THOMPSON RIVERS UNIVERSITY | Integrated Planning & Effectiveness

envision TRU

Environmental Scan Series.6

Cybersecurity

Cybersecurity has topped the EDUCAUSE Top Ten IT Issues list for three years in a row.[1] As stated in Chapter 1 of the Envision TRU scan "*cybersecurity threats remain one of the most significant technological factors affecting higher education today*". Cybersecurity is frequently listed as one of the critical issues facing higher education institutions, and can impact financial, social, and operational sustainability.[2,3] This report will detail cybersecurity threats in higher education, their impact, and what institutions (including TRU) are doing to defend against these threats.

Cyber threats in the higher education sector

Higher education institutions are facing a rapidly-changing technological environment.[2,4] A massive volume of malicious cyber activities is targeted at higher education institutions on a daily basis.[5] In 2017, higher education institutions in the UK faced 400,000 new malware attacks every day.[6] Six percent (6%) of Canadian universities experienced cybersecurity incidents in the same year, which was the second highest level of incidents across all industries in this country.[7]

Cybersecurity incidents are increasingly aggressive and sophisticated.[8] The isolated hackers of the past have given way to advanced, well-organized, and state- affiliated attackers.[9] For example, one attack by nine Iranian government-affiliated hackers in March 2018 affected over 300 universities worldwide and exposed 31 terabytes of intellectual property.[10]

Many security experts believe that cybersecurity incidents are inevitable.[11] It is no longer a question of if incidents will happen, but when they will happen and what the impacts of such attacks will be.[11]

What make higher education institutions prime targets for cybercriminals?

According to Statistics Canada, banking institutions and universities are most likely to experience cybersecurity incidents.[12] Cybercriminals are targeting higher education institutions because of asset value, the decentralized structure of higher education, and the large and diverse user base.[4,11,13]

Glossary

Malware An abbreviated form of "malicious software." Software specifically designed to gain access to or damage a computer, usually without the knowledge of the owner.

Cybersecurity The state or process of protecting and recovering networks, devices, and programs from any type of cyberattack.

Cybercriminal An individual who commits cybercrimes and makes use of the computer either as a tool or as a target or as both.

Hack The action of performing activities on a computer system in an unauthorized manner; it is considered an infringement of protected data and property and thus constitutes a malicious act.

Breach Occurs when an intruder gains unauthorized access to an organization's protected systems and data.

Incident Any occurrence that threatens the confidentiality, integrity or availability of information. This might be the result of a cyber attack, perimeter breach or an insider threat (including policy violations).

Phishing A common online scam designed to trick the recipient into disclosing personal or financial information for the purpose of financial fraud or identity theft.

Select term to be directed to more information.

Cybersecurity

Institutions have a large amount of valuable data (e.g. personal information, financial data, and intellectual property) that are attractive to cybercriminals.[4,11,13] Research universities also house proprietary data from corporations and government agencies.[11] Cybercriminals are also interested in the advanced infrastructure of these institutions for the sheer computation capability they can use for malicious cyber activities; i.e. high-speed computers can be hacked and used as a platform for other cyber crimes.[13]

The decentralized structure of higher education institutions also makes them more susceptible to cyber incidents.[4,13] Institutions tend to house sensitive data in different locations (like the registrar's office, research departments, and labs) rather than one centralized hub.[4,13] The proliferation of connected devices on campuses also makes it hard to protect all entry points (laptops, smartphones, wireless devices, LAN networks, etc).[13] This decentralized structure makes it harder to ensure that all security protections and protocols are functioning, and may give cybercriminals opportunities to exploit these structural vulnerabilities for valuable data.[4]

There is also a human factor that contributes to the cyber security vulnerability of higher education.[13] Higher education institutions have a large and diverse population of users, including students and staff from around the world who bring with them various levels of technological expertise.[13] Many users do not enter academia with pre-existing cybersecurity awareness training.[13] Even if an institution has robust security measures in place, it could still be vulnerable because of the lack of cybersecurity awareness among users.[13]

Why does cybersecurity matter?

