Deloitte.

Cybersecurity and privacy impacts on higher education in Canada

How will your institution recover from the pandemic and thrive well into the future?

Contents

Higher education in times of a global pandemic COVID-19

The COVID-19 pandemic has caused widespread uncertainty and presented numerous pressing and complex challenges across the higher-education sector. It will continue to do so for some time to come. Colleges and universities have had to respond quickly to a number of urgent educational issues, including expanding remote delivery—i.e., adapting in-class course instruction to the virtual sphere—and online learning, determining strategies for marking and graduation, and providing additional support to students through wellness programs. This has fast become our new normal in a COVID-19 world.

As part of our commitment to this scholastic sector, Deloitte published earlier this year the report *Planning for the impact of COVID-19 on higher education in Canada*. It outlined the firm's framework of **Respond–Recover–Thrive**, which offers a three-dimensional view on crisis management. This paper focuses on cybersecurity and privacy concerns, clarifying a series of what we believe to be critical considerations during what has proven a highly fluid situation.

Although these **cybersecurity and privacy concerns** may not previously have been top of mind, we feel the focus now needs to shift toward them because:

- The pandemic has resulted in an **unanticipated yet substantial increase in remote working**, with students and employees logging in from personal laptops and unsecured networks.
- **Threat actors** have been **abusing** the COVID-19 environment, increasing attacks on employees and students in the remote-work and learning
- **Researchers continue to be targeted**. At some institutions,[1] COVID-19 researchers are being exploited by means of sophisticated phishing emails, which can spread ransomware and otherwise disrupt research activity.
- There may be inadequate protection of an institution's **crown jewels** (i.e., its key systems and data).
- **New applications** continue to be introduced during the pandemic to facilitate remote-working conditions; they did not undergo the same rigorous privacy tests that would have been required before the pandemic.

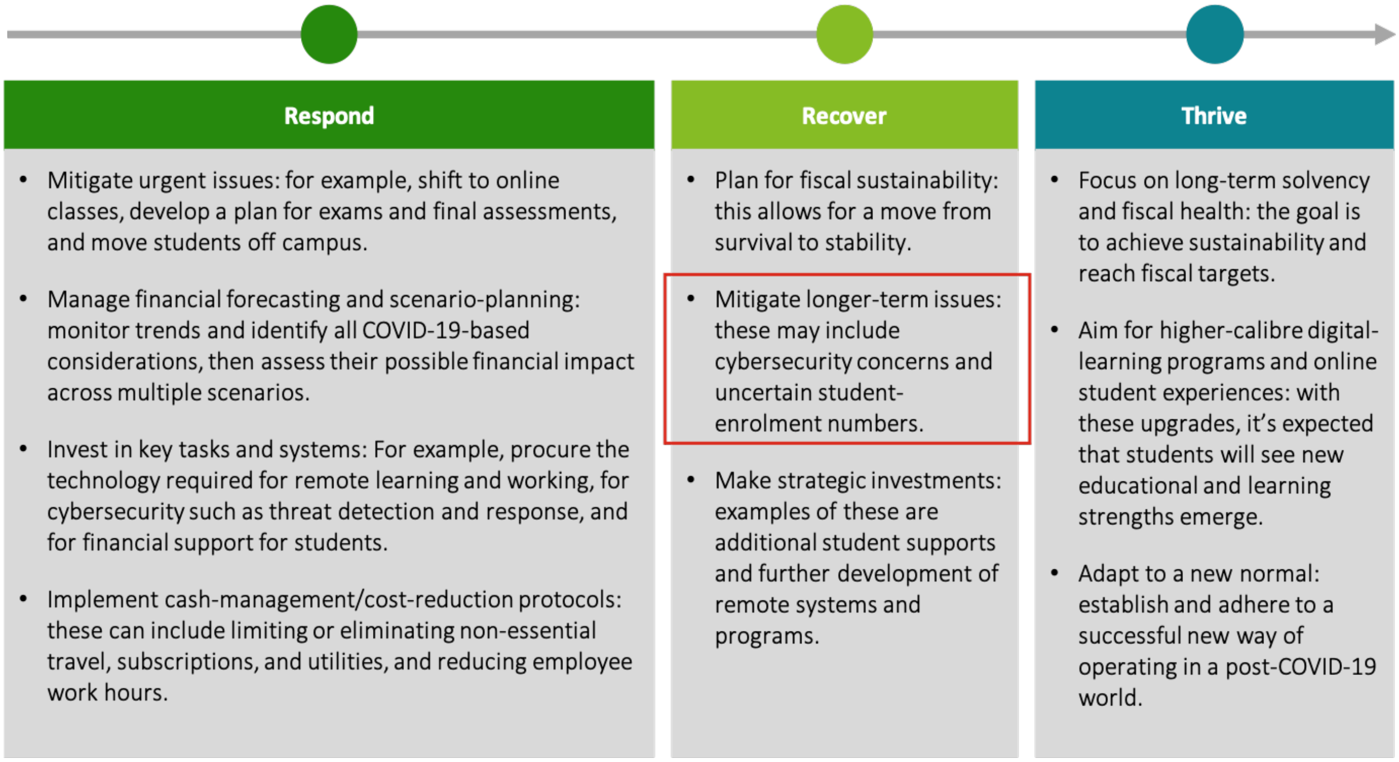
Given the sensitivity of data that exists in a higher-education environment, and as we begin to imagine what a return to work may look like, it's important to focus on such cybersecurity and privacy considerations in order to continue to move forward securely. The return to the c**lassroom, the lab, and the office will likely take place in phases, with the number of students and employees who are on campus only gradually increasing**. This will provide higher-education institutions with an opportunity to implement additional controls while continuing to monitor existing regulations.

