CYBER RISK SURVIVAL:

Emerging Threats, Strategies, and Legalities

HIGHER EDUCATION SUMMIT
November 16, 2015

BLG
Borden Ladner Gervais

Deloitte.

CYBER RISK SURVIVAL

Ira Nishisato
Partner and National Leader –
Cybersecurity and Cyber-Risk Management

BLG
Borden Ladner Gervais

"The data breach we experienced in 2013 has resulted in government inquiries and private litigation, and if our efforts to protect the security of information about our guests and team members are unsuccessful, future issues may result in additional costly government enforcement actions and private litigation and our sales and reputation could suffer".

-Target Corporation, SEC Form 10Q, filed November 26, 2014


HYATT
ebay
THE HOME DEPOT
kmart
SONY
DQ
ROGERS
J.P.Morgan
Neiman Marcus
Ontario
MINISTRY OF EDUCATION
Michaels

"There are two kinds of companies. Those that have been hacked, and those that have been hacked, but don't know it yet"

— US House of Representatives Intelligence Committee Chairman Mike Rogers, November 30, 2011

- ***Cyber Security*** – Technologies, processes and practices designed to protect information technology systems and related data from attack, damage or unauthorized access.

- ***Cyber Risk*** – Any risk of damage, loss or liability (e.g. financial loss, business disruption loss, loss to stakeholder value, legal non-compliance liability or reputational harm) to an organization resulting from a failure/breach of the organization's information technology systems.

TOP QUESTIONS

- What are the threats?
- How can we manage them?
- How much cyber security is enough cyber security and how do we put our organization in a defensible position?

Cyber risk in the higher education sector

Transform your cyber defences

Nick Galletto, Partner &
Americas Cyber Risk Services Leader
Monday, November 16th
10:45 – 11:45 am

Contents

Cyber landscape in higher education

Understand the evolution

Cyber threat landscape in higher education

Higher education's unique environment

- Higher education typically has lean IT teams to serve a transient population
- Universities and colleges often have decentralized IT, with shadow IT departments within different faculties, departments, or research areas – making it more difficult to protect and defend against more advanced attacks
- Most universities and colleges must allow for BYOD that require both policies and technology to control access and prevent data loss

Cyber threat landscape in higher education

Shifts in cyber threats

In the last 3 years, we have seen a shift in cyber threats to higher education:

- Higher education ranked third in percentage of reported security breaches (Source: Symantec Internet Security Threat Report)
    1. Health 37%
    2. Retail 11%
    3. Higher Education 10%
- No longer students trying to change grades - recent attacks on Universities of Virginia, Washington, and Maryland are believed to be by nation states
- Cyber adversaries are interested in research, people of interest, and intellectual property

Borden Ladner Gervais

Cyber threat landscape in higher education

Understanding your adversary – who might attack and what are they attacking

- **Cyber criminals** looking to profit from personal information
- **Nation states** looking for key research or information about key individuals
- **Hackivists** with a social agenda who seek to disrupt or embarrass schools
- **Accidental disclosure** or loss of personal information on portable devices by staff or partners

Borden Ladner Gervais

Cyber threat landscape in higher education

Tactics – how are they attacking

- Cyber attacks are no longer the result of a **single hacker, looking for bragging rights**. Most attacks are now performed by **well-funded, well-resourced professionals and teams (e.g. nation states, organized crime) seeking to profit from the attack**.
- **24 zero day vulnerabilities** were reported in 2014 that cyber criminals could immediately start exploiting to gain access to organizations' environments. Of the top 5 vulnerabilities, cyber criminals exploited them for a combined 295 days before vendors made patches were available (Source: Symantec Internet Security Threat Report).
- **"Booter" services** provide a distributed denial-of-

Cyber threat landscape in higher education

Cyber attacks – how schools are responding

University of Virginia	University of Maryland	University of Washington
University of Virginia was the victim of a sophisticated cyber attack originating from China and targeting two specific individuals employed by the University. Two email accounts of individuals with connections to China were targeted as a result of this attack.	University of Maryland was the victim of a sophisticated attack that exposed personal information, including name, Social Security number, date of birth, and University identification number. In the investigation, the University found that that the threat actors had a significant understanding of how the school's database was designed and protected.	University of Washington was the victim of malware sent by email, which was opened by a University medical employee. This resulted in the breach of the medical information of 90,000 patients, including 15,000 social security numbers.
Response • Employees were required to change their passwords within the system that was compromised • Comprehensive security update aimed to enhance the security of data	**Response** • Audit performed on the school's security • The University set aside more than $6 million to pay for a 5-year credit monitoring program for the victims of the breach.	**Response** • Breach notification letters were sent to all individuals affected and victims were offered free credit monitoring service to monitor their credit activity for any signs of fraudulent activity

Cyber threat landscape in higher education

What higher education has learned

- Significant data comprises appear to be the result of **targeted attacks**
- In most cyber attacks, one or more severs were running **outdated operating systems** and were vulnerable to exploitation
- **Phishing** continues to be a threat vector of choice for attackers
- **Credit monitoring services** continues to be the expected standard for personal information breaches

