UNISYS | Securing Your Tomorrow®

Time for universities to teach cybercriminals a lesson

Six keys to security peace of mind for students, faculty and staff

The Asia Pacific education sector experienced a 21% increase in cyberattacks, compared with just an average 3.5% increase across all other sectors.

The higher education sector has learned the hard way about cybersecurity, thanks to cybercriminal intrusions that cost billions and disrupted university services and functioning. The security techniques and technology that other sectors have deployed can be quickly adapted for university systems. And none too soon, now that the government prepares to enforce an "enhanced framework to uplift security and resilience" upon universities, and now that students, faculty, researchers, and IT professionals are increasingly sensitive to a university's cybersecurity performance and making their choices accordingly, with cybersecurity a firm competitive advantage.

Unsurprisingly, the COVID-19 pandemic exposed the higher education sector's susceptibility to cybersecurity attacks. While the rush to virtual learning allowed a massive increase in attacks, the truth is, cybercriminals have long been aware that higher education is a target-rich, insufficiently defended environment. Recently the UK's National Cyber Security Centre (NCSC) issued a fresh, urgent security alert as universities were assailed with waves of cybersecurity breaches. In the second half of 2020, the Asia Pacific education sector experienced a 21% increase in cyberattacks, compared with just an average 3.5% increase across all other sectors, according IT Brief Australia.

A Sizeable and Urgent Challenge

The Australian Centre of Cyber Security (ACCS) reports that Education and Training in the 2020-2021 financial year ranked number five in terms of number of security incidents and number four in terms of ransomware-related incidents.

Analysis of the QS World University Rankings 2020 by ProofPoint found that "almost half of Australia's top 20 institutions in the QS World University Rankings 2020 appear to have had no protection in place against hackers trying to trick people to take over their computer systems," while only two universities proactively were blocking fraudulent emails. The costs of such fraudulent emails are staggering – $81 billion AUD in the 2020-2021 financial year, according to the ACSC Annual Cyber Threat Report. Even if there is no data lost, system downtime when responding to a suspected breach can vastly disrupt a university's ability to deliver its services, as was shown when RMIT cancelled online and in-person classes following an IT outage caused by a phishing scam.

In one example cited by the ASCS, the network of a leading university in Australia was penetrated by a ransomware attack that caused the administration to suspend its network until it could reopen uncompromised. The report notes that by penetrating education IT environments, criminals can then find pathways to other organisations like research and governments for access to their information and for purposes of additional ransom demands.

There is good reason for higher education's appeal to intruders, including tons of valuable information about students, staff, vendors, alumni that intruders can monetise.

A Favourite Target

There is good reason for higher education's appeal to intruders: There are vast stores of valuable information about students, staff, vendors, alumni that intruders can monetise and vital research data can be sold to shady nation states. A security talent shortage leaves higher education competing at a disadvantage with the private sector. The decentralised structure of the academic world enables disparate departments to invest in their own IT without the oversight of security professionals – creating shadow IT. Universities have a culture of sharing information not just within the university but with other schools, governments, and private entities.

And finally, universities networks serve many different types of individuals with various devices who expect ready access to a vast number of systems across numerous locations, offering intruders multiple entry points to compromise. It only took a single email for hackers to enter the Australian National University's network, where they were able to explore and exfiltrate undiscovered for weeks and then cover their tracks so successfully that the perpetrators have never been identified. Deakin University discovered that employees were using unsecured methods to store and share highly sensitive information. Monitoring and responding to these environments is a tricky business.

Results from the 2021 Unisys Security Index™ for Australia indicate heightened recognition of these vulnerabilities and growing concern. The overall measure of security concerns of the Australian public rose two points from 2020, the highest for Australia in the 15 year history of the study. The top security concerns cited were data/privacy related: ID theft (59% of Australians are concerned about this issue) and hacking and viruses (57%).

Six Keys for Better Security

So, with all those vulnerabilities, how does the sector provide the level of cybersecurity that its constituents deserve and expect? By adopting a variety of measures that have already been proven in other sectors.

1. **Limit Damage** - You are bound to have many legacy systems and they are likely to have vulnerabilities – accept that as a fact, patch them as best you can, and accept that you will experience a breach accordingly. Your responsibility is to ensure that the inevitable breach doesn't lead to a wholesale penetration of your environment – lateral movement of the intruder across your network, which is how serious damage occurs. By micro-segmenting your systems, you can wall off intruders from your most sensitive information.

2. **Test Your Defences** - Don't let criminals be your cybersecurity quality control. Don't wait to be attacked to see if your defences work. Do your own penetration testing. Test, test, test. Exploit your own vulnerabilities and prevent ransomware and exfiltration of data not only to be in compliance but to demonstrate a strong security posture. This includes testing people to see if they will fall for a dummy attack. Especially if they accept payment cards, as universities do, you are obliged to comply with the Payment Card Industry Data Security Standard (PCI DSS) with penetration testing every six months.

Zero Trust means exactly what it says. Nobody knocking at your network door is to be trusted to be who they say they are. Every person or device seeking access must be able to verify any and everything before being granted access.

3. **Verify, Don't Trust** - In today's hyper security environment, there's no alternative to adopting the concept of Zero Trust. That means exactly what it says. Nobody knocking at your network door is to be trusted to be who they say they are. Every person or device seeking access must be able to verify any and everything before being granted access. Zero Trust is a posture, principles, and architecture. It is a journey of many steps: authenticating users and least privilege access. Micro-segmenting mission critical systems. Asset discovery and inventory management. And so on. Start now with your top priorities – your most sensitive data and systems – and build security into them.

4. **A Holistic Security Mindset** - There is also a critical cultural aspect to cybersecurity. It requires a holistic mindset that unites all parts of the university in thinking about security in everything they do, rather than siloed departments making their own decisions, purchases, policies, and procedures. All parties must focus as much on security as on availability, access, and capacity – and all driven from the top. Cybersecurity belongs in every conversation at the top of the organisation. Your cybersecurity leaders and partners belong in every strategic conversation.

5. **Internal Accountability** - It can be tempting to simply outsource security responsibilities to vendors with impressive credentials, but that is a dangerous mistake. No outside party can be as familiar with your organisation, its strategies, its systems, its day-to-day operations, and its people as well as internal experts whose entire focus is on your university. To be sure, they will want reliable partners with extensive experience who can advise them on best practices and common mistakes. But ultimately, if you suffer a breach, it will be your university, not the vendor, in the damning headlines, so keep it within your authority.

6. **Education Is Forever** - Educate your users – and re-educate them every time a new lesson is learned from another entity's misfortune. Cybercriminals are often highly sophisticated operators who have all the time in the world to probe your defences, trick your users, and deploy innovative schemes. Make sure your users know how these tricks work, how damaging they can be, and how to avoid and report them. Don't settle for memos and alerts that might not be noticed. Require affirmative acknowledgement and proof of compliance. And don't forget – learning embeds best when it is engaging. Don't make people feel guilty – and don't be afraid to make it fun.

The good news is that the pandemic escalated the transition to digital education and highlighted the critical importance of a university's IT systems. But it also exposed its unique vulnerabilities. Cybersecurity now an urgent priority and a competitive advantage for higher education. The path is clear for university leaders and their cyber experts to earn the security credentials that their constituent needs and expects.

To learn more about how Unisys can help your university become cyber-resilient, visit www.unisys.com/offerings/security-solutions or contact us at www.unisys.com/contact-us

For more information visit www.unisys.com

© 2022 Unisys Corporation. All rights reserved.

Unisys and other Unisys product and service names mentioned herein, as well as their respective logos, are trademarks or registered trademarks of Unisys Corporation. All other trademarks referenced herein are the property of their respective owners.