Cyber-Security in Higher Education: Mobilizing to Respond

Highlights from the CAUBO/CUCCIO Workshop held in Montreal, November 30 and December 1, 2017

More than 120 members from over 50 institutions participated in this interactive workshop featuring speakers from the legal, security, and communications fields as well as case studies presented by institutions who have experienced cyber-security breaches. The workshop was organized around the premise that the main question is no longer if your institution will be faced with a breach -it will-, but whether it is ready to respond effectively when it does. As attested by the diverse make-up of the workshop participants interested in this issue, cybersecurity is not just an IT issue, but an institutional one thus responding to breaches demands an institutional effort.

Here are five main takeaways from the workshop. We hope these will be helpful as your institution plans and implements its response plan.

1. **Education and awareness is one of the best and most cost effective way to protect your institution against intentional and unintentional data breaches**

The main types of cyber-threats include phishing (spoof emails designed to fool you into providing data), spear phishing (using an infected attachment to gain access to your systems), malware (predatory software that installs itself on your computer or network), and ransomware (locks your computer and requires you to pay a ransom to regain access). Personal information and research data are the targets.

Phishing attempts are the doorway through which most cyber-attacks take place, so it is important to be able to detect it successfully. Report all phishing attempts, so others in your organization are made aware of the threat. Internal security breaches are generally accidental, not malicious, but the effect is just as devastating.

Mandatory training is essential to promote fraud awareness and IT security. User education and awareness is the most cost effective and impactful solution to preventing breaches. In many instances, existing resources, techniques and strategies can be leveraged. User education and awareness has been found to reduce the overall click-open rate on phishing emails by half (currently 41 per cent of phishing email attempts are successful). Education, training and awareness of cybercrime, how it is executed and its impact on institutions should be constantly reinforced by sharing current and real and through targeting all members of the institutional community (i.e. faculty, staff and students).
Phishing simulations can be used effectively as training, if framed correctly and positively to help people become proficient at identifying threats. It is important not to shame individuals who click on these fake emails. Rather, educate entire teams without naming names, and encourage people to share successes.

Promote a security mindset across the institution to effectively deal with cybercrime. Senior leadership should spearhead this effort to ensure staff are aware that security is everyone’s responsibility.

2. Respond quickly and effectively to a breach: Have a plan and be ready to execute it

Being prepared and building the right team is essential to a quick, competent response. Despite best efforts, breaches will happen. The results will be much more costly if your institution does not have a response plan in place. Some universities use their emergency operations group to respond to a breach, but a business continuity group may make more sense, depending on your organizational structure.

Consider signing contracts with third-party consultants (cyber-forensics specialists, lawyers, insurance providers) in advance if you have concerns about your capacity to respond to a breach internally. Among others, many institutions retain the services of a lawyer to act as their “breach coach.”

Run tabletop exercises regularly to ensure your plan works well and adapt as needed. In addition, IT staff can also run technical tests (i.e. penetration tests, network scans, etc.), perform risk assessments (both external and internal) and maintain an organization-wide threat catalogue to help ensure an effective response.

Communications require more than a spokesperson. As part of your response plan, template messages can be created ahead of time so that communications staff can react appropriately and quickly in a breach situation. Create appropriate messages for each stakeholder group to avoid information overload and communications errors. In the event of a breach, the first message sent should be notification to those affected.

3. You need a policy, but you also need guidelines, procedures, and metrics.

Your institution needs policies about data use, computer and network use, and so forth to combat cybercrime. However, having a policy in place without the necessary guidance to support the policy, actually establishes liability. Guidelines, procedures, and controls should also be in place to support those policies.

Use a collaborative process to develop the policy. It is a challenge to create a workable policy and get buy-in from staff and faculty. A good relationship between administration and unions is essential. Everyone needs to understand why structures are being put into place and how they will protect the institution. Bring them into discussions rather than simply informing them of the end results.
Higher education's data security needs and norms are industry-specific. Institutions need to be responsive to stakeholder needs while safely managing access to data. University culture promotes open access to information, but limitations are still required. Framing it as the need to ensure privacy, rather than data protection, may help faculty understand the aims of cyber-security policies.

Get the correct governance structures into place. This is instrumental to creating and enforcing policies, protocols, and guidelines. One option is a cyber-security council with representation from areas such as audit, IT, legal, the CIO's office, staff relations, campus police, etc.