Borden Ladner Gervais

Defining the need

Challenge your thinking

Defining the need

Challenge conventional thinking for security

1. Difficult to demonstrate **alignment with the organization**
2. Lacks clear vision on communication and **articulation of value**
3. Limited consensus towards a **common goal/framework**
4. Just too much to think of (process, capability etc.). **Overwhelming Cyber Program and too much technology**
5. Traditional frameworks primarily focus on **reactive methods**

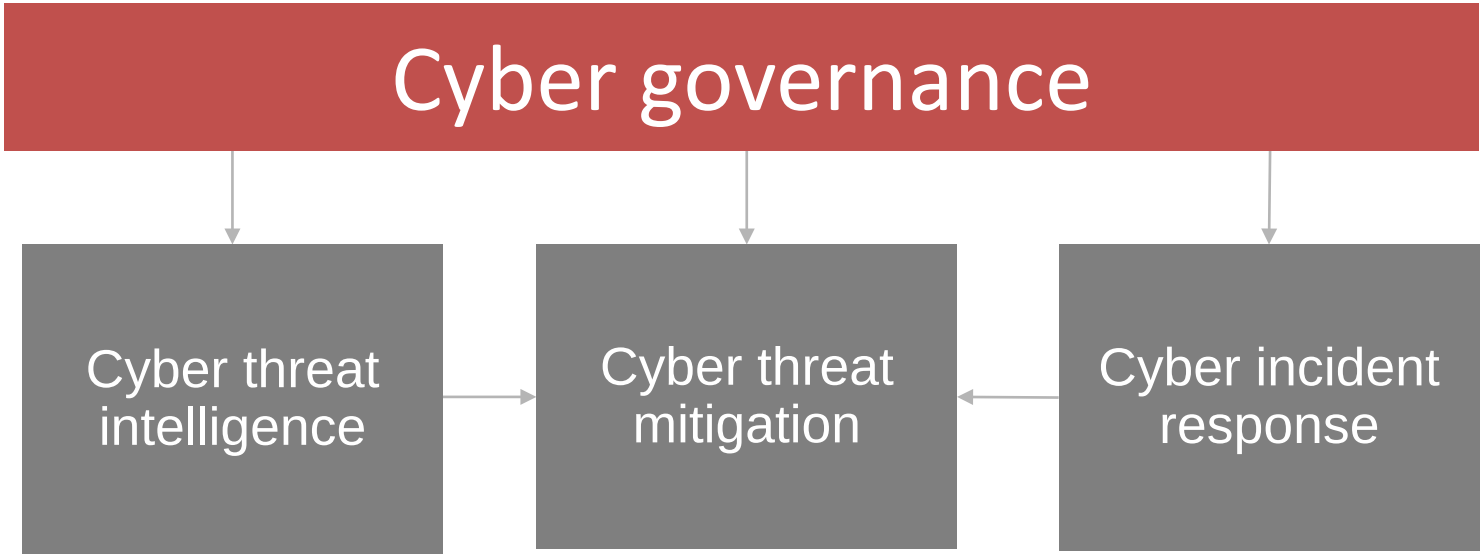
Transforming your defenses

Become secure, vigilant, resilient

Transforming your defenses

Become secure, vigilant, resilient

Secure	Vigilant	Resilient
Are controls in place to guard against known and emerging threats?	Can we detect malicious or unauthorized activity, including the unknown?	Can we act and recover quickly to minimize impact?



Borden Ladner Gervais

Transforming your defenses

Cyber is not longer an IT issue

- **Effective cyber security starts with awareness at the board – the recognition that at some point your school will be attacked**
- **Management teams are taking a more active role in protecting their schools, but grapple with how to make the role effective (what are their responsibilities, which competencies should they be cultivating, what are the right questions to ask, etc.)**

Transforming your defenses

Cyber governance starts at the top

Your management team should be asking:

1. **Are we focused on the right things?**
2. **Do we have the right talent?**
3. **Are we proactive or reactive?**
4. **Are we incenting openness and collaboration?**
5. **Are we adapting to change?**

Borden Ladner Gervais

Transforming your defenses

Evaluate the effectiveness of your cyber risk program

- The **management team is engaged on a regular basis** to review and discuss the implementation of the school's cyber security framework and implementation plan, including the adequacy of existing mitigating controls?
- Basic **cyber security assessments take place** on a fixed, unvarying schedule and are not industry specific?
- **Internal audit evaluates cyber risk management** effectiveness no more than once a year?
- Cyber security assessments and internal audit evaluations **are sporadic or non-existent**?

Borden Ladner Gervais

Closing remarks

Closing thoughts

1. Know your crown jewels – not just what you want to protect,
   but what you **need to protect**.
2. Know your friends – partners and suppliers **can be security allies or liabilities**
3. Make **awareness a priority** within every faculty and department
   and among external parties
4. Fortify and monitor – situational awareness, diligently gather intelligence, build, maintain and **proactively monitor**
5. Prepare for the inevitable – **test** your incident management process

Borden Ladner Gervais

Thank you

Nick Galletto
Partner, Americas Cyber Risk Services Leader
ngalletto@deloitte.ca
416-601-6734

Nick Galletto is a Partner with Deloitte and he is the Americas Cyber Risk Services leader, and also leads our National Technology Risk Services Practice in Canada. Nick has over 25 years of experience in information technology, networking, systems management and information security management. He has accumulated extensive experience in the management, design, development and implementation of cyber security and risk management programs.

