California Community Colleges | Information Security Center

AT A **GLANCE**

INFORMATION SECURITY ON YOUR CAMPUS

Amidst a growing number of information security attacks, community colleges, like other major organizations, have a legal and ethical responsibility to secure their information:

Data breach incidents are widespread and significant

- Cyberattacks on education and research institutions increased 75% from 2020 to 2021
- Ransomware is responsible for one third of education sector data breaches
- In 2022, 64% of higher education institutions were affected by ransomware
- All California public higher education systems have been recent targets
- Data breaches in the education sector have exposed more than 24.5 million personal records since 2005

Sources of public-sector security breaches

- External threats motivated by financial gain are the most common source of security breaches
- System intrusion represents nearly half of all data breaches, followed by errors and web application attacks
- Since many organizations do not publicly report breaches, there may be more instances than are known

Information security in California

- California law requires organizations to notify any California resident whose unencrypted personal information may have been acquired by an unauthorized person
- Incidents must also be reported to the Office of the Attorney General

Be prepared

- Higher education rivals only the healthcare industry in the amount of personally identifiable information generated and stored
- Security breaches places colleges' data integrity, liability, reputation, and budget at risk
- Vulnerability assessments, training, best practices, and monitoring platforms and resources are available at no cost to California Community Colleges

INFORMATION SECURITY BEST PRACTICES

The information Security Center recommends adopting the Critical Security Controls developed by the Center for Internet Security (CIS). According to CIS, organizations that apply the first five controls can reduce their risk of cyberattacks by around 85 percent. These five security controls help colleges actively manage authorizations for personnel and devices as well as the implementation of processes for vulnerability assessments.

1	2	3	4	5
Inventory of Authorized and Unauthorized Devices	Inventory of Authorized and Unauthorized Software	Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers	Continuous Vulnerability Assessment and Remediation	Controlled Use of Administrator Privileges

INFORMATION SECURITY CENTER RESOURCES

To confront the challenges explored in its white paper, "Managing Information Security on Campus," the CCC Tech Center's Information Security Center has developed six resources, provided at little to no cost, specifically designed to help improve information security at the California Community Colleges.

1. **Vulnerability assessments**
   Vulnerability assessments scan internet-facing servers, helping colleges discover vulnerabilities before criminals.
2. **Information security policy and templates**
   Access sample policies and procedures at cccsecuritycenter.org. Policies address data handling and protection, access control, and end-user awareness.
3. **Employee information security awareness training**
   Self-paced, online training is available to California Community College administrators who handle secure information on campus.
4. **Vulnerability management software**
   Vulnerability management through Tenable will allow colleges to gain actionable insight into security risks through a cloud-based vulnerability management platform that will be available soon.
5. **Centralized logging and analysis software**
   Search, alert, report, and monitor logs from one location in real time. Through Splunk, administrators can troubleshoot applications outages, investigate security incidents, and demonstrate compliance.
6. **Unlimited SSL certificates**
   Create secure connection from a web server to a browser with unlimited SSL certificates through a partnership with InCommon.

Contact Information:
Omer Usmani
ousmani@ccctechcenter.org