[1]. "Caution: Cyber security campaign targeting COVID-19 researchers," Research Alerts, University of Guelph, https://www.uoguelph.ca/research/alerts/content/caution-cyber-security-campaign-targeting-covid-19-researchers

A framework for crisis management

Our **Respond-Recover-Thrive** framework offers a three-dimensional view on crisis management over time. Educational institutions are currently in the midst of the respond phase and have done much work to mitigate urgent issues. As they prepare to shift their efforts to the recover phase, it will be important for them to focus on longer-term implications and for this planning to be well positioned for a return to work.

The purpose of this paper is to assist institutions in the Recover phase of the crisis and specifically about longer-term concerns related to cybersecurity and privacy (see the relevant step in the table below, identified with a red rectangle).



Respond	Recover	Thrive
• Mitigate urgent issues: for example, shift to online classes, develop a plan for exams and final assessments, and move students off campus. • Manage financial forecasting and scenario-planning: monitor trends and identify all COVID-19-based considerations, then assess their possible financial impact across multiple scenarios. • Invest in key tasks and systems: For example, procure the technology required for remote learning and working, for cybersecurity such as threat detection and response, and for financial support for students. • Implement cash-management/cost-reduction protocols: these can include limiting or eliminating non-essential travel, subscriptions, and utilities, and reducing employee work hours.	• Plan for fiscal sustainability: this allows for a move from survival to stability. • Mitigate longer-term issues: these may include cybersecurity concerns and uncertain student-enrolment numbers. • Make strategic investments: examples of these are additional student supports and further development of remote systems and programs.	• Focus on long-term solvency and fiscal health: the goal is to achieve sustainability and reach fiscal targets. • Aim for higher-calibre digital-learning programs and online student experiences: with these upgrades, it's expected that students will see new educational and learning strengths emerge. • Adapt to a new normal: establish and adhere to a successful new way of operating in a post-COVID-19 world.

Key factors and uncertainties for institutions to consider

During this unpredictable time, the **speed** and **agility** with which institutions address concerns is essential; it's not the time for striving for perfection and focusing on details. In a typical higher-education environment, key factors driving the changes required in the Recover phase include:

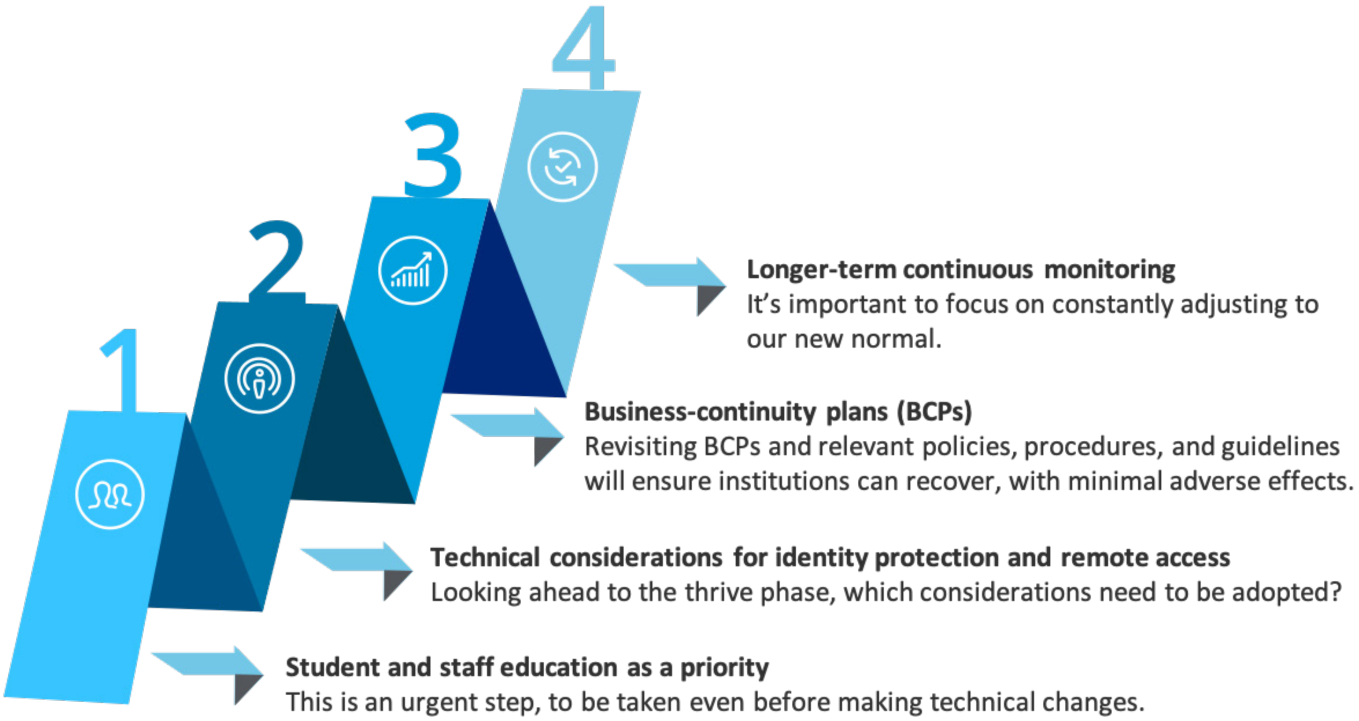
1. **Crown jewels**: It’s important to determine which crown jewels (i.e., the institution’s mission-critical assets) are most affected by the pandemic, as well as how to quickly address any related cybersecurity and privacy concerns. For example, if international students have remote access to schools and courses, what are the risks to be considered? Will security measures preclude geo-location-based login filtering?

2. **Decentralized operations**: How are institutions dealing with the highly decentralized nature of faculties and data ownership

- In many scenarios, for example, it’s the researcher who owns/controls rights to the research. Is that data being stored on a secure server maintained by a centralized IT group, or is it being stored on the researcher’s computer?
- Were the changes that were quickly adopted at the onset of the pandemic to facilitate virtual learning and other required tasks vetted with the relevant unions and labour-relation groups?

3. **Policy/procedure/contractual impacts**: Higher-education institutions quickly implemented remote-working systems in the last year. Is it now time to consider the impact on policies and procedures and on the business-continuity plan (BCP) Has the appropriate stakeholder management been completed (e.g., labour-relation groups, collective-bargaining agreements)?

Summarized below and further detailed on pages 5–9 are **four tactical considerations** and recommendations that we believe should be assessed along with the concerns noted above:



Longer-term continuous monitoring
It’s important to focus on constantly adjusting to our new normal.

Business-continuity plans (BCPs)
Revisiting BCPs and relevant policies, procedures, and guidelines will ensure institutions can recover, with minimal adverse effects.

Technical considerations for identity protection and remote access
Looking ahead to the thrive phase, which considerations need to be adopted?