In addition to disrupting an institution's daily operations, cyber security incidents can have profound impacts on institutions and their students and staff. These include financial loss, reputational damage, loss of research and intellectual property, or even identity theft.[11,13] Cybersecurity is a business challenge that affects all areas of the institution (including marketing, advancement, human resources, IT, academic departments, recruitment, learning platforms, student support services etc.). [11]

The average cost of a data breach in the education sector in Canada is estimated at 4.3 million USD.[14] The average size of a data breach at a Canadian organization in 2017 was 21,750 records, and the average cost was 200 USD per compromised record in the education sector.[14] Costs include investigations, organizing and preparing response, and implementing call center procedures.[14] Additional financial losses include data recovery costs, ransom payments, and losses through fraud or theft.[13,15]

Apart from creating public embarrassment, cybersecurity incidents can damage an institution's reputation for intellectual security and jeopardize trust among stakeholders.[13] Corporations are less likely to partner with universities whose research data has been stolen. Donors may also lose confidence in the institution, resulting in fewer contributions.[13]

Apart from disrupting learning, cybersecurity incidents have other profound impacts on students and employees.[9] There are short-term inconveniences (such as changing passwords and needing to contact one's financial institutions) and there may be long-term consequences.[9] Identity thieves could use stolen personal information for credit card fraud and student loan fraud, the impacts of which could affect students' credit scores, disability tax credits, approvals for grants, etc.[9,16,17]

Recent incidents of stolen dissertations included the loss of all the raw data, research notes, drafts, and even completed chapters.[18,19] In these cases, the student victims may be granted extensions to redo the work.[20] The lasting effects of intellectual or identity theft could include program withdrawal (especially for students who do not have the financial resources to extend their studies), stress, depression, or even suicide.[21]

How prepared are higher education institutions for cybersecurity?

Until recently, higher education institutions were not well prepared for cybersecurity.[1,22] In 2018, education came last out of 17 industries in the U.S. in terms of cybersecurity.[22] In a recent UK survey, only 15% of IT and security staff in higher education scored their institutions 8 or above on a 10-point perception scale where 1 meant "Not at all well protected" and 10 meant "Very well protected".[23]

Educational institutions in the UK have acknowledged the risk of cyber threats and started to work on the issue.[23] Canada's McMaster University doubled the number of employees focused on cyber security from two to four to combat the growing wave of attacks in 2013.[5] The University of New Brunswick is approaching future systems and technologies with, "an eye to a seamless, highly integrated holistic security approach that will see tools transfer threat information to each other in order to take automated action".[24]

What can universities do to defend themselves against malicious cyber activities?

In the 2018 CUCCIO Cybersecurity Benchmarking Report, Canadian university cybersecurity experts suggest that institutions consider working on six areas to improve information security: phishing simulation; two factor authentication; deny by default firewall policy; vulnerability management; bring your own device controls; and providing sufficient financial and human resources to keep information security up to date.[25] The report also suggests a risk-based approach: "These recommendations do not represent all-encompassing security advice. Universities should adopt a cybersecurity framework such as NIST or ISO 27002 and measure their maturity against the framework. A risk-based approach is recommended".[25]

Cybersecurity is the responsibility of each student and employee.[15,26] Experts suggest that users should know what policies and procedures they need to follow, and that users should also be aware of the legal and financial consequences a breach could cause.[27,28] Cybersecurity training is one way to raise awareness within an institution.[28] User education is a cost-effective way to protect institutions against cyber threats.[28] Curation of access through role-based authorization and up-to-date access control also limits risk and makes investigations easier.[27]

Cybersecurity

Despite best efforts, cybersecurity incidents will occur, and institutions should have a plan in place for them to respond quickly and effectively.[28] The Society for College and University Planning suggest that it is vital for institutions to have sufficient resources to tackle the challenge of cybersecurity.[3] For instance, institutions will be susceptible to cyber threats if the data management infrastructure is outdated, or if departments are understaffed.[3] To that end, institutions should allocate a specific budget for cybersecurity investment.[29]

Cybersecurity at Thompson Rivers University

TRU has taken many of the six recommended steps above including continuous engagement for phishing, implementation of two factor authentication in high risk areas, a deny by default firewall policy, monthly vulnerability scanning and reporting, purchase of new technologies for bring your own device controls, increased funding of the Information Security Program, and use of an information security framework that incorporates both NIST and ISO 27000 for risk and gap analysis.[30] TRU also maintains both an Incident Response Plan and a Breach Protocol to allow rapid and effective response to incidents.[30]

Another crucial effort of the team is to raise awareness.[30] The Information Security Team offers both online and face-to-face mandatory information security awareness sessions that introduce key policies and procedures for new employees along with a variety of shorter engagements for staff, faculty, and students.[30] As a result, information security awareness is relatively high in the TRU community and the number of incidents that TRU has experienced have remained reasonably low.[30]

Like other higher education institutions, Thompson Rivers University (TRU) faces a large number of malicious cyber activities every day, one of the highest risk attacks being ‘phishing’.[30] TRU expanded its Information Security Team in 2018 to handle this increasing volume and sophistication of attacks, and the team keeps developing new procedures and tools to deal with emerging malicious cyber activities.[30]

The TRU Integrated Planning and Effectiveness team gratefully acknowledges the contribution of the TRU Information Technology Services information security team in preparing this report.

