)

- chief IT security officer (or equivalent)
- director of administrative computing
- director of academic computing
- director of networking
- other IT management
- other administrative management
- other academic management

2.2 Does the person in this position focus on IT security full time? Yes No

2.3 What is this person's salary range?
(Single selection)

- \$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 When did your institution first designate this position as responsible for managing IT security? (Single selection)

- 2003
- 2002
- 2001
- 2000
- 1997-1999
- 1994-1996
- Pre-1994
- Don't know
- No official designation

2.5 To whom does this person report?
(Single selection)

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

2.6 Does the person in this position have IT security certification?
(Single selection) Yes No Don't know

If you answered "Yes" to 2.6, continue with 2.7
If you answered "No" or "Don't know" to 2.6, skip to 2.12

Which of the following certificates has this person earned? Select all that apply.

2.7 Certified Information Systems Auditor (CISA)	Yes	No	Don't know
2.8 Certified Information Systems Security Professional (CISSP)	Yes	No	Don't know
2.9 Global Information Assurance Certification (GIAC)	Yes	No	Don't know
2.10 Security +	Yes	No	Don't know

2.11 Other (please specify):

2.12 How many full-time central IT security staff are employed by your institution?
(Single selection)

- None
- One
- Two
- Three
- Four
- Five
- Five – Ten
- More than 10
- Don't know

2.13 How many IT security staff have IT security certification?
(Single selection)

- None
- One
- Two
- Three
- Four
- Five
- Five – Ten
- More than 10
- Don't know

2.14 Within the next two years, central IT security staffing at my institution will:
(Single selection)

- Increase by more than 2 FTE staff
- Increase by 2 FTE staff
- Increase by 1 FTE staff
- Stay the same
- Decrease by 1 FTE staff
- Decrease by 2 FTE staff

- Decrease by more than 2 FTE staff
- Don't know

2.15 What is the operational staffing structure for IT security?
(Single selection)

- Single staff member
- A dedicated security operations staff
- Spread across multiple functions
- Outsourced
- Other
- Don't know
- Does not apply

3. Policy

My institution has formal policies that cover IT security issues. Choose all that apply.

- 3.1 Yes
- 3.2 We have some interim policies
- 3.3 We are implementing formal policies
- 3.4 No
- 3.5 Don't know

If you answered "Yes", "We have some interim policies", or "We are implementing formal policies" continue with 3.6

If you answered "No" or "Don't know," skip to 4.1

3.6 My institution has had formal IT security policies in place since:
(Single selection)

- 2003
- 2002
- 2001
- 2000
- 1997-1999
- 1994-1996
- Pre-1994
- Don't know
- No official designation

My institution's IT security policies cover:

- | | | | |
|---|-----|----|------------|
| 3.7 Appropriate use of institutional IT assets | Yes | No | Don't know |
| 3.8 Data security (encryption, confidentiality, privacy, integrity) | Yes | No | Don't know |
| 3.9 Enforcement of institutional security policies | Yes | No | Don't know |
| 3.10 Desktop security (viruses, etc) | Yes | No | Don't know |
| 3.11 Application development | Yes | No | Don't know |

3.12 System access control (password mgmt, privilege control, authentication, authorization, data access)	Yes	No	Don't know
3.13 Physical security of IT assets	Yes	No	Don't know
3.14 Network security	Yes	No	Don't know
3.15 Remote devices	Yes	No	Don't know
3.16 Residence halls	Yes	No	Don't know
3.17 Authority to shut off Internet access	Yes	No	Don't know

My institution has IT security policies that are:

No opinion Strongly Agree Agree Disagree Strongly Disagree Don't know

- 3.18 Clear and easy to read
- 3.19 Accessible
- 3.20 Enforced
- 3.21 Comprehensive
- 3.22 Regularly updated
- 3.23 Consistent across the institution

Please give your opinion on the following statements:

Strongly Agree Agree Neutral Disagree Strongly Disagree Don't know

3.24 The institution's CIO was very much involved in developing the institution's IT security policies.

3.25 The institution's president was very much involved in developing the institution's IT security policies.

3.26 The institution's provost was very much involved in developing the institution's IT security policies.

3.27 The institution's Board of Trustees was very much involved in developing the institution's IT security policies.

3.28 The institution's central IT organization was very much involved in developing the institution's IT security policies.