Student and staff education as a priority
This is an urgent step, to be taken even before making technical changes.

1. Prioritize student and staff education

With a large remote workforce and student population, the increase in potential cybersecurity threat vectors is quite significant. Since the chief implication of this shift to remote access is that both employees and students are now conducting activities from often unsecured and unmonitored home Wi-Fi networks, there's likely to be greater exposure to phishing and network attacks. The following key actions regarding these users are recommended for immediate implementation:

- Assist users with **basic home-network hygiene**, such as providing best practices to divide their home networks into private and business segments and to restrict their use of public or unsecured Wi-Fi networks without proper encryption.
- Ensure that **default router passwords** are changed in users' home Wi-Fi networks and strongly secured.
- Educate users about avoiding **commonly chosen and dictionary-entry passwords**.
- Inform users about social-engineering scams and COVID-19 phishing campaigns, and teach them to identify and avoid these. For students, it might be worthwhile to undertake these info and training sessions within the **first five minutes of a class.** Use tool kits such as those offered by the security-research and education organization SANS (see bullet points below)—which recommend **relying on people rather than technology** in order to avoid social-engineering scams—using a password manager, and, for employees, limiting devices to either work or leisure use.
  - SANS security awareness work-from-home deployment kit
  - SANS learning management platform and phishing
- Educate users about **securing physical access** to their devices to avoid theft of their devices, and therefore their universities' data.
- Educate users about their institutions' remote **cybersecurity policies** and best practices—in particular, those regarding remote-access protocols, personal-device use, password and authentication guidelines, and privileged-access control.

2. Focus on recovering from the technical impact of COVID-19

As higher-education institutions quickly pivoted to function in the new normal, in some cases, decisions may have been made to facilitate the ease and speed of operations. In order to identify these instances, it's recommended to conduct quick **risk-assessments of distance-learning computing set-ups**, such as how and from which devices users (i.e., students and employees) connect to an institution's portals. It's further advised that these and other **risk acceptances** be documented and formally logged.

As users shift to **connecting from home,** it can be difficult for IT teams to **enforce and maintain tight security controls.** Since network traffic monitoring is not generally an option with centrally managed corporate networks that have remote users, security policies and monitoring should focus on the following basics, which will help ensure your crown jewels are protected. Note these considerations must be flexible enough to adapt to the highly decentralized nature of many higher-education institutions.

- **Identity protection**: Ensure that remote users of online learning portals undergo multifactorial validation and verification procedures, including:
  - **Strong password policies.** These should be sufficiently complex, with expiry standards aligned with those of the institution.
  - **Limited failed login attempts.** A specific number of attempts should be set before a user is temporarily locked out.
  - **Two-factor authentication (2FA) or multi-factor authentication (MFA).** Consider the enrolment of students into the 2FA or MFA solution, if available, along with the impact on the remote workforce. Will more help-desk staff be available virtually to assist students during these enrolment periods?
  - **Geo-location-based login filtering.** Note this option may not always be available.
- **Remote-access options: Use secure networks.** Consider a virtual private network (VPN) or a remote desktop protocol (RDP) gateway (over the more vulnerable hypertext transfer protocol secure, or HTTPS, system) for a university network. Secure networks are more important than ever, given the varied way in which users connect to work and study remotely.
  - Wherever possible, ensure that users have to log in to VPN to access the university portal; this adds a layer of protection, given users often connect via non-secure home networks.
  - Provide detailed instructions to ensure students download VPN from an institution's approved website in order to avoid viruses, malware, and other system-wide breaches that can result from applications obtained from unauthorized sites.
  - Consider the impact of these new ways of working with the relevant labour-relation groups.
- **Conduct third-party risk assessments.** Communicate with your Software-as-a-Service (SaaS) application providers and inquire about their business-continuity plans.
- **Confirm licensing.** Consider the costs for new Voice-over-Internet Protocol (VoIP) services, additional Web-conferencing-services licenses, and/or added VPN capacity to accommodate the influx of remote users.
- **Other technical considerations:**
  - Have security teams review and establish **firewall rules** for remote access, user execution and behaviour analytics (UEBA), file-integrity monitoring, and anti-malware and intrusion prevention. Security gaps should be assessed and countermeasures put in place as quickly as possible.
  - **Examine all** remote-access services and devices for both firmware and security-patch updates. Close any unneeded ports and investigate traffic on non-standard ports.

