Information security activities are of strategic importance to higher education institutions. Trusted with large amounts of varied types of sensitive information, colleges and universities are under pressure from a number of sources to ensure that all institutional data are properly safeguarded and used. No longer a "nice to have" function, information security in higher education is a "must have" function that is maturing beyond the provision of basic security technologies. Today, information security is an institutional concern that must be addressed in a collaborative manner by many stakeholders across multiple departments. When approached thoughtfully and strategically, good information security practices help minimize institutional risk, ensure reliable institutional operations and decision making, and increase trust in the institution.

**What is the current state of information security?**

2% of the IT budget at U.S. institutions is spent on information security.

There are 0.1 central IT information security FTEs per 1,000 institutional FTEs.

71% of U.S. institutions have mandatory information security training for faculty or staff.

At most institutions, the person with primary responsibility for information security is not the CIO or CISO. 19% of U.S. institutions have a CISO who has primary responsibility for information security, and 59% of CISOs devote 100% of their time to IT security.

Only 50% of U.S. institutions track information security metrics. Of those that do, these are the most commonly tracked metrics:

- Vulnerability scan coverage: 29% AA, 18% BA, 35% MA pub., 18% MA priv., 43% DR pub., 37% DR priv., 35% All U.S.
- Incident rate: 21% AA, 14% BA, 28% MA pub., 14% MA priv., 38% DR pub., 31% DR priv., 29% All U.S.
- Number of known vulnerability instances: 23% AA, 13% BA, 30% MA pub., 30% MA priv., 31% DR pub., 31% DR priv., 27% All U.S.
- Patch management coverage: 32% AA, 19% BA, 24% MA pub., 24% MA priv., 21% DR pub., 20% DR priv., 27% All U.S.
- Patch policy compliance: 32% AA, 16% BA, 24% MA pub., 18% MA priv., 21% DR pub., 31% DR priv., 26% All U.S.

Information for this Spotlight was derived from Modules 1 and 7 of CDS 2014. Module 1 focuses on IT financial and staffing data. Module 7 focuses on information security and identity management practices. Responses from 545 institutions were analyzed. Only U.S. institutions with a designated Carnegie class of AA, BA, MA, or DR were analyzed for this bulletin.
Institutions are maturing in their information security practices and programs. Many higher education institutions are no longer content to simply put a number of information security practices in place. Instead, they want to strategically implement practices that ensure the success of the institutional information program. Institutions also want to use data about program capability to drive future information security actions. Since 2002, the EDUCAUSE Core Data Service (CDS) has been providing higher education CIOs and senior IT leaders with the benchmarks they need to make strategic decisions about IT at their institutions. In 2014, CDS was enhanced to help institutions understand their maturity in delivering information security services. Understanding this maturity will help institutions evaluate and improve their information security practices.

INFORMATION SECURITY PROGRAM MATURITY IS ASSESSED IN FIVE KEY AREAS:

- Information Security Organization: Understanding how the institution manages information security across the institution, including management responsibility for information security activities and overall direction for information security activities.
- Information Security Policy: Understanding how the institution approaches formalized information security policies, standards, and procedures.
- Data Security and Data Management Processes: Understanding how the institution manages and protects data during its entire life cycle.
- Access Control Processes: Understanding how the institution manages the way in which users and information systems communicate with one another.
- Information System Security Processes: Understanding the practices and processes that an institution takes to protect its information systems.

INFORMATION SECURITY MATURITY IS MEASURED ON THE FOLLOWING SCALE:

1. Absent/Ad Hoc: An institution doesn’t currently have this capability or addresses it in an ad hoc way.
2. Repeatable: An institution has established this capability, but its practices are mostly informal.
3. Defined: An institution has standardized this capability and has documented procedures related to it.
4. Managed: An institution manages this capability to achieve predictable results on the basis of reliably measured performance indicators.
5. Optimized: An institution regularly measures performance and reassesses the way it delivers this capability in order to improve practices and manage risks.

See Also
- EDUCAUSE Cybersecurity Initiative.

About the Authors
- Joanna L. Grama is the Director of IT GRC and Cybersecurity Programs at EDUCAUSE.
- Leah Lang is the Director of Analytics Services at EDUCAUSE.