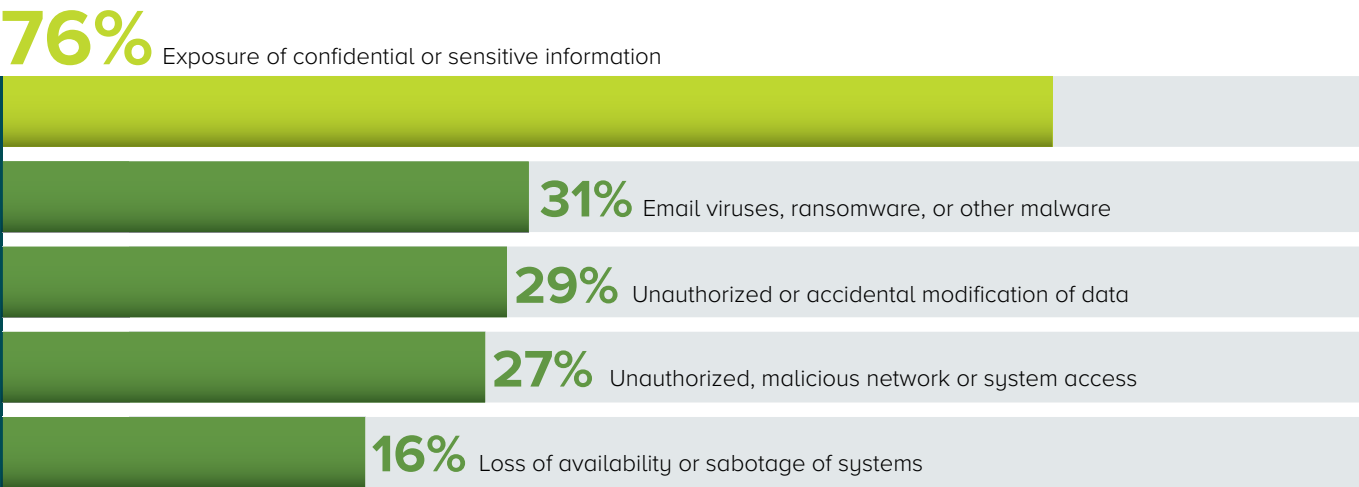# Spring Cleaning:
Security and Privacy

Spring is traditionally a time for cleaning and organizing. Information security and privacy practices need as much upkeep as (or more upkeep than) storage sheds and closets. In fact, in the EDUCAUSE 2019 TOP 10 IT Issues research, Information Security Strategy was #1 and Privacy was #3. Let's find out how higher education institutions view and treat these critical topics.

2019 TOP 10 IT ISSUE #1 — INFORMATION SECURITY STRATEGY

What it means: Developing a risk-based security strategy that effectively detects, responds to, and prevents security threats and challenges

What are the biggest threats?

76% Exposure of confidential or sensitive information

31% Email viruses, ransomware, or other malware

29% Unauthorized or accidental modification of data

27% Unauthorized, malicious network or system access

16% Loss of availability or sabotage of systems

Are institutions offering training?

85% Mandatory information security training for **faculty or any staff**

49% Mandatory information security training for **students**

What's the leadership and spending landscape?

41% Institutions with a dedicated person whose primary responsibility is information security

3.6% Central IT spending on information security as a percentage of total central IT spending

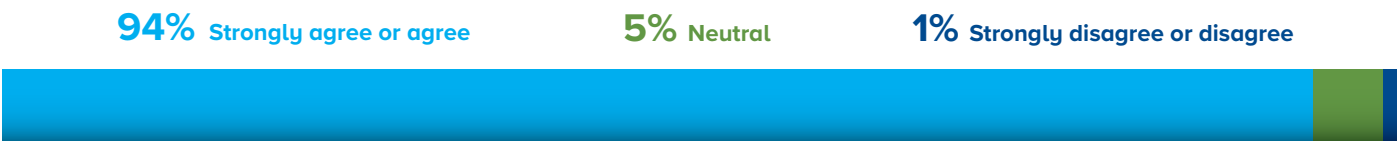*Source: EDUCAUSE Information Security Almanac 2019*