  - Ensure tools and applications/systems used through the IT landscape, including VPN, are **fully patched** (i.e., vulnerabilities removed and/or systems updated).
  - **Revisit the process of approving/denying user access based** on the reasons for access, as well as on the length and frequency of the access request.
  - Maintain **consistent and stringent audit and compliance requirements** during a user's remote-access period. Organizations should be keen to capture and document all remote-session activity and credential usage in order to meet system-compliance requirements and facilitate any future forensic analyses.

3. Revisit business-continuity plans and relevant security and privacy policies, procedures, and guidelines

Given the changeable environment in which colleges and universities are now operating, and considering the level of agility that's required in each key task, it's important to revisit the following typical strategic-guidance tips, which are meant to shepherd organizations during such variable times. Remember, given the current reality, these tasks shouldn't take months, but rather should be quick exercises:

- **Revisit and revamp existing protocols:**
  - Review and prioritize current security policies, procedures, and guidelines to ensure they can account for students' increasing shift to distance learning. These protocols should address factors such as remote-access management, personal-device use, updated data-privacy considerations for access to documents and other information, and increased use of shadow IT (i.e., programs that are not managed or overseen by the institution's IT department) and cloud technology.
  - Ensure an institution's security and privacy policies, procedures, and guidelines **allow visibility** into SaaS collaboration and chat services such as Zoom (used frequently for virtual learning), Google Meet, Cisco Webex, Google Classroom, Slack, and Microsoft Teams, which users (i.e., students and professors/instructors) have adapted to during the current global reality. This also applies to data ownership and the tools used to facilitate it (see Decentralized operations on page 4 of this document).
  - Define and continue to assess systems and strategies that adhere to privacy, security, and ethics guidelines for distance-learning users.
  - Have ongoing discussions and consult with administrators, instructors, and student groups on privacy and security implications related to virtual learning as this information becomes available. Questions to ask during these meetings can include:
    - Is personally identifiable information (PII) and/or protected health information (PHI) being captured when a student uses such products/platforms? If so, this may constitute a violation of Canadian privacy regulations such as the Freedom of Information and Protection of Privacy Act **(FIPPA)** and/or the Personal Health Information Protection Act **(PHIPA)** and may lead to personal data being treated as marketable and/or resold.
    - Is the institution acting alone or has it opted into a consortium—e.g., Ontario's research-and-education ORION system, British Columbia's higher-education shared-services network BCNET—to oversee appropriate vendor-privacy practices?
    - Update protocols to address any issues identified during ongoing system reviews.

- **Update BCPs and disaster-recovery plans (DRPs):**
  - Update an institution's BCP to account for remote learning. Use **tested and proven** continuity procedures, including DRPs, to avoid service disruptions and maintain operations. Assess the institution's needs with questions such as the following:
    - Are your crown jewels identified appropriately within your business continuity/ disaster-recovery plans and procedures?
    - Have your crown jewels changed since the last review and/or update?
    - Review BCPs to ensure they support **secure remote classes**. This assessment should include whether students can securely access required network resources from home, and should consider methods for secure file-sharing between students and teachers.
    - Develop a plan and a playbook to address cybersecurity breaches (e.g., crisis-management and data-breach plans), and which include all key stakeholders, such as the school's faculty and other instructors, as well as new **distance-learning-use cases.**
    - Conduct a **remote-work-tabletop exercise** with administrators and faculty heads. Take inventory of the institution's current business applications and identify crown-jewel (i.e., mission-critical) systems.
    - Update security policies to address **increased remote connectivity**, with a stronger focus on data privacy and on intrusion-detection across a now larger number of entry points.

4. Longer-term continuous monitoring

As we adjust to the new normal, institutions need to guide and monitor how students and employees continue to collaborate remotely. In addition to the previous recommendations, the following initiatives can help us return to normality as we return to work:

- Ensure **continuous monitoring and inspection** of internal IT assets while automating log-correlation-and-analysis to detect anomalous behaviors. Can these be viewed through a virtual security-operations centre as physical access to buildings continues to be restricted access?