Consider asking departments to create guidelines, standards, and procedures in support of your policy. You want to make it easy for people to get it right, so the standards should be relevant to what they do.

Measure and track how things are going, and set goals for future achievement. This data will help show your Board and leadership where progress is being made and where further work may be needed. Examples of metrics include number of incidents, threat levels of those incidents, and types of risk. Metrics can also be used to demonstrate the need for policies and procedures in the first place.

4. **Legal liability is a major concern: Integrate your legal team into all cyber-security measures and plans**

Do your due diligence. The law does not expect perfection, and a cyber-security breach does not equal liability. However, an institution will be evaluated based on its response to the breach, including what necessary prevention measures were in place.

Use solicitor-client privilege to protect your institution. Universities are advised to involve their legal team (internal and external) in their breach response process so that related documents are protected under solicitor-client privilege. Communications must be explicitly for the purpose of seeking legal advice about response to the breach. However, institutions must also be careful not to claim privilege for a document that must be generated for other purposes or manufacture privilege claims after the fact.

Commission any reports or studies on cyber-security specifically for your legal team, rather than for the IT department or senior leadership. This will privilege the document so that, in the event of litigation, any recommendations that were not implemented cannot be cited as evidence of liability.

Regularly dispose of old or unnecessary data, in order to decrease the number of people affected by a breach. Electronic records fall under the same retention guidelines as paper records.

Determine who must be notified and do so as quickly as possible, then conduct a full investigation. The timing of a breach response may be scrutinized by authorities. Effective preparation and response (such as prompt and comprehensive notification notices) can help avoid or mitigate liability, while a poor response can lead to additional liability or punitive damage awards by the courts.
Keep an eye on litigation trends. There is a growing body of individual-plaintiff court cases where people affected by a breach have successfully sued and been compensated for damages (awards in the low thousands of dollars). This has led to a wave of class-action suits, though none has gone to trial and may never do so. Remember, if a breach is addressed quickly and effectively, it can drastically reduce the risk of litigation.

A breach can damage your institution’s reputation. Educate and remind staff and faculty not to discuss a breach via email, text, or social media, and to follow prescribed response processes. Provide correct and timely information to avoid the spread of rumors.

In Canada, no entity is currently obligated to disclose a breach and may not even be required to inform the affected persons. Revisions to PIPEDA will change this for the private sector next spring. Although universities are not affected, there are many valid legal reasons to notify people of a breach, including the court of public opinion. In the long run, it may be better for an institution’s reputation to disclose.

A liability to-do list:

- Create, update, and test an incident response plan before you need it
- Review privacy policies and consent forms for anything that looks like a promise to keep data safe, as this may lead to liability
- Review vendor and partner contracts to determine what the consequences will be in the event of a breach on either side
- Put risk transfer measures such as contracts and cyber-insurance into place
- Ensure your policies and procedures meet legal standards; this is a moving target, so be vigilant
- Set up protocols regarding legal role (privilege) in vendor contracts, cyber-security assessments, and incident response plans
- Meet privacy requirements
- Purge information that is no longer needed

5. Universities find it challenging to share information about cyber-crime, but there are many benefits to doing so, if done correctly and safely.

Cyber-incidents are a “public health risk” to universities, which have many common systems, services, and practices. A threat to one is a significant probability at others. This speaks strongly to the need for mutual communication and disclosure, but institutional culture makes many universities wary.

Sharing information helps institutions assess the efficacy of their processes, re-assess threats, and ensure effective IT practices are in place, but university administrators must be convinced that the benefits outweigh any potential liability or reputational issues.
Cultivate trusted networks and communities, which provide an increased level of comfort and a recognition of the context in which such information exists. The CUCCIO IT and IS Security Special Interest Group (SIG) and the CIO group are two existing communities where information-sharing is already taking place.

A version of the Traffic Light Protocol has been proposed by the Security SIG to share information about cyber-security threats and breaches. A designation of red (for recipient’s eyes only), amber (share on a need-to-know basis), green (share among institutional members), or white (share publicly) is attached to information shared with another group member. This protocol is currently being used by the SIG.

Information can be shared by modes other than email so as to leave no paper trail in the event of litigation. Any information shared in recorded formats should be carefully worded to avoid liability. On-boarding for those new to the protocol has also been suggested.

