HARVARD
Office of the Vice Provost for Advances in Learning

CYBERSECURITY:
MANAGING RISK IN THE INFORMATION AGE

A visionary paper on risk mitigation for Ontario's digital BDE delivery

By Carmel Tse

HARVARD
Office of the Vice Provost for Advances in Learning

HarvardX

Learning outcome:

Develop a cyber risk mitigation strategy specific to your organization.

Plagiarism declaration:
1. I know that plagiarism is wrong. Plagiarism is to use another's work and pretend that it is one's own. **2. This assignment is my own work.** **3. I have not allowed, and will not allow, anyone to copy my work with the intention of passing it off as his or her own work.** **4. I acknowledge that copying someone else's assignment (or part of it) is wrong, and declare that my assignments are my own work.**

This module focused on the importance of risk mitigation and the value companies can derive from implementing a risk mitigation strategy to improve organizational resilience and manage risks effectively. This assignment requires you to complete a cyber risk mitigation strategy for your organization.

As the notes made clear, a risk mitigation strategy helps an organization prioritize its risks so it can allocate resources efficiently. This final submission is an opportunity for you to reflect and condense all the knowledge you have gained over the duration of the course by incorporating feedback from your previous ongoing project submissions into a consolidated cyber risk mitigation strategy.

Note:

All ongoing project submissions throughout the course need to focus on the **same** organization. This case study uses a newspaper group's operation in the New York area.

To avoid disclosing any confidential information in this assignment, the name of the organization and brands used are removed. The assignment is drawn on real-world experience but sensitive details or data have been removed or altered.

Introduction

Ontario is about to embark on the digital delivery of driver's ed. A Draft Digital Learning Standard for Beginner Driver Education (BDE) has been circulated to stakeholders after submissions have been made to the Ministry of Transportation of Ontario, including one submitted by this author In November, 2018 as part of a pedagogical project at the Harvard Derek Bok Center for Teaching and Learning.

The draft, prepared by MTO's Evaluation and Training Office, of MTO's RUS Division, is quite comprehensive as a universal framework for curriculum development. The three sections in the draft cover technical requirements, quality requirements and digital course instructional requirements. In terms of improving on the existing brick-and-mortar classroom curriculum, the draft certainly reflects the inclusion of modern technology and eLearning pedagogies.

Two critical requirement topics, however, are either missing or not substantially discussed in the draft:

- Cybersecurity
- Learning Management System

These two requirement topics, if made mandatory and implemented properly, will secure the credibility and integrity of digital BDE delivery initiative.

Cybersecurity

Cybersecurity is not identical to network security, and the latter is only a subset of the former. With digital BDE delivery, we are now anticipating a large amount of data to be collected, processed and stored through internet transactions. We will also be collecting a lot of personal and financial information from students, parents and instructors.

Identity stolen is identity lost forever. Driving schools, like any other businesses, are always legally liable for security breaches. With digital delivery, the risks escalate.

Typical cyber workflow

In a typical enrollment process, a digital BDE program will collect personal information from the student, an image of the driver's licence may have to be uploaded for verification purpose, and payment card information of the student or parent is transmitted.

Once a student is in the program, a login password protected account is created and each candidate will access the course through the login process.

Tel: +1 519-673-7333 | **Email:** ctse@qint.com

All course materials will be stored somewhere and be accessible to registered students.

All the attendance record, financial transactions, finished assignments, quizzes and exam results for each individual student will be stored digitally.

In-car session records will be submitted by in-car instructors and with a digital course, the submission ideally should be electronic.

Certification information will be entered into MTO's RUS system when a student completes the course.

Cybersecurity requirement questions [Bold face indicates item addressed in the draft]

1. Is your web site secured? e.g. https, trusted
2. What information is collected? The ideal answer is only the bare essential data should be asked for.
3. Where and how the information is stored? Is it backed up?
4. How long will the information be kept and when will they be purged?
5. What encryption requirements are in place?
6. Is your network segmented and is the system protected behind a firewall?
7. Is your payment card process PCI DSS compliant?
8. **Multi-Factor Authentication (MFA) or Two-Factor Authentication for user access.**
9. When will a student's login access be removed?
10. Do you have a staff person or contractor acting as a point person or steward on cybersecurity.
11. What communication requirements do you have in place in the event there is a data breach.

