The EDUCAUSE Information Security Almanac

April 2019

This almanac shares the most important EDUCAUSE data regarding the state of information security in higher education. Data are derived from the 2018 EDUCAUSE Core Data Service.

INFORMATION SECURITY SPENDING AND STAFFING

3.6% Central IT spending on information security (including identity and access management) as a percentage of total central IT spending

0.26 Central IT information security FTEs per 1,000 institutional FTEs

INFORMATION SECURITY LEADERSHIP AND STAFF CERTIFICATION

41% 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 (42%)
- Information security officer (20%)
- Director of information security (15%)

Most common reporting lines for a full-time information security leader:

- Highest-ranking IT administrator/officer (e.g., CIO) in central IT (83%)
- Other IT management (4%)
- Director of networking (3%)

Most common preferred certifications for information security professionals (at institutions that require or prefer certifications):

- Certified Information Systems Security Professional (CISSP) (93%)
- Certified Information Security Manager (CISM) (38%)
- GIAC Security Essentials (33%)

INFORMATION SECURITY RISK ASSESSMENTS

76% Institutions that have conducted any sort of information security risk assessment

25% Institutions that have conducted an information security risk assessment of cloud-service or third-party providers

23% Institutions using the Higher Education Cloud Vendor Assessment Tool (HECVAT)

Main reasons for performing information security risk assessments (at institutions that perform risk assessments):

- Planning/prioritizing institutional security work (63%)
- Regulatory requirement (e.g., HIPAA, GLBA) (48%)
- Contractual requirement (e.g., PCI) (45%)

TRAINING AND AWARENESS

85% Institutions with mandatory information security training for faculty or any staff

49% Institutions with mandatory information security training for students

Most common information security training topics for faculty or any staff:

- Regulatory compliance—FERPA (64%)
- Usage policies (AUP) (56%)
- Regulatory compliance—PCI DSS (51%)
- Security policies (51%)

Most common mandatory training topics for students:

- Usage policies (AUP) (36%)
- Security policies (23%)
- Self-defense (e.g., phishing) (23%)
- Privacy policies (21%)

INFORMATION SECURITY METRICS AND FRAMEWORKS

71% Institutions that track any information security metrics

Most commonly tracked information security metrics (at institutions tracking any information security metrics):

- Vulnerability scan coverage (44%)
- Incident rate (40%)
- Number of known vulnerability instances (39%)
- Patch policy compliance (32%)

Most commonly deployed information security standards or frameworks:

- NIST 800-53/FISMA (33%)
- NIST Cybersecurity Framework (32%)
- NIST 800-171 (31%)

INFORMATION SECURITY RESPONSIBILITY AND PRACTICES

Areas for which central IT most commonly has primary responsibility:

- Network security (94%)
- Monitoring (88%)
- Communications security (86%)
- Identity management (83%)

EDUCAUSE

Areas for which other administrative or academic units most commonly have primary responsibility:

- Records retention (37%)
- Cyberliability insurance (28%)
- Physical security (28%)

Areas most commonly outsourced:

- Forensic analysis (10%)
- Cyberliability insurance (2%)
- E-discovery (2%)

Most commonly deployed information security technologies:

- Antivirus/antispam/spyware/malware protection (99%)
- Secure remote access (93%)
- Secure wireless access (93%)

Most commonly reported disaster recovery (DR) practices:

- Presence of a formal IT DR plan (64%)
- IT DR plan assigns clear responsibility to lead the recovery process (63%)
- IT DR plan assigns clear responsibility to carry out the operational process of recovery (62%)

Information security threats most commonly rated as a concern to the institution:

- Exposure of confidential or sensitive information (79%)
- Email viruses, ransomware, or other malware (31%)
- Unauthorized or accidental modification of data (29%)
- Unauthorized, malicious network/system access (27%)
- Loss of availability or sabotage of systems (16%)

51% Percentage of institutions that are part of three or more multi-institutional collaborations related to information security

Multi-institutional collaborations that institutions most commonly participate in:

- REN-ISAC (64%)
- State or regional group (56%)
- Internet2 (42%)
- Public/private information-sharing activities (41%)
- HEISC (25%)

IDENTITY AND ACCESS MANAGEMENT PRACTICES

Institutions that require authentication for:

- Wireless access for institutional users (94%)
- Wireless access for guests (57%)
- Wireless access using Eduroam (54%)
- Wired connections from public devices/endpoints (54%)

75% Institutions tracking, planning, or with partially deployed nonbiometric multifactor authentication (MFA)

17% Institutions with institution-wide deployment of nonbiometric MFA

Top uses of MFA at institutions using multifactor authentication:

- Business-critical applications (e.g., financial or HR systems) (57%)
- IT administrative access (55%)
- Remote access to IT services (46%)
- Email (38%)

Top types of institutionally provided MFA (at institutions using MFA):

- Mobile device authenticator apps (72%) provided for:
  - Faculty (77%)
  - Staff (95%)
  - Students (49%)
- Text message one-time passwords (51%) provided for:
  - Faculty (80%)
  - Staff (90%)
  - Students (61%)
- Key fobs (41%) provided for:
  - Faculty (74%)
  - Staff (92%)
  - Students (30%)
- Security tokens (41%) provided for:
  - Faculty (84%)
  - Staff (95%)
  - Students (39%)

13% Institutions using biometric authentication for students, faculty, or staff

Percentage of institutions allowing most or all users to have local system admin rights on institutionally managed devices (including workstations and other end-user devices):

- Faculty (44%)
- Staff (36%)
- Students (17%)

ABOUT THE DATA IN THIS ALMANAC

In the summer of 2018, 3,800 institutions were invited to contribute data to the EDUCAUSE Core Data Service (CDS). This almanac summarizes data from the 457 US institutions with Carnegie Classifications of AA, BA, MA, or DR that responded to the optional information security module. Some publicly available data from the Integrated Postsecondary Education Data System (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.

ABOUT THE EDUCAUSE CYBERSECURITY PROGRAM

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.