As a collective, universities must try to change their mindset that cyber-incident information is proprietary and should never be shared. Our institutions are being studied and that information is being shared by criminals; by not sharing with one another, we do ourselves a disadvantage.

Sharing information among institutions can promote more effective preparation, prevention, and response to cyber-security breaches. There is a need to shift away from the current mindset at many universities that such information should remain confidential, towards a culture of trust and interchange within the higher education community.
Appendix A: Cyber-Security Report Excerpt

The following presents eleven “best practices” that institutions should consider when defining their cyber-security plans. This list of best practices is not intended to be prescriptive (i.e. exactly what institutions should follow) nor comprehensive (i.e. do them all and you’ll be OK), rather these are eleven areas that deserve consideration.

4.1 INSIST UPON A FORMAL WRITTEN CYBER-SECURITY PLAN

Using the cyber-security framework presented in section 3, Executives should insist upon a written cyber-security plan that addresses the four pillars (Preparation, Prevention, Response, and Improvement) with consideration given to each of the three dimensions (People, Practices, Resources). This plan should be reviewed, discussed, and understood by the board. It should then be updated regularly and discussed at the Board level, quarterly or at least semi-annually.

The plan should have measures (see 4.7) that can be tracked over time to denote progress or lack thereof.

4.2 CYBER-SECURITY GOVERNANCE: BE PROACTIVE AND HOLD REGULAR FORMAL REVIEWS

In many cases Canadian higher education cyber-security is delegated to the Audit Committee and resides within the purview of a single “C” level university executive (typically the VP Finance and Administration). This report argues that such responsibility should not be fully delegated and that both full Board and full Executive groups need to be involved on a regular basis.

As noted, cyber-risks evolve much more quickly than other risks thereby requiring continuing attention, re-calibration and investment. In this rapidly evolving threat landscape, institutions need to keep cyber-security on the Executive’s radar on a continual basis.

While cyber-security may not advance the mission of higher education it can certainly impede it by draining resources. If cyber-security is fully delegated it may suffer from trade-offs made when planning and budgeting decisions are made by those not exposed to dangers of cyber-security failures. Therefore, best practices suggest that the full Board and Executive group receive at least annual cyber-security education and consider conducting “table-top” exercises simulating cyber-breaches and how the institution might make decisions regarding paying ransom to recover data, who/when to notify people regarding the loss of personnel data, what should be the institution’s stance from a public relations perspective, etc. These and other questions belong to the full Board and Executive group.

Regular, frequent reporting on cyber-security is strongly recommended. The following suggestions are presented for consideration:

- present quarterly update reports to Board or Board Committee and separately to the Executive group
- make cyber-security a standing item on the Executive agenda where immediate issues are brought to Executive attention
- present semi-annual or annual cyber-security education sessions to the full Board outlining the current and emerging trends
- involve Internal Audit and Risk Management when cyber-security is discussed within senior groups.

Appendix “C” presents some topics that should be included in regular cyber-security reports to Board Members and Executives.

Material breaches would be reported to the Executive group and, as appropriate, to the Board immediately upon occurrence.
4.3 EDUCATING USERS AND TRANSFORMING CULTURE

Improving end-user IT practices may be the single least expensive, and most cost-effective, step a University can take to improve cyber-security. This is because credential theft (e.g., userids/passwords stolen in Phishing attacks) account for a majority of breaches. What is needed is a means to shift culture in user practices over time – from too wide-open to more disciplined and security conscious. However, as noted in Section 1, end-user training does not eliminate the risk of careless handling of phishing attempts.

Institutions should consider some or all of the following:

- Annual mandatory user education\(^\dagger\) e.g. an online course with questions that some/all users must take. Follow-up and compliance enforcement are necessary to ensure people not only take the course, but also remediate incorrect answers to questions.
- Planned Phishing attacks with immediate user feedback that demonstrates inappropriate behaviour.
- Two factor authentication\(^\ddagger\) – some estimates suggest that this eliminates the majority (>80%) of credential loss/theft.

The above techniques may be viewed as overly intrusive and hence may require introduction over time. Executive support is needed to introduce such programs and ensure compliance.

4.4 A COMPREHENSIVE RISK ASSESSMENT PROGRAM AND INVOLVEMENT OF INTERNAL AUDIT/RISK MANAGEMENT (IA/RM)

One of the key pieces in the Preparation pillar is the use of a formal, comprehensive Threat/Risk Assessment of the Institution’s exposure to cyber-risks, potential consequences (financial, reputational, liability, etc.) from cyber-crime and their likelihood of occurrence. Internal Auditors and/or Risk Management personnel should be intimately involved in assessing cyber-threats and risks.