Visit tru.ca/envision/environmental-scans to read other chapters in this series.

Next in the Series

The next reports in the Envision TRU Environmental Scan series will focus on enrolment trends, Indigenous education, and the cost of education.

Environmental Scan Series.6

Cybersecurity

Sources

1. Grama, J., Vogel, V., Corn, M., & Pitt, S. (2018, January 29). The Third Time's the Charm? Information Security at the Top of the List Again. Retrieved May 8, 2019, from EDUCAUSE Review.
2. Society for College and University Planning. (2018). Implications of the External Environment: Fall 2018.
3. Society for College and University Planning. (2019). Implications of the External Environment: Spring 2019.
4. Vantage Technology Consulting Group. (2018, June 12). Should We Worry about Information Security in Higher Education? Retrieved May 8, 2019, Vantage Technology Consulting Group.
5. Andrew-Gee, E. (2013, September 22). Cyber attacks a growing problem for Canadian universities. Thestar.Com.
6. Horizons Group Members. (2019). Horizons report on emerging technologies and education.
7. Statistics Canada. (2018). Cyber security incidents experienced by industry and enterprise size (No. Table 22-10-0076-01).
8. Pérez-Peña, R. (2013, July 16). Universities Face a Rising Barrage of Cyberattacks. The New York Times, p. Page A1.
9. National Student Clearinghouse. (n.d.). Why Cybersecurity Matters: What Registrars, Enrollment Managers and Higher Education Should Do About It.
10. Cuthbertson, A. (2018, August 24). Iranian hackers attack UK universities to steal secret research. The Independent.
11. Dovey Fishman, T., Clark, C., & Lyn Grama, J. (February 22, 20118). Elevating cybersecurity on the higher education leadership agenda. Deloitte Center for Higher Excellence.
12. Statistics Canada. (2018). Cyber security incidents experienced by industry and enterprise size (No. Table 22-10-0076-01).
13. Cyber-Security in a University Setting: Materials to Assist Board Members and Senior Executives Provide Oversight on Cyber-Security Matters. (2016, December). Presented at the Canadian Association of University Business Officers.
14. IBM Security, Ponemon Institute. (2017). 2017 Cost of Data Breach Study: Global Overview [Research Report]. Ponemon Institute LLC.
15. National Student Clearinghouse. (n.d.). Why Cybersecurity Matters: What Registrars, Enrollment Managers and Higher Education Should Do About It.
16. Canada Revenue Agency. (2019, February 12). Disability tax credit [Service description].
17. Government of Canada. (2019, May 1). Education funding for people with disabilities [Navigation page - topic page].
18. Lewis, A. (2017, December 14). A PhD student has lost her thesis after thieves took her laptop and hard drives.
19. Jaschik, S. (2015, August 25). When Dissertation Materials Are Stolen. Inside Higher Ed.
20. Proctor, D. (2019, April 15). North-east student granted more time to complete dissertation following laptop theft. Press and Journal.
21. Grace Johansen, A. (n.d.). 4 Lasting Effects of Identity Theft. LifeLock.
22. Security Scorecard. (2018). 2018 Education Cybersecurity Report.
23. Chapman, J., Francis, J., & Harre, L. (2018, July). Cyber Security Posture Survey 2018 Research Findings.
24. Shipley, D. (2015, September 28). The Cyber Siege of Higher Education in North America. Retrieved May 8, 2019, from EDUCAUSE Review.
25. Canadian University Council of Chief Information Officers (CUCCIO). (2018). Executive Summary: 2018 CUCCIO Cybersecurity Benchmarking Report [Executive Summary].
26. Simeone, S. (2016, October). The 3 R's of a Cybersecure Business Culture. Retrieved May 8, 2019, from Healthcare Insights hc1.com.
27. Readiness and Emergency Management for Schools (REMS) TA Center. (n.d.). Cybersecurity Considerations for Institutions of Higher Education [Fact Sheet].
28. Cyber-Security in Higher Education: Mobilizing to Respond Highlights from the CAUBO/CUCCIO Workshop held in Montreal, November 30 and December 1, 2017 [Highlights]. (n.d.).
29. Society for College and University Planning. (2019). Implications of the External Environment: Spring 2019.
30. Burley, H. (2019, May 8). CyberSecurity Topical Briefing Note.