- Monitor and review critical-applications logs for unusual activity and data-leakage/theft points— including VPN sessions and applications such as Office 365 in these evaluations. This is particularly relevant for systems that contain **PII** and **PHI,** including video-conferencing tools that allow for virtual learning. Note that compliance with regulatory data-protection and privacy requirements, such as those outlined in FIPPA and PHIPA, extend to our current pandemic-related situation.

- Monitor and investigate **data-loss prevention (DLP)** and data-leakage alerts.

- Review and test the **detection and response** capabilities of security tools, and assess these programs' abilities to respond to remote access, regardless of where a user is located.

- Provide security analysts with the tools and permissions to offer remote incident-response (IR) and threat-assessment support—that is, equip them to remotely detect, contain, and further prevent cybersecurity breaches. These tools and permissions can include:
  - Access to logs and security data on the central network
  - Access to the institution's network (e.g., a VPN, HTTPS, or RDP system)
  - Access to home-office laptops and/or bring-your-own-device (BYOD) software or hardware
  - Administrator credentials, such as those provided by service accounts (i.e., accounts with special privileges beyond those granted to other users), *sudo* Linux accounts (i.e., those that allow access to restricted files and operations), and *ssh* keys (which allow for secure access to a system without requiring a password)
  - Antivirus white-listing instructions for any forensic and IR tools that might be used (i.e., to ensure the antivirus program recognizes a security analyst's assessment programs as safe, versus as possible threats to the system)

Top tips for guarding against a cyberattack during online learning

Cyberattacks can increasingly take a toll on the finances and reputations of higher-education institutions—especially during this time of COVID-19, when these establishments can least afford losses. Therefore, users—e.g., administrators, students, and employees—must act now to help prevent these breaches.

While business as usual may no longer be possible nor attainable in these disruptive times, higher education as an institution now has an opportunity to consider the major risks of disruptions to society as a whole—i.e., cyber-breaches and compromised personal data that may result from remote access to and/or from non-secure computer systems—as well as the far-reaching implications of these changes. The **Respond–Recover–Thrive** framework allows for institutions to evolve during times of unprecedented change until a new-normal plateau is reached. As part of our dedication to this sector, we commit to continue sharing our views and recommendations based on our crisis-management framework.

Contacts

Daisy Vora
Partner, Risk Advisory
dvora@deloitte.ca

Aneesa Ruffudeen
Director, Risk Advisory
aruffudeen@deloitte.ca

Acknowledgements

Mark DiNello
Partner, Consulting
National Leader, Higher Education

Bruce Adams
Director, Consulting

Craig Robinson
Director, Consulting

Jamie Lanoue
Partner, Cyber and Strategic Risk

Noemi Chanda
Senior Manager, Cyber and Strategic Risk

Trimaan Dang
Manager, Cyber and Strategic Risk

Surbhi Purwar
Manager, Cyber and Strategic Risk

Deloitte.

Disclaimer

This publication contains general information only and Deloitte is not, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor. Deloitte shall not be responsible for any loss sustained by any person who relies on this publication.

www.deloitte.ca

About Deloitte

Deloitte provides audit and assurance, consulting, financial advisory, risk advisory, tax, and related services to public and private clients spanning multiple industries. Deloitte serves four out of five Fortune Global 500® companies through a globally connected network of member firms in more than 150 countries and territories bringing world-class capabilities, insights, and service to address clients' most complex business challenges. Deloitte LLP, an Ontario limited liability partnership, is the Canadian member firm of Deloitte Touche Tohmatsu Limited. Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee, and its network of member firms, each of which is a legally separate and independent entity. Please see www.deloitte.com/about for a detailed description of the legal structure of Deloitte Touche Tohmatsu Limited and its member firms.

Our global Purpose is making an impact that matters. At Deloitte Canada, that translates into building a better future by accelerating and expanding access to knowledge. We believe we can achieve this Purpose by living our Shared Values to lead the way, serve with integrity, take care of each other, foster inclusion, and collaborate for measurable impact.

To learn more about Deloitte's approximately 330,000 professionals, over 11,000 of whom are part of the Canadian firm, please connect with us on LinkedIn, Twitter, Instagram, or Facebook.