When preparing a threat/risk assessment the Institution’s data and other assets must be classified and treated accordingly. The concept of data stewardship should be considered so the “owners” of different datasets (student information, financial information, sensitive research data, etc.) are charged with the responsibility to manage data access and provide input to security measures.

Some Canadian institutions\(^\dagger\) already practice comprehensive Threat/Risk Assessments of cyber-risk. As such, readily available templates, processes, etc. can be shared without disclosing confidential information.

4.5 CONSIDER HAVING IT SKILLS ON BOARD, JUST LIKE FINANCIAL, LEGAL AND HR ACUMEN

Having one, or better several, people on the University Board (and/or Audit Committee) with IT backgrounds/skills is recommended. Best practice dictates that this should be a mandatory component of the board skills/matrix.

If such expertise is not on the Board, consider retaining an IT/cyber-security advisor to attend Board/Committee/Executive meetings when cyber-security is reported. This advisor should review material before the meeting and help prepare the members to respond to the material presented.

---

\(^\dagger\) Mandatory user education programs are already in use at some institutions.

\(^\ddagger\) Two-factor authentication is a method of computer access control in which a user is only granted access after successfully presenting two separate pieces of evidence to an authentication mechanism – for example a password and fingerprint combination or a password and dynamically changing random number from a token or mobile phone combination.
4.6 SHARED SERVICES/OUTSOURCING AND COMMUNITY SHARING: YOU CAN’T DO IT ALONE

SHARED SERVICES/OUTSOURCING
Given the increasing virulence and sophistication of cyber-attacks it is unlikely that any institution, especially smaller ones, can provide adequate cyber-security totally in-house. The list of major organizations (see section 1.1) that have been hacked clearly demonstrates the difficulties in protecting organizational assets and data. Universities face the same issues and, per section 1.3, being attractive targets they must expect regular cyber-attacks. Keeping data in-house, protected by a small IT staff, is extremely risky when there are better alternatives.

Cloud service providers, such as Microsoft, Amazon, Google, Dropbox and others, invest millions in cyber-security and therefore using services and placing data with these suppliers should be considered a “best practice.” Cloud services, for eMail, ERP systems (student/faculty/staff records, financial information, etc.), eLearning data and research data are all available and usually cost less than running in-house equipment when IT staff costs and overheads are included. None of these are differentiating activities, yet they often consume the bulk of the IT budget, staff time, and management attention. In addition to the security benefits, selective outsourcing can improve business continuity, reduce the time needed to introduce a new system or service, and release IT staff to work on the differentiating, mission-based requirements that are unique to the institution.

There are a host of services that institutions could “outsource” to existing consortia such as CANARIE, Regional Area Networks, Merlin (Manitoba), ECN (NB & PEI), etc. for more specialized higher education needs or simply to “keep it in the family.” At present these sharing organizations generally lack the scale to be truly effective in the cyber-security realm, although they do an excellent job within their current mandates. Hence, they could be a platform upon which to build a shared cyber-security capacity and develop the expertise that could be shared by multiple institutions. For example:

- No single institution could afford a full service Security Operations Centre (SOC) however a national SOC, staffed by experts could help institutions prepare for and respond to cyber-breaches.
- Sharing a Chief Information Security Officer (CISO) – with a small staff - among institutions is being considered in Ontario.
- Regional Area Networks (BCNet, Orion, RISC, etc.) are all currently pursuing shared services in a number of areas.

What appears to be lacking is the institutional commitment to fund, transfer authority and adhere to “outside” policies to enhance cyber-security through sharing and outsourcing. In the future this will become a necessity.

COMMUNITY SHARING
Another area where CAUBO/CUCCIO members can benefit greatly is termed Community Sharing. If institutions follow similar models for governing cyber-security then Board Members, Executives, and IT staff have colleagues with whom they can exchange operational practices, risk assessments, identification of potential vulnerabilities and educational/informational materials. Some of this currently exists and should be strongly encouraged.