3.29 The institution's internal auditor was very much involved in developing the institution's IT security policies.

3.30 An external auditor was very much involved in developing the institution's IT security policies.

3.31 A campus/faculty task force was very much involved in developing the institution's IT security policies.

3.32 The institution's system office was very much involved in developing the institution's IT security policies.

3.33 A state agency was very much involved in developing the institution's IT security policies.

4. Current Environment

4.1 Is IT security an integral part of your strategic IT plan?
(Single selection) Yes No Don't know No strategic IT plan

4.2 At what stage is your institution's IT security planning?
(Single selection)

- Comprehensive plan in place
- Partial plan in place (some units have plan)
- Currently developing a plan
- No plan in place
- Don't know

Describe your institution's current IT security approaches:
(Single selection of status that best applies for each of 4.3 – 4.15)

Implemented In Progress Piloting Will implement within 12 months
May implement within 24 months Not Under consideration Don't know

- 4.3 Network firewalls (perimeter)
- 4.4 Network firewalls (interior)
- 4.5 Enterprise directory
- 4.6 Electronic signature
- 4.7 Shibboleth
- 4.8 Encryption
- 4.9 Centralized data backup system
- 4.10 Virtual private network (VPN) for remote access
- 4.11 Security standards for application or system development
- 4.12 Secure Sockets Layer (SSL) for secure web transactions
- 4.13 Intrusion detection
- 4.14 Intrusion prevention tools
- 4.15 Active content monitoring / filtering

4.16 Do you have wireless technologies installed on your campus?
(Single selection) Yes No Don't know

If you answered "Yes" to 4.16, continue with 4.17
If you answered "No" or "Don't know" to 4.16, skip to 5.1

What level of wireless encryption/authentication do you enforce?
(Single selection of status that best applies for each of 4.17 – 4.26)

Implemented In Progress Piloting Will implement within 12 months
May implement within 24 months Not Under consideration Don't know

- 4.17 40-bit Wired Equivalency Privacy (WEP)
- 4.18 128-bit Wired Equivalency Privacy (WEP)
- 4.19 Extensible Authentication Protocol (EAP)
- 4.20 Internet Protocol Virtual Private Network (IP VPN)
- 4.21 Firewall
- 4.22 Kerberos
- 4.23 Remote authentication dial-in user service (RADIUS)
- 4.24 Advanced encryption standard (AES)
- 4.25 Wireless vendor supplied proprietary solution
- 4.26 3rd party hardware/software solution

5. Awareness

Strongly Agree Agree Neutral Disagree Strongly Disagree 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 problems inadvertently caused by authorized users are a significant concern at my institution.

My institution has a formal IT security awareness program for its:

- | | | | | |
|--------------|--------------------|-----|----|------------|
| 5.4 Students | (Single selection) | Yes | No | Don't know |
| 5.5 Faculty | (Single selection) | Yes | No | Don't know |
| 5.6 Staff | (Single selection) | Yes | No | Don't know |

My institution's IT security awareness programs have been effective for our

Strongly Agree Agree Neutral Disagree Strongly Disagree Don't know

- 5.7 Students
- 5.8 Faculty
- 5.9 Staff

Strongly Agree Agree Neutral Disagree Strongly Disagree Don't know

- 5.10 My institution communicates IT security awareness issues to its faculty, students and staff regularly.
- 5.11 My institution communicates IT security awareness issues to its faculty, students and staff in response to specific incidents.

