BitLyft

CYBERSECURITY

*8 STEPS FOR*

# HIGHER ED CYBERSECURITY HYGIENE

# INTRODUCTION

Let's face it. Colleges and universities face many challenges when it comes to cybersecurity. In fact, these institutions are highly sought out by cyber criminals. Not only do they possess a vast amount of personally identifiable information (PII), but they also house compensation data, intellectual property and much more. IT staff is responsible for protecting this data, but many find themselves competing with other departments for budget dollars to do so. To top it off, many institutions lack the staff and training needed to implement a cybersecurity strategy.

Despite these challenges, leadership still holds the IT department responsible for the integrity and security of the university's network. That's a lot of pressure.

## BitLyft understands.

Over the years, we've seen many of our higher education partners face these same challenges. Based on these experiences, we compiled eight cybersecurity tactics that we think every college or university should implement.

## 1 ASSET INVENTORY

Before you even begin to create a cybersecurity plan, you need to know which assets you need to protect. Therefore, the first step you should take is to conduct an inventory of your assets.

## 2 APPLICATION INVENTORY

After you complete an inventory of your assets, you should take an inventory of your applications. This includes approved and unapproved apps used within your environment. You may discover software running in your network that you didn't know about. This creates a potential exposure risk to your organization and the devices that software is communicating with.

## 3 VULNERABILITY SCANNING

The next step is to scan for vulnerabilities. This critical step allows you to prioritize your patching workload by outlining which assets need attention first. Then, you can move down the list from most to least critical. Conducting a vulnerability scan is recommended before you move on to penetration testing. Patching vulnerable systems before the "pen test" even begins allows you to get the most value from the process.

## 4 PROCEDURES AND POLICIES

With the increase of cyber threats and compliance guidelines, having an incident response procedure is required. This plan helps reduce panic when a situation arises since you already have a "checklist" to follow. Included in the incident response strategy is a comprehensive backup and disaster recovery plan. Some universities have procedures in place like cleaning all viruses off the machines before a new school year, but that isn't enough. You need a better way to ensure the malware is successfully removed from the hardware within your environment.

## 5 VISIBILITY

Visibility into possible malicious activity within Workday, Ellucian, or other Enterprise Resource Planning (ERP) solutions is paramount. Higher education institutions require the ability to pull logs from these apps along with other education-specific applications. The risks posed to these programs are great. You need to monitor your most prized assets and keep the data of students, faculty and staff secure.

## 6 MONITORING AND RESPONSE

Advanced visibility and detection of Office 365, emails and management activity (including Azure and Active Directory) is a minimum. With the amount of data transferred over the average institution's network, you need the ability to verify that the users and recipients are legitimate. If anomalous activity is detected, it should get neutralized within seconds, not days or weeks.

## 7 CENTRAL SOURCE OF TRUTH

Even though every institution utilizes a different system, the goal is the same for them all. At the end of the day, you want to ensure the correct users are performing the intended actions within your environment. So whether you have an on-premise infrastructure or use AWS, Azure, or another cloud-based CRM system or ERP, you should use a centralized source of logging. Otherwise, with so many systems and software, it is hard to tell if one small event is connected to another. Your approach must include real-time analysis of logs, data correlations of events and quick discovery of incidents so you can neutralize threats before they become problematic.

## 8 AUTOMATED INCIDENT RESPONSE

Many of our clients require automated threat response since they lack the staff to cover this task on their own. Cybersecurity is not the only facet of their job. They still need to work on new projects and keep other systems operating while protecting their IT environment. An end-to-end system must be in place to aid this requirement.

Read more about our work in the higher ed space at:
**www.bitlyft.com/higher-education.**