2019 TOP 10 IT ISSUE #3 — PRIVACY

What it means: Safeguarding institutional constituents' privacy rights and maintaining accountability for protecting all types of restricted data
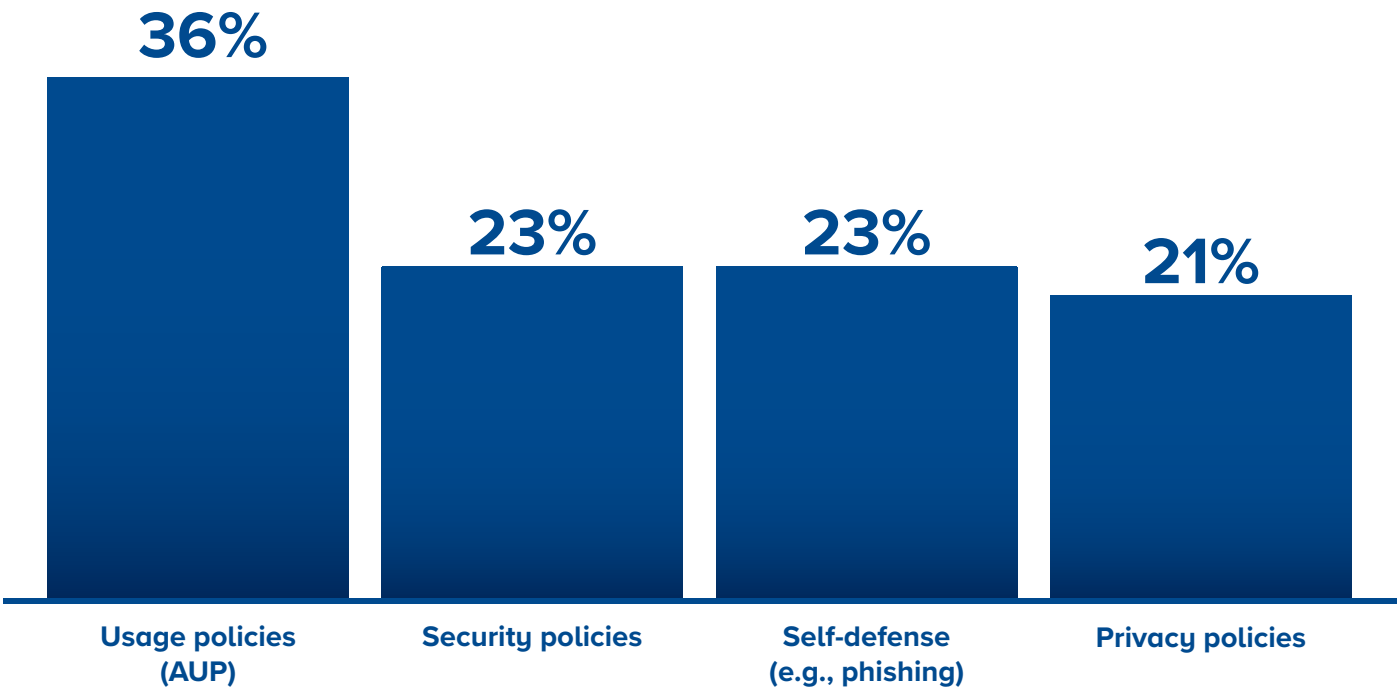
How do stakeholders view privacy practices?

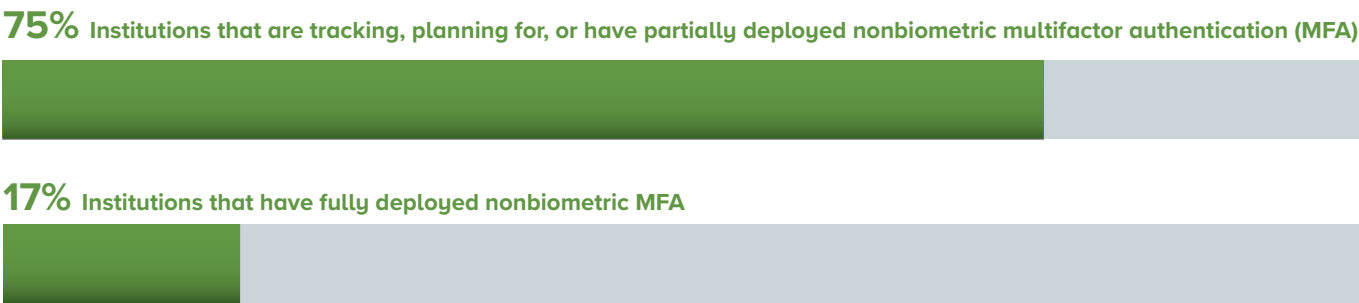In conducting student success studies, privacy rights are respected:

94% Strongly agree or agree   **5%** Neutral   **1%** Strongly disagree or disagree

Source: AIR/NASPA/EDUCAUSE data

What are the most common mandatory training topics for students?

36% Usage policies (AUP)

23% Security policies

23% Self-defense (e.g., phishing)

21% Privacy policies

How are institutions employing identity and access management?

75% Institutions that are tracking, planning for, or have partially deployed nonbiometric multifactor authentication (MFA)

17% Institutions that have fully deployed nonbiometric MFA

Source: EDUCAUSE Information Security Almanac 2019