5.12 IT security is an important priority at this institution

Very often Often Occasionally Seldom Never Don't know

5.13 How often is IT security discussed at the president/chancellor's cabinet?

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

6. Enterprise Processes

6.1 Does your institution have a unified login or single sign on system?
(Single selection)

- Implemented
- Implementing now
- Will implement in the next two years
- Not under consideration
- Don't know

Which of the following does your institution use for authentication?
(Single selection of status that best applies for each of 6.2 – 6.11)

Implemented In Progress Piloting Will implement within 12 months
May implement within 24 months Not Under consideration Don't know

- 6.2 Multiple use passwords
- 6.3 Multi-level passwords
- 6.4 Single use passwords
- 6.5 Kerberos
- 6.6 PKI
- 6.7 Electronic signatures
- 6.8 Hard/soft tokens
- 6.9 Smart cards
- 6.10 Password/PIN combination
- 6.11 Biometric technologies

6.12 Is there an institution-wide password policy?
(Single selection) Yes No Don't know

6.13 Does your institution have a procedure for identifying users before resetting passwords, tokens or PINs?
(Single selection) Yes No Don't know

If you answered "Yes" to 6.13, continue with 6.14
If you answered "No" or "Don't know" to 6.13, skip to 6.15



6.14 Do you feel the procedure (for identifying users before resetting passwords, tokens or PINs) is effective?

(Single selection) Yes No Don't know

6.15 Do you routinely terminate access when authorized users leave the institution?

(Single selection) Yes No Don't know

If you answered "Yes" to 6.15, continue with 6.16

If you answered "No" or "Don't know" to 6.15, skip to 6.20

Does termination of access (when authorized users leave the institution) cover:

6.16 Network access (Single selection) Yes No Don't know

6.17 Remote access (Single selection) Yes No Don't know

6.18 Email access (Single selection) Yes No Don't know

6.19 Access to key enterprise systems (HR, student, financial)
(Single selection) Yes No Don't know

How often does your institution monitor the following for vulnerabilities and attempts at unauthorized access?

Daily Weekly Monthly Quarterly Annually Other Not regularly Don't monitor Don't know

6.20 Networks

6.21 Operating Systems

6.22 Enterprise Systems

6.23 Does your institution's implementation protocol require that all new enterprise systems and applications are tested for IT security?

(Single selection) Yes No Don't know

6.24 Does your institution's implementation protocol require that all new enterprise systems and applications be certified for IT security?

(Single selection) Yes No Don't know

Do you have anti-virus protection installed?

6.25 Operating systems (Single selection) Yes No Don't know

6.26 Application servers (Single selection) Yes No Don't know

6.27 Email servers (Single selection) Yes No Don't know

6.28 Other servers (Single selection) Yes No Don't know

6.29 Are all institutionally owned systems required to have anti-virus software installed in order to be connected to the network?

(Single selection) Yes No Don't know

6.30 Are all non-institutionally owned systems (faculty, student, staff) required to have anti-virus software installed on their computers in order to be connected to the network?

(Single selection) Yes No Don't know

6.31 Does your institution have a site or volume license for anti-virus software?
(Single selection) Yes No Don't know

If you answered "Yes" to 6.31, continue with 6.32
If you answered "No" or "Don't know" to 6.31, skip to 6.33

6.32 Does the license cover personally owned (faculty, student, staff) computers?
(Single selection) Yes No Don't know

6.33 How many of your critical systems and applications do you require to be patched and updated in an expeditious manner?
(Single selection) All Most Some None No requirement Don't know

How do the following statements apply at your campus regarding security-related software patches and updates?
(Single selection of status that best applies for each of 6.34 – 6.36)

Strongly Agree Agree Neutral Disagree Strongly Disagree Don't know

6.34 We require all campus owned computers connected to our network to have known security holes fixed.

6.35 We conduct regular and frequent scans to detect known security exposures in our critical systems.

6.36 We conduct regular and frequent scans to detect known security exposures in all campus owned computers connected to our network.