---

15 University of Alberta is one example.
4.7 DEVELOP AND MONITOR CYBER-SECURITY METRICS

Without appropriate metrics (or measures) it is impossible to understand not only where an institution stands with respect to cyber-security but also if you are moving forward or slipping. Any risk management process demands that metrics are put in place and continually monitored. Many institutions already have metrics and regularly measure and report on them.

Best practice suggests that all institutions should select and monitor cyber-security metrics and report them on a regular basis. Some cyber-security metrics include:

- university owned devices that are managed vs unmanaged
- accounts compromised per week, month etc.
- devices compromised (failing Nessus or whatever) and percentage cleaned up
- breaches identified during the time period and amount of data compromised
- users taking cyber-security educational courses
- users phished and credentials stolen
- number of external attacks, probes

Inherent in this best practice is the need to define, for each measure, the steps/actions to improve its rating. Developing a roadmap and associated cost to make improvements is suggested.

4.8 EVALUATE CYBER-INSURANCE

Cyber-insurance is not a panacea and should not be viewed as a solution to cyber-security. Rather it is a means of limiting financial loss and possibly gaining access to 3rd party cyber-security experts. Some cyber-insurance policies put at your disposal "cyber-coaches" and other expertise to help manage breaches.

At present the Canadian cyber-insurance market is immature in that both insurers and the insured have difficulty defining what coverage to offer, coverage details, and pricing. Some Canadian universities have acquired cyber-insurance directly from insurers, others are considering it, but find the costs/coverage uncertain. Insurers look for effective cyber-security practices, such as those advocated here, when assessing the risks and merits of coverage.

Many institutions are hoping that CURIE will take the lead and provide/source useful cyber-insurance policies. Assuming enough institutions agree to actively participate and provide details of their existing practices and infrastructure then CURIE can proceed to work with providers to provide suitable coverage.

It is recommended that cyber-insurance be evaluated as part of any Institution’s approach to cyber-security. Appendix “A” includes cyber-insurance questions and information on coverage currently available in Canada, although its suitability to universities is not clear.

4.9 RETAIN OUTSIDE CYBER-SECURITY EXPERTISE

One of the key requirements of containing and resolving a cyber-breach is to have expertise available to conduct a forensic analysis of the cause and extent of the breach. Other aspects of breach management such as notifications, legal requirements, ransom negotiation and communications are similarly complex. Hence a best practice for any institution is to have ready access to cyber-security experts when the need arises. As noted some insurance policies provide these services, however, every institution should consider arrangements with suppliers who provide such services and pre-plan the “what, when and how” these experts can be accessed should a breach arise. Waiting until after a breach has occurred, and only then trying to hire experts, is too late, and will very likely delay and weaken the institution’s response.

External experts can also provide services such as penetration testing, security audits and training for the university as part of the overall prevention plan.
4.10  LOOK TO THE FUTURE NOT JUST CURRENT THREATS
Cyber-attacks are rapidly and continually evolving. Computer viruses mutate, DDoS attacks shift from computers to other devices (phones, printers, internet-of-things devices), quantum computing threatens current security protocols and personalized phishing attacks (spearfishing) are becoming the norm. While no one is sure what will be next, institutions need to be forward looking when considering evaluating plans and programs that have cyber-security implications, which is almost everything these days. Best practice dictates that cyber-security be part of most decisions considering both current and likely future cyber-risks.

4.11  RESPECT, BUT NOT OVERPLAY CULTURE/ACADEMIC FREEDOM AS REASONS NOT TO ADOPT SOLID CYBER-SECURITY PRACTICES
Finally, university culture and academic freedom are factors that differentiate higher education from other organizations. Some feel that these can be huge impediments to deploying and enforcing cyber-security policies and standards. Regardless institutions should not allow these factors to stop them from taking appropriate steps to reduce cyber-risk.

Institutions should consider:

• Developing tactics and processes to ensure that both central and distributed IT groups adhere to cyber-security policies, standards and procedures. These can involve both incentivizing the implementation of appropriate safeguards and compliance with policy, and sanctions with clear escalation paths in the event of non-compliance.

• Ensuring that all IT groups report on the selected metrics.

• Restricting access to systems and data from those who violate standards.

Cyber-security is only useful if people follow the rules. Best practice implies that cyber-security be practiced by everyone.

In summary the above 11 “best practices” are all things that universities should consider. Certainly not all can be implemented at once, nor are they the only things that any institution should evaluate, however paying attention to the above will help to improve cyber-security.