Nick has a Master of Business Administration and he is a Certified Information Systems Security Professional, a Certified Information Security Manager, Certified in Risk and Information Systems Control and SABSA Certified Architect.

Borden Ladner Gervais

Deloitte.

- Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee (“DTTL”), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as “Deloitte Global”) does not provide services to clients. Please see www.deloitte.com/about for a more detailed description of DTTL and its member firms.
- Deloitte provides audit, consulting, financial advisory, risk management, tax and related services to public and private clients spanning multiple industries. With a globally connected network of member firms in more than 150 countries and territories, Deloitte brings world-class capabilities and high-quality service to clients, delivering the insights they need to address their most complex business challenges. Deloitte’s more than 210,000 professionals are committed to becoming the standard of excellence.

- This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited, its member firms, or their related entities (collectively, the “Deloitte network”) is, by means of this communication, rendering professional advice or services. No entity in the Deloitte network shall be responsible for
- any loss whatsoever sustained by any person who relies on this communication.

-

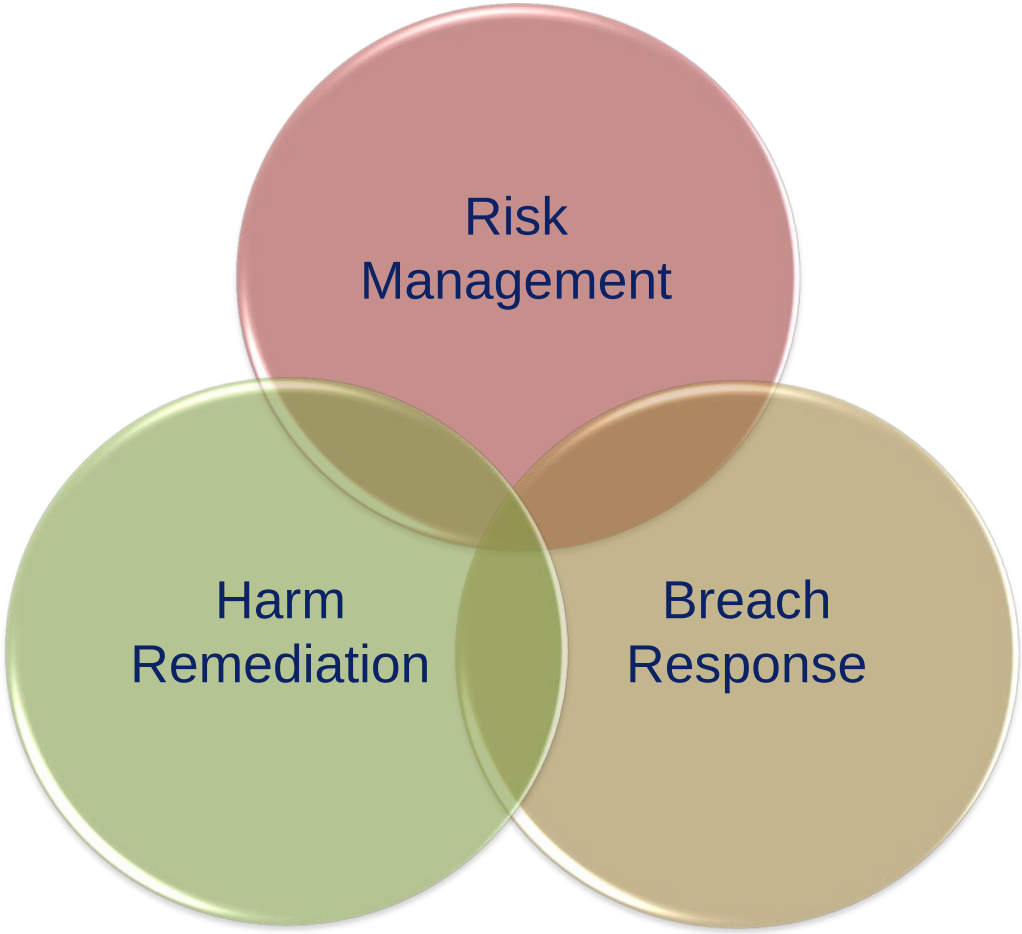
BLG
Borden Ladner Gervais

FRAMEWORK FOR CYBER RISK MANAGEMENT

Ira Nishisato
Partner and National Leader –
Cybersecurity and Cyber-Risk Management

BLG
Borden Ladner Gervais

Cyber Security and Cyber Risk



Borden Ladner Gervais

Framework for Management of Cyber Risk

1. Understand the Risk
2. Understand the Standard of Care
3. Engage the Board
4. Build a Team
5. Assess Your Risks
6. Develop a Cybersecurity Plan
7. Develop a Breach and Continuation Plan
8. Test, Assess, and Revise