Which of the following is your institution considering in order to reduce its IT security vulnerability? Which of the following does your institution use for authentication?
(Single selection of status that best applies for each of 6.37 – 6.44)

Implemented In Progress Piloting Will implement within 12 months
May implement within 24 months Not Under consideration Don't know

- 6.37 Limiting the types of protocols allowed through the firewall/router
- 6.38 Limiting the URLs allowed through the firewall
- 6.39 Restricting and eliminating access to servers and applications
- 6.40 Timing out access to specific applications after an idle period
- 6.41 Using security devices (cards, biometric scanners, etc.) for personal authentication
- 6.42 Installing a directory software inventory system to watch for undesired programs or program changes
- 6.43 Installing closed desktop systems that don't allow user configuration changes
- 6.44 Instituting a recovery or back-up plan in the case of disasters caused by natural events or by human acts.

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



- Single Use
- Daily
- Weekly
- Every 30 Days
- Every 60 Days
- More than 60 Days
- It varies
- No requirement
- Don't know

7. Incident Handling

For this survey, an IT security incident is defined as any adverse event whereby some aspect of IT security could be or has been threatened: loss of data confidentiality, disruption of data or system integrity, or disruption or denial of availability.

7.1 Do you have a formal IT security incident handling procedure?
(Single selection) Yes No Don't know

If you answered "Yes" to 7.1, continue with 7.2
If you answered "No" or "Don't know" to 7.1, skip to 7.9

Does the procedure include the following offices:

7.2 Police and Security	(Single selection)	Yes	No	Don't know
7.3 Campus Legal	(Single selection)	Yes	No	Don't know
7.4 Campus Communications	(Single selection)	Yes	No	Don't know
7.5 Student Judicial Affairs	(Single selection)	Yes	No	Don't know

Does the procedure include:

7.6 Centralized mechanisms for alerting faculty/staff/students/administration
(Single selection) Yes No Don't know

7.7 Other mechanisms for alerting faculty/staff/students/administration
(Single selection) Yes No Don't know

7.8 Other (please specify):

7.9 Have you ever had a significant IT security incident that was reported in the press?
(Single selection) Yes No Don't know

If you answered "Yes" to 7.9, continue with 7.10
If you answered "No" or "Don't know" to 7.9, skip to 7.11

7.10 In what year did the first incident reported to the press occur? (Single selection)

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

7.11 How many IT security breaches at your institution have involved police intervention? (Single selection)

- None
- 1
- 2
- 3
- 4
- 5
- 6-10
- More than 10
- Don't Know

7.12 How many IT security incidents has your institution reported to law enforcement within the last 12 months? (Single selection)

- None
- 1
- 2
- 3
- 4
- 5
- 6-10
- More than 10
- Don't Know

7.13 Are IT security incidents reported regularly to senior officials of your institution? (Single selection)

- When incident happens
- Monthly
- Quarterly
- Annually
- Not regularly
- No
- Not at all

8. Risk Assessment

8.1 Has your institution undertaken a risk assessment to determine the value of your IT assets and risk to those assets?

(Single selection) Yes No Don't know

8.2 Does your institution have a risk assessment methodology for IT?

(Single selection) Yes No Don't know

Does your institution perform IT security audits/review and vulnerability assessments on a regular basis? (Select all that apply.)

8.3 Monthly

8.4 Quarterly

8.5 Annually

8.6 Don't audit

8.7 Not regularly

8.8 By departmental request

8.9 On a recharge basis

8.10 No

8.11 On what regular basis does your institution audit key enterprise systems (HR, student, financial) regularly to assess their integrity and to look for unauthorized changes? (Single selection)

- Daily
- Weekly
- Monthly
- Quarterly
- Annually
- Not regularly
- Not at all

8.12 On what regular basis does your institution audit router configurations regularly to assess their integrity and to look for unauthorized changes? (Single selection)

- Daily
- Weekly
- Monthly
- Quarterly
- Annually
- Not regularly
- Not at all

Which of the following have conducted IT security audit/reviews?

