SIKICH®

HIGHER ED

FIVE IT SECURITY BEST PRACTICES
TO STRENGTHEN YOUR UNIVERSITY CYBERSECURITY

Over the 2017 winter holidays, a thief made the headlines. It didn't matter that generous volunteers dressed up as Santa Claus and stood in the freezing Chicago cold beside their red bucket asking for donations. All that mattered was that the chime of their bells signified cash donations, marking the thief's next target. Someone was stealing thousands of dollars in donations by simply grabbing the buckets filled with donations when "Santa Claus" wasn't looking. What went wrong? Simple. Defenses were down, and volunteers weren't prepared.

Much like Santa, higher education institutions are seemingly innocent bystanders and may not expect to be the targets of a cybersecurity attack. In reality, universities need to protect their databases more so than for-profit businesses. Why? Not unlike businesses, colleges accept and handle donations, which means credit card processing and PCI DSS compliance requirements. In addition, these institutions also store and transfer personally identifiable information (PII) and collect everything from sensitive data about donors to information about their email preferences.

Practicing good IT security is just as important for colleges as it is for for-profit businesses, since colleges are just as vulnerable to attack. Consider ransomware attacks. In these instances, the attackers don't typically target specific types of businesses; they just hope to find any business they can cripple to get a ransom payment. It's more imperative now than ever for universities to implement the right infrastructure and improve their IT security with these five best practices.

Five IT Security Best Practices for Higher Education Institutions

1. **Designate an Individual as an IT Security Lead** – Designate someone in your institution as the lead of your IT security. This individual should have at least a basic understanding of IT security and know who to contact should your security become compromised.
2. **Conduct an IT Risk Assessment** – Know where you stand. How vulnerable is your university now? Conducting an IT risk assessment will help you understand the threats to your organization—who has tried to attack your systems before? What are your IT weak points?
   Utilize the results of your IT risk assessment to make decisions on how to test your environment. For example, if it's determined that external threats present a greater risk to your organization than internal threats, allocate a higher portion of your security budget for external testing.
3. **Implement Security Controls** – Where are your most vulnerable points within your infrastructure? Knowing this information can help you build up your security systems to prevent future attacks. The results of your IT risk assessment can also be used to help you focus the implementation of your security controls in the most efficient and effective manner.
4. **Conduct Penetration Testing** – Running your institution through penetration testing is one of the best ways to test the efficacy of the controls you've implemented as a result of the IT risk assessment. It simulates a real-world attack against your organization and provides great insights into your security posture. However, it's important to note that you should conduct due-diligence in vendor selection for penetration testing—chose a vendor that conducts manual testing with experienced staff. Not all penetration testing is created equal.
5. **Test Your Systems *and* Your Team** – While you might think your IT systems are relatively secure, is your team prepared, should something happen? Institutions often overlook the user aspect of IT security—don't just test your systems, test your team. Most attacks still involve some type of social engineering, which is why it's important to conduct regular social engineering testing to keep it top of mind for your staff.

If your higher education institution underwent a penetration test today, would it pass? If it

detected a compromise of its security, how would it respond? Being able to answer such IT security questions is important across all types of organizations, including colleges. Evaluate the state of your university cybersecurity, then implement these best practices to make sure your organization continues to grow with IT safety and security in mind.

At Sikich, our team of technology and higher education experts can assist you with the security challenges your institution faces. Visit our website at www.sikich.com to schedule a consultation.