The risks

As long as there is internet accessible data, there will be bad actors – willing or innocent:

Curious intruders. There are always people out there looking for free BDE courses. Many of them have much better computer skills than driving school operators.

Organized crime. They will hack any into system that hosts personal or financial information. They achieve this using simple tactics such as phishing, spear phishing or web site impersonating.

Malware and ransomware. They will tailgate registered users and send trojan malware or ransomware into commercial systems.

Innocent users. Users lacking computer skills may trigger system crashes.

DDoS. Distributed denial of services. The threats can come from nation states, competing businesses or hackers for fun.

Contractors. Your suppliers may be a gateway for bad actors.

Vision

Any new system with public access, such as digital BDE, will attract intruders. My vision is the Government, the stakeholders and the service providers will work together on a cybersecurity framework to protect the digital BDE rollout. Together, we will implement a secure and resilient cyber environment to secure our assets, train our workers, safeguard the privacy of our customers, and use new innovation and technology to grow this industry in the new information decade.
If we look back 30 years and plan our next cybersecurity decade based past key developments, we might be able to plot – not imagine – the cyber path we may have to go through in the next decade.

1990s

- Arpanet becomes the internet
- SSL encryption for transactions implemented
- 2G wireless phone technology introduced

2000s

- Advanced Encryption Standard (AES) for classified information
- ILOVEYOU worm spreads
- iPhone, Android, 3G introduced
- Aurora with Chinese footprints attacks Google and 33 other businesses

2010s

- Yahoo, Target, Sony, Anthem, Ukraine power grid breached
- WannaCry ransomware attacks
- U.S. banks hit
- 4G introduced, 5G hatching
- U.S. curbs ZTE and Huawei activities

Strategic goals and objectives

Bad actors will continue to cut through our digital fences, intrude into our properties, interrupt our business, steal customer data and may alter our digital assets. Through four broad strategic goals, our plan is to move in parallel in the following measures:

Prepare. This is a Government-led initiative and directions will have to start at the MTO with support of the private service providers.

Secure. This will focus on fortifying our perimeters, discouraging intrusions, encrypting our data and strengthening security for passages through our gateways.

Defend. We have to be vigilant and be prepared to be fend off and chase out any invasions through preemptive strikes, removing any sleeping malware before they start attacks. Our arsenal shall include latest detection software, scalable cloud storage and eradication tools. Wargames will be used to prepare our strike teams and all staff will be trained to be cybersecurity aware.

Forward thinking. Technology does not freeze on January 1, 2020. We will have to adjust and revise our cybersecurity initiatives from time to time.

To achieve our strategic goals, initiatives must be based on risk mitigation and we need to prioritize on the following objectives:

Prepare.

- Initiatives are to be spearheaded by the Government.
- To lower the R&D costs for the driving school industry, the Government can help by identifying qualified service providers.
- Initiatives must have the full support of the industry and service provider.

Secure.

- Cloud-based technology be used and request for proposal be issued.
- Encryption of different data types to be defined and implemented.

Defend.

- The service providers have to have the capability to detect and eradicate threats before they will exert harm on the systems, in that we need to rely on artificial intelligence and machine learning.
- Defensive tactics and weapons are to be one-step ahead of bad actors.
- Collaborations are to be established with industry peers and enforcement agencies.

Forward thinking.

- As part of the procurement process, we will require suppliers to constantly review their products and services to take into consideration arising threats.

Metrics

The No. 1 metrics to measure achievement is the buy-in by the ministry and the industry. This is to be followed by funding allocation and appointment of the cybersecurity leadership. A general cannot win the war without soldiers and cybersecurity staff has to be in full compliment.

The progress of the cybersecurity initiatives will be tracked and calculated using a Gantt chart. In this type of projects, a cross-departmental waterfall project management schema may be more effective than an agile model. The cybersecurity project manager is the steward of the Gantt. Training and certification, as examples, are best tracked with targeted start and finish dates. Other tasks that can be tracked by the Gantt chart includes 2FA, password policies and encryption sub-projects.
To really test the effectiveness of the initiatives, results of the wargames are good indicators of how ready we are. The wargames should be umpired by an outside judge.

Cybersecurity Policy Chart
It is recommended that we develop and publish a Cybersecurity Policy Chart modeled after the CSAIC's DoD Cybersecurity Policy Chart. At a glance, this chart will enable our industry to identify the statutes and