8.13 IT Staff (Single selection) Yes No Don't know

8.14 Internal Auditor (Single selection) Yes No Don't know

8.15 External Auditor (Single selection) Yes No Don't know

8.16 Vendor (Single selection) Yes No Don't know

8.17 External consultant (Single selection) Yes No Don't know

8.18 How frequently does your institution audit central user account activity to detect dormant, invalid, or misused accounts? (Single selection)

- Daily
- Weekly
- Monthly
- Quarterly
- Every semester or term
- Annually
- Not regularly
- Not at all

8.19 How frequently does your institution regularly review its access control lists? (Single selection)

- Daily
- Weekly
- Monthly
- Quarterly
- Every semester or term
- Annually
- Not regularly
- Not at all

8.20 Does the institution provide departments/units a guide or protocol to perform IT Security self-assessment? (Single selection) Yes No Don't know

8.21 Do individuals receive only enough access to do their jobs? (i.e., least privilege) (Single selection) Yes No Don't know

8.22 Have employees who have access to key enterprise systems undergone criminal background investigations? (Single selection) Yes No Don't know Sometimes

8.23 Are employees who have access to key enterprise systems bonded? (Single selection) Yes No Don't know Sometimes

8.24 Have contractors who have access to key enterprise systems undergone criminal background investigations? (Single selection) Yes No Don't know Sometimes

8.25 Are contractors who have access to key enterprise systems bonded? (Single selection) Yes No Don't know Sometimes

9. Consultants/Purchasing/External Services

9.1 Have you used outside IT security consultants or services in the past 18 months, including services from your IT security technology vendor(s)?
(Single selection) Yes No Don't know

If you answered "Yes" to 9.1, continue with 9.2
If you answered "No" or "Don't know" to 9.1, skip to 10.1

Has your institution purchased, or is it considering the purchase of the following?
(Single selection of status that best applies for each of 9.2 – 9.16)

Purchasing Considering purchasing Not under consideration Don't know

- 9.2 IT security planning services
- 9.3 IT security architecture and design services
- 9.4 Electronic security audit
- 9.5 IT security technical support services
- 9.6 Managed firewall services
- 9.7 Physical security audit (related to IT Security)
- 9.8 Help setting IT security policy
- 9.9 Managed intrusion detection services
- 9.10 Project management (for IT security projects)
- 9.11 Managed Virtual Private Network (VPN) services
- 9.12 Managed antivirus services
- 9.13 Custom engineering to address IT security
- 9.14 Managed incident response services
- 9.15 IT security end user/client training and awareness
- 9.16 IT security training for technical IT staff

Strongly Agree Agree Neutral Disagree Strongly Disagree Don't know

- 9.17 Using consultants/external services helped my institution achieve its IT security objectives.
- 9.18 My institution got the value we expected for the money spent on consulting/external services.

What did you see as the benefit of working with IT security consultants?

Strongly Agree Agree Neutral Disagree Strongly Disagree Don't know

- 9.19 Provided technical expertise unavailable internally
- 9.20 Provided product expertise unavailable internally
- 9.21 Provided project management expertise unavailable internally
- 9.22 Brought methodology or insights from previous engagements
- 9.23 Helped us meet our project timeline
- 9.24 Helped us meet our project budget
- 9.25 Allowed us to staff without hiring new FTEs
- 9.26 Helped us derive additional value or functionality from our IT security program

What aspects of working with IT security consultants caused you the most concern?

Strongly Agree Agree Neutral Disagree Strongly Disagree Don't know

- 9.27 Costs ended up higher than originally estimated
- 9.28 Personnel were not a good fit
- 9.29 Experience was overstated
- 9.30 Knowledge was not transferred to internal resources
- 9.31 Did not work well with internal resources
- 9.32 Did not understand higher education / institutional culture
- 9.33 Trained their personnel at our expense
- 9.34 Project resources were changed midstream
- 9.35 Price was not tied to achieving milestones and/or value

10. Funding

10.1 What percent of the central IT budget is dedicated to IT security?
(Single selection)

- Less than 1%
- 1-5%
- 6-10%
- 11-15%
- 16-20%
- Over 20%
- Don't know

Do you expect increases or decrease to the following categories of expenditures in the next 12 months?

Significant increase Some increase About the same Some decrease Significant decrease Don't know

- 10.2 Staffing
- 10.3 Hardware/Software/Products
- 10.4 Education/Training
- 10.5 External Services

Strongly Agree Agree Neutral Disagree Strongly Disagree Don't know

10.6 My institution has provided the needed resources to address the institution's IT security issues?

10.7 What is the primary method your institution uses to justify IT security expenditures?
(Single selection)

- In reaction to major incident
- By risk assessment
- As a strategic investment in security
- As incident prevention



- By external mandates (e.g. HIPAA)
- By IS/IT projects
- By operations (as opposed to projects)
- By governance
- Not at all
- Don't know

11. Outcomes

11.1 How would you characterize the success of your IT security programs?
(Single selection)

- Highly successful
- Fairly successful
- Neither successful nor unsuccessful
- Fairly unsuccessful
- Highly unsuccessful

Please give your opinion on the following statements:

Strongly Agree Agree Neutral Disagree Strongly Disagree Don't know

11.2 My institution today has gone beyond the federal and state government's recommendations for IT security.

11.3 I feel that the data, networks, and applications that are my responsibility are secure.

11.4 We have developed metrics to determine the effectiveness of our IT security activities.

11.5 I feel my institution is more secure today than it was 2 years ago.

12. Issues/Future Directions

Evaluate the major barriers to IT security at your institution. Please select up to 3 of the following:

- 12.1 Technology
- 12.2 Resources
- 12.3 Awareness
- 12.4 Absence of policies
- 12.5 Senior management support
- 12.6 Enforcement of policies
- 12.7 Freedom of speech
- 12.8 Academic freedom
- 12.9 Culture of decentralization
- 12.10 Privacy of the individual

12.11 Time lag between deployment of technology and the development of legal and policy framework for its appropriate use

12.12 Vendor hardware/software

12.13 Other

12.14 If you selected "Other," please specify:

We would like your opinion of the following statements about your institution:

Strongly Agree Agree Neutral Disagree Strongly Disagree Don't know

12.15 Business requirements take precedence over IT security when there is a conflict.

12.16 Centralization of networks and network management is the only way we will be able to comply with federal and state requirements concerning IT security.

12.17 Standardization of networks and network management is the only way we will be able to comply with federal and state requirements concerning IT security.

12.18 My institution's IT security architecture and implementation sacrifices some level of protection to ensure ease of use.

12.19 Please describe the status of your organization's compliance with HIPAA's Privacy deadline: (Single selection)

- We will be compliant as of April 14, 2003 deadline
- We aren't required to be compliant as of the April 14, 2003 deadline
- We aren't required to be compliant
- Don't know

12.20 Please describe the status of your organization's compliance with HIPAA's Security deadline: (Single selection)

- Compliant – currently meet or exceed requirements
- We will be compliant as of April 21, 2005 deadline
- We aren't required to be compliant as of April 21, 2005 deadline
- We aren't required to be compliant
- Don't know

13. Conclusion

13.1 May we contact you by phone to obtain further insights or clarifications on your responses? Yes No

13.2 If yes, what is your phone number?

13.3 Do you wish to receive a copy of the key findings from this survey? Yes No



13.4 If you have any other comments or insights about IT security in higher education, please feel free to share them with us, below.

13.5 My institution's IT security policies are available via the Web at the following URL(s):