MATERIALS FOR CAUBO/CUCCIO MEMBER INSTITUTIONS TO ASSIST BOARD MEMBERS AND SENIOR EXECUTIVES PROVIDE OVERSIGHT ON CYBER SECURITY MATTERS

April 2017
A Sense of Urgency, A Case for Action

- All Canadian universities, large and small, are vulnerable to cyber-attack.
- Today’s attackers are malicious, organized, sophisticated, stealthy, and well-resourced.
- Cyber-security is a major and growing problem that requires active board and executive oversight.
- The mission of Canadian universities makes them attractive targets for all types of cyber-attacks.
- The impact of a breach involves both quantitative (financial) and qualitative (reputational) factors. Cost estimates are in the millions for a medium size attack on a medium size organization.
Cyber-Security Landscape: Attackers are Organized, Sophisticated, Stealthy and Well Resourced

• The average time between a breach and its discovery is 200 – 400 days. Once inside hackers stay hidden and can maintain their access for long periods;

• There is ready market for personal information (to create and profit from fake identifies). For instance, one figure quoted 50 cents per record;

• A study found that about half of the subjects clicked on links from strangers in e-mails and Facebook messages—even though most of them claimed to be aware of the risks – illustrating the breadth of vulnerability and the limitations of user education;

• The Federal Government has passed legislation (expected to be enacted in 2017) with fines up to $100,000 per person if an organization fails to appropriately notify that person if their personal information has been stolen;

• Devices (phones, tablets, building systems, “internet of things”, etc.) are being used to launch massive distributed denial of service (DDoS) attacks. A recent example was the use of common digital video recorders (DVR’s) to attack the KrebsOnSecurity website;

• Bitcoin has a 1-800 number where organizations can buy bitcoins to pay cyber-ransom.
Universities are Ripe Targets: Balancing Risk and Mission

• Decentralized communications, systems, structures and decision-making authority can make universities easier to attack and exploit than other entities. (Soft targets.)

• Students constitute a large, inquisitive, tech-savvy population. A few use institutional cyber-infrastructure to alter grades or illegally download media. (Exposure to liability.)

• Institutions thousands and sometimes millions of personal records containing personally identifiable information (PII), payment card information (PCI) and protected health information (PHI), all of which have value to hackers. (Privacy and liability concerns.)

• Valuable research data and other forms of intellectual property are contained in university systems. (Targets for competitors and State Sponsored organizations.)

• Universities have the ability to pay reasonable sums which makes them attractive to fraudsters and organized crime. (Financial and Reputational Risks.)

• University infrastructure features high speed networks and massive computation capability which can serve as a useful platform to attack others, e.g. DDoS. (Universities have useful cyber-infrastructure.)
Conclusion: Urgency and Action Required re: Cyber-Security

• Oversight of cyber-security is not “one-and-done”, nor solely incident based responses; rather there is a need for a continuing process to regularly monitor activity, enforce compliance and ensure necessary improvements are made.

• Cyber-security should be proactively monitored through a set of plans and ongoing reviews that are formally part of leadership meeting agendas, i.e. an appropriate cyber-security Governance process.

• The combination of sophisticated attackers + rapid change + vulnerable institutions + significant risks implies (demands) an ongoing commitment to cyber security.
This diagram illustrates that the broad responsibilities of Board Members and Executives are distinct and different, but also have areas of commonality as defined by the institution.
Four Pillar Cyber-security Model for Canadian Universities

For each of the four pillars (Prepare, Prevent, Respond, Improve) Institutions should evaluate the institutional readiness and capacity along three dimensions: People, Practices and Resources.
### Key Characteristics of the Four Pillar Model

<table>
<thead>
<tr>
<th></th>
<th>PEOPLE</th>
<th>PRACTICES</th>
<th>RESOURCES</th>
</tr>
</thead>
</table>
| **PREPARE** | • Determine balance of internal and external capabilities  
• Develop/maintain internal skills  
• Seek external relationships for specialized expertise | • Promulgate policies & practices that address current & emerging threats  
• Develop/maintain cyber-security governance  
• Conduct a formal Threat/Risk Assessment | • Define priorities and investment criteria  
• Develop/maintain cyber-security plan  
• Conduct table-top exercises with key stakeholders |
| **PREVENT** | • Engage the community through effective, persistent communication and education | • Monitor compliance  
• Maintain active governance  
• Ensure effective IT practices | • Provide robust user awareness training and feedback  
• Implement intrusion prevention tools |
| **RESPOND** | • Contract for staff augmentation and specialized expertise to address forensics and workload | • Emphasize speed of response to a breach (governance gives clarity to roles and communication when under duress) | • Implement intrusion detection tools  
• Activate pre-planned incident response protocols |
| **IMPROVE** | • Assess new or emerging skills  
• Assess efficacy of current practices and resources | • Reassess threats  
• Ensure ongoing board engagement | • Assess efficacy of prevention and detection tools  
• Conduct forensic audits |

*Note: When preparing cyber-security reports, institutions would replace the generic statements in the matrix with specific information pertinent to their circumstances.*
Implementing and Governance Using the Four Pillar Model

**Baseline Report**
- Demonstrates due diligence
- Identifies key vulnerabilities and priority actions
- Track changes over time through consistent measures

**Governance Process Defines:**
- Who is involved in preparing and reviewing cyber-security reports and presentations;
- Frequency of reporting to Executive and Board/Board committee – Quarterly Written Reports and Presentation;
- What follow-up occurs in response to questions and concerns;
- What education is delivered to full Board and Executive group and what frequency.
Best Practices for Board and Executive Consideration

1. Insist upon a formal, written cyber-security plan.
2. Develop governance, be proactive, hold regular reviews.
3. Educate your community, expect some resistance to the need for behavioral change.
4. Create a risk management program, involving internal audit and risk managers.
5. Consider having IT skills on the Board, much like financial, legal, and HR acumen.
6. Promote shared services, outsourcing, and community sharing to augment internal resources.
7. Develop and monitor appropriate cyber-security metrics.
8. Evaluate cyber-insurance. The market is immature today, but continues to develop.
11. Respect but do not be constrained by institution and academic culture.

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.
Conclusions

1. Oversight of cyber-security is **not “one-and-done”**, nor solely incident based responses; rather there is a need for a continuing process to regularly monitor activity, enforce compliance and ensure necessary improvements are made.

2. The rapidly evolving and increasing virulence of cyber-crime makes this a **continuing drain** on university resources and Executive time.

3. Waiting until after a breach has occurred, and only then trying to hire experts and/or put response protocols in place, is too late, **must plan and prepare before a breach occurs**.

4. Boards have a general obligation to protect University assets, including confidential and proprietary information, reputation and goodwill from cyber-attacks. Executives have responsibility for providing leadership and putting the necessary plans, policies and processes in place. This is similar to other areas, e.g. safety, fiduciary responsibilities.

5. Cyber-security should not be fully delegated to a Committee or “C” level executive. The full Board and Executive must participate, especially when **making trade-offs on budgets, priorities**, etc.

6. Universities face a **range of cyber-security risks/costs**:  
   • Direct financial losses, Privacy and liability claims, Operational disruptions  
   • Reputational damage, Regulatory intrusion

7. Board, Executives and Technical Staff must be **on the same page and work together**.