**INFORMATION SECURITY SPENDING AND STAFFING**

- 3% Central IT spending on information security (including identity and access management) as a percentage of total central IT spending
- 0.2 Central IT information security FTEs per 1,000 institutional FTEs

**INFORMATION SECURITY LEADERSHIP**

- 34% Percentage of institutions with a dedicated person whose primary responsibility is information security

**Most common titles for a full-time information security leader:**
- Chief information security officer (37%)
- Information security officer (23%)
- Director of information security (10%)

**Most common reporting lines for a full-time information security leader:**
- Highest-ranking IT administrator/officer (e.g., CIO) in central IT (76%)
- First-line director in central IT (16%)
- Chief financial officer (4%)

**Top information security leader responsibilities:**
- Information security policies (99%)
- Awareness and training (97%)
- Incident management (97%)

- 83% Information security leaders who are male
- 84% Information security leaders who are white/Caucasian
- 49 Median age of information security leaders

**INFORMATION SECURITY RESPONSIBILITY AND PRACTICES**

**Areas for which central IT most commonly has primary responsibility:**
- Network security (92%)
- Identity management (86%)
- Security software procurement (84%)
- Monitoring (84%)

**Areas for which other administrative or academic units most commonly have primary responsibility:**
- Records retention (36%)
- Cyber liability insurance purchases (29%)
- E-discovery (5%)

**Areas most commonly outsourced:**
- Forensic analysis (9%)
- E-discovery (2%)
- Cyber liability insurance purchases (1%)
- Monitoring (1%)

**Most commonly achieved information security practices:**
- Acceptable use policy defining the misuse of institutional IT resources and data (91%)
- Data backup process consistent with availability requirements (78%)
- Access control procedures to authorize/revoke access rights to information systems (75%)

**INFORMATION SECURITY RISK ASSESSMENTS AND FRAMEWORKS**

- 75% Institutions that have conducted any sort of information security risk assessment
- 21% Institutions that have conducted an information security risk assessment of cloud-service or third-party providers

**Main reasons for performing information security risk assessments:**
- Planning/prioritizing institutional security work (68%)
- Contractual requirement (e.g., PCI) (41%)
- Regulatory requirement (e.g., HIPAA, GLBA) (38%)

**Most commonly deployed standards or frameworks:**
- ISO 27001 (22%)
- NIST 800-53/FISMA (20%)
- CIS Critical Security Controls (18%)
IDENTITY AND ACCESS MANAGEMENT PRACTICES

64% Institutions that require authentication for wired connections from public workstations
92% Institutions that require authentication for wireless access for institutional users
57% Institutions that require authentication for wireless access for guests
1% Institutions using biometric authentication for students, faculty, and staff

Top uses of multifactor authentication:
- Business-critical applications (e.g., financial or HR systems) (32%)
- E-mail (10%)
- IT administrative access (8%)
- Remote access (8%)

60% Institutions that are members of an authentication federation (e.g., InCommon)

TECHNOLOGY DEPLOYMENT

Most commonly deployed information security technologies:
- Malware protection (94%)
- Secure remote access (93%)
- Secure wireless access (91%)

Top trends influencing the adoption of emerging security technologies:
- Continued complexity of security threats
- Increasing complexity of technology, architecture, and data
- Compliance environment
- Campus safety

TRAINING AND AWARENESS

53% Institutions with information security training and awareness budgets of less than $5,000
5% Information security training and awareness professionals who spend 90–100% of their time on training and awareness activities
11% Information security training and awareness professionals who have developed a detailed yearly plan for training and awareness activities, topics, and communications
53% Information security training and awareness professionals who report sufficient executive support for information security training and awareness activities

USER PERCEPTIONS OF INFORMATION SECURITY

33% Students who own four or more Internet-capable devices
66% Students who typically connect two or more devices to the campus network simultaneously
36% Students who are concerned that technology advances may increasingly invade their privacy (excluding "Don’t know" responses)

ABOUT THE DATA IN THIS ALMANAC

EDUCAUSE Core Data Service
In the summer of 2016, 3,500 institutions were invited to contribute data to the EDUCAUSE Core Data Service (CDS). This almanac summarizes data from the 607 institutions that responded to the optional information security module. Some publicly available data from the Integrated Postsecondary Education Data System (IPEDS, nces.ed.gov/ipeds/) are used in calculating metrics. Reported statistics are either an estimated proportion of the population or an estimated median (rather than a mean). CDS participants can access data at www.educause.edu/coredata.

EDUCAUSE Center for Research and Analysis
IT Workforce Research
This research focuses on the evolving IT workforce needed to support contemporary models of IT service delivery. It also analyzes the skills needed to prepare for and fulfill functional roles such as that of the CISO. Read the reports at https://library.educause.edu/resources/2016/3/the-it-workforce-in-higher-education-2016.

Higher Education’s Top 10 Strategic Technologies for 2017
This research studies the new technologies that institutions are implementing, planning, and tracking in 2017 and the trends influencing institutional IT strategy. Read the reports at https://library.educause.edu/resources/2017/1/higher-educations-top-10-strategic-technologies-for-2017.

Information Security Training and Awareness Programs Research
In early 2016, the SANS Institute released its second annual SANS Securing The Human report. The educational services industry represented 21% (n = 76) of the SANS survey responses, the largest sector represented in this research. SANS graciously shared anonymized data results with the EDUCAUSE Center for Analysis and Research (ECAR) to report on the state of higher education awareness and training programs. Read the ECAR report at https://library.educause.edu/resources/2016/8/higher-education-information-security-awareness-programs.

Undergraduate Student and Technology Research
This almanac summarizes data collected from the 2016 ECAR Undergraduate Student and Technology survey. In this research, ECAR collaborated with 183 institutions to collect responses from 71,641 undergraduate students about their technology experiences. A stratified random sample of approximately 10,000 respondents was drawn from the overall response pool to proportionately match a profile of current U.S. undergraduates regarding age, gender, ethnicity, Carnegie class, and institutional control (public/private). Learn more at https://library.educause.edu/resources/2016/6/2016-students-and-technology-research-study.

ABOUT THE EDUCAUSE CYBERSECURITY INITIATIVE

The EDUCAUSE Cybersecurity Initiative supports higher education institutions as they improve information security governance, compliance, data protection, and privacy programs. For more information, visit www.educause.edu/security.