Prashant Shokeen(01213303118)

Cybersecurity for Higher Education Institutes: Impact & Solutions

The COVID-19 pandemic changed our world and the way businesses operate dramatically. It has also brought about a diametrical change in the way education is delivered and accessed. Education workers, students, and teachers around the world drastically altered the way they taught, learnt and worked. While this led to a massive increase in access to education for many and a wider student pool, it also created a ripe and wider attack surface for cyber criminals.

According to a cybersecurity survey at CustomWritings professional essay services, there has been an astronomical rise in cyber-attacks on educational institutions. Cybersecurity attacks on higher education institutions are now an expected trend, instead of a speculative possibility.

Impact

Cybersecurity attacks on educational institutions are not just an operational or financial issue. They compromise student data and harm the overall integrity and reputation of institutions that have been built painstakingly over the years.

Systems are brought down to their knees, information is lost, anxiety and stress levels of staff and students skyrocket. Universities spend millions trying to recover from cyberattacks, and the recovery itself could take months as they try to first find the compromise before attempting to fix it.

Cybersecurity consultancies are often brought in to advise universities on how to defend against these cyberattacks, but with the constant evolution of these attacks, there has been no respite for universities and schools.

Why Are Universities Being Targeted?

Prashant Shokeen(01213303118)

Of course, major industries and companies are the most popular victims of cyberattacks. But higher education institutions have become a huge target because of the large amounts of personal data, medical records, and advanced project research papers they store in their system databases.

We will take a more in-depth look at some key reasons why universities are being avidly targeted by cybercriminals.

Universities, unlike their industrial counterparts, adopt a more open and transparent take on their infrastructure. These colleges and universities make sure that their sites can be connected to easily and without trouble by students and parents. This has unknowingly thrown the door wide open to cybercriminals.
Many leading global universities were early adopters of digital tools and internet access. Their systems hold valuable troves of knowledge and research materials that go way back. This makes them attractive targets for data theft. The situation is exacerbated by the fact that, unlike corporate networks, educational networks aren't always the most advanced or up-to-date. Therefore, they don’t end up being a good match against the advanced and highly sophisticated tools of the modern cyber-criminal.

Another reason why universities fall prey to cyber attacks is the limited talent in their cybersecurity or IT departments. Most technology graduates are lured away by handsome remuneration packages offered by companies like Apple and Microsoft. Thus, educational institutions, whose pockets aren't always as deep as the corporate bigwigs’, aren't necessarily able to attract the best talent who can keep their cybersecurity infrastructure robust and relevant all the time.

Common Cybersecurity Attack Trends

Now we’re going to take a look at some forms of cybersecurity attacks that pose potential risks to institutions of higher learning and ways to mitigate them.

Phishing - This is one of the most common forms of cybersecurity threats we face today yet it’s not always easy to identify a phishing attack. Phishing attacks are a type of social engineering attack. To put it simply, when a cybercriminal takes up a false identity to scam or trick someone into soliciting sensitive/important information or installing some sort of virus/malware on their system through malicious downloads, it is known as phishing. These cybercriminals often use popular topics or extremely attractive propositions to lure users into clicking strange links or downloading dangerous files.

Ransomware - After cybercriminals have managed to get your vital information or gained access to your crucial files, they then hold this information for ransom for outrageous financial demands. This is usually the aim of ransomware attacks. So students who are innocently looking for help writing an essay or are in need of online writing assistance often fall prey to phishing attacks which can then lead to larger ransomware attacks on the network they were using.

Evolving Attacks - As technologies become updated and evolved, so do cybersecurity attacks. One worthy of mentioning is fileless malware, which has been on the rise lately. This does not require the user to download any file or install any code. Instead, it uses the tools built into the system to initiate and perform these attacks. It makes legitimate programs execute dangerous attacks while your programs continue to run in the background. This form of attack is hard to detect as it leaves no footprint and is a nagging headache for most antiviruses
Solutions

While there's no denying that the threat of cyber-attacks is imminent and almost every business and institution is likely to get attacked at some point in their existence, here are a few steps universities and schools can take to ensure greater protection from cyber threats and more resilience in case of an incident.

Cybersecurity training: Staff and students alike should be given relevant cyber awareness training. They need to be helped in understanding that they play an important role in organisational cybersecurity and often they can be the ones preventing a phishing attempt or a ransomware attack from having any significant impact on the organisation.
Make sure all systems are updated regularly. Operating systems, browsers, and applications should always be up-to-date as each update fixes vulnerabilities and protects against new threats. This is a simple good practice that can make a world of difference when it comes to cyber safety of educational institutions.

Be Prepared. While creating awareness and instilling the importance of good security habits is imperative, unfortunately, this may not be enough. Your school or university could still come under attack and it's important to be prepared for that eventuality. Make sure you have a good incident response plan or ransomware response checklist that your team can refer to in case of an incident. When a crisis hits, it becomes difficult to think straight so visual workflows and pre-vetted response plans can really help to cut the chaos and take the right steps.
New call-to-action

Conclusion

The responsibility for the protection of cyber information in universities falls on the shoulders of the senior management and board members. However, it's the staff and students who use the institutional systems and networks every day. This creates a bit of a divide when it comes to ensuring complete cyber resilience.

It must be noted that understanding the universities' vulnerabilities, how these cyberattacks work, and how to stop these attacks is key to creating a more secure and stable future for higher education learning.

Prashant Shokeen(01213303118)

Further, higher education institutions should get continuous support from the government to critically build up their infrastructure, along with the necessary guidance and cybersecurity consultancy from external experts if required.

Another key to meeting future cybersecurity challenges, mentioned briefly in this article, is employing a robust, steady team of experts in the field. This is, of course, easier said than done, as university budgets are tight and talent is scarce. Still, there are several ways around this issue, including hiring virtual CISOs.

Though the cybersecurity challenges facing higher education institutions are great and the cost of solving them is steep, the potential financial and reputational risks that come with insufficient defence are likely even higher. Institutions across the higher education landscape will find that effective cybersecurity solutions can ultimately pay for themselves over the long term.