MANAGING INFORMATION SECURITY ON CAMPUS
A Guide for California Community Colleges

March 2017
CCCTECHCENTER.ORG
College and university information systems are under attack. The Information Security Center, housed at Butte College, reports a large number of higher education institutions are victims of information security attacks. Even the most prestigious universities in our country, including Harvard, Stanford, and Johns Hopkins, have suffered information security attacks. The publicly funded group Privacy Rights Clearinghouse has compiled an in-depth list of K-12 schools, colleges, and universities recovering from information security attacks. A sample of schools is available in Appendix A.

In just over a decade, within the U.S., nearly 100 million personal records were hacked. In California, within the last five years, nearly 34 million personal records were hacked. The California Data Breach Report suggests the problem may be even more severe because many organizations are: 1) unaware of the reporting requirements; 2) ignorant of an ongoing information security attack; or 3) not reporting or under-reporting breaches because of public relations concerns.

Colleges, like other major organizations, have a legal and ethical responsibility to secure their information. The law requires colleges to notify the users whose data was breached and to report the breach to the California Attorney General’s office.

According to the Office of the Attorney General:

California law requires a business or state agency to notify any California resident whose unencrypted personal information, as defined, was acquired, or reasonably believed to have been acquired, by an unauthorized person. Any person or business that is required to issue a security breach notification to more than 500 California residents as a result of a single breach of the security system shall electronically submit a single sample copy of that security breach notification, excluding any personally identifiable information, to the Attorney General.

This white paper explores the security needs of the California Community Colleges (CCC), specifically: information security attacks on higher education institutions are rising and there are significant consequences for neglecting the threat. This white paper also describes the resources the CCC Technology Center Information Security Center provides specifically designed to help CCC leaders secure their systems and protect their users’ information.
Higher education is a prime data-security attack target because of the massive amount of personal data stored on potentially vulnerable campus servers (e.g., student, financial aid, administrative, syllabi, curriculum, assessment, grades). The increased use of digital teaching technologies such as cloud computing, streaming video, and learning management systems also generates large amounts of data, making them attractive information security-attack targets. In fact, higher education rivals only the healthcare industry in the amount of personally identifiable information generated and stored. As college processes increasingly become digitized, the potential risks also increase. And, the total number of student, former student, and employee records increase each year.

According to Dave Reese, vice president of infrastructure strategy and security at the Corporation for Education Network Initiatives in California (CENIC), CENIC has more outgoing than incoming tickets for Denial of Service (DoS) attacks. According to Jeff Holden, chief information security officer for the CCC Tech Center, this means network computers are compromised and the attackers are using them to try to take down other networks.

But, external data breaches are not the only threat. According to the Verizon Data Breach Investigations Report, human error is a far more common cause of a data security breach for public sector organizations. In fact, employees and contractors make up the largest share of 2016 public sector data breaches.

The breach at the Riverside Community College District demonstrates how easy it is for personal information to get into the wrong hands. The data compromise occurred when a district employee used an external e-mail account to send a file to a colleague’s home e-mail because the file was too large for the district’s secure, encrypted e-mail server. The employee accidentally sent the file to the wrong e-mail address, exposing the confidential records of more than 35,000 students.

Cuesta College suffered a different type of attack. A Cuesta College employee was jailed for breaching the campus data system when she stole employee names, home addresses, e-mail addresses, phone numbers, and Social Security numbers in an attempt to sell the information to identity thieves. College of the Desert, Solano Community College, City College of San Francisco, and the San Jose Evergreen Community College District also reported breaches within the last year.

Information security attacks against U.S. colleges and universities are proliferating. A dean at the University of Wisconsin told the New York Times his school sees 90,000 to 100,000 hacking attempts from China every day, plus countless probes from other countries. According to Rodney Petersen of Educause, the number of attacks is going up exponentially and as the
attacks increase so do the costs. **Information security breaches place the college’s data integrity, liability, reputation, and budget at risk.**

Costs are difficult to quantify. Generally, liabilities come from a number of areas including data loss, litigation, damaged reputation, and financial costs to employees and students from identity theft. For example, Maricopa County Community College District (MCCCD) in Arizona suffered the compromise of personal and financial information for 2.5 million students despite an FBI warning that MCCCD’s systems were vulnerable. The district has spent $20 million addressing the issue.

After Cuesta College discovered it was the victim of an information security attack, the school covered the costs for one year of identity theft protection for the 4,000 victims to mitigate its liability. The protection cost the college $110 per employee, for a potential cost of $440,000.

The U.S. Department of Justice reports the average identity theft victim suffers a loss of more than $2,000, not including the time and effort needed to clear their credit record. Nearly a third of identity theft victims in the report spent a month or more resolving problems, while more than one out of three identity theft victims reported moderate or severe emotional distress as a result of the incident.
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. The first five security controls help colleges actively manage authorizations for personnel and devices and implement processes for vulnerability assessments.

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Inventory of Authorized and Unauthorized Devices</td>
<td>Inventory of Authorized and Unauthorized Software</td>
<td>Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers</td>
<td>Continuous Vulnerability Assessment and Remediation</td>
<td>Controlled Use of Administrator Privileges</td>
</tr>
</tbody>
</table>

Source: CIS Critical Security Controls
INFORMATION SECURITY CENTER RESOURCES

To confront the challenges explored in this white paper, the CCC Tech Center’s Information Security Center has developed six resources, provided at no cost through support from the California Community Colleges Chancellor’s Office.

1. **Vulnerability assessments**
   Vulnerability assessments scan internet-facing servers, helping colleges discover vulnerabilities before they are exploited by 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. Colleges can select from 30 training modules to create custom training programs for individuals or teams.

4. **Vulnerability management software**
   Coming in 2017, vulnerability management through Tenable will allow colleges to gain actionable insight into security risks through a cloud-based vulnerability management and container security platform.

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 a secure connection from a web server to a browser with unlimited SSL certificates through a partnership with InCommon, a community of professionals dedicated to protecting online resources in U.S. education and research. InCommon memberships for California Community Colleges are underwritten by the California Community Colleges Chancellor’s Office.

The number, size, and scope of information security attacks is proliferating. Colleges that neglect to address information security place their students, employees, and reputations at risk. The burden is now on colleges and their employees to demonstrate that their digital information is secure. The Information Security Center is the state’s resource designed to meet the California Community Colleges’ information security needs. Go to cccsecuritycenter.org for more resources and information.
APPENDIX A

Breach Incidents in Higher Education (2014-2016)

Number of users exposed

Source: Privacy Rights Clearinghouse
NOTES


Note: No data breach list can be comprehensive.


8. California Civil, Code Division 3, Part 4, Title 1.8 (Article 7) & Title 1.81 (1977) oag.ca.gov/ecrime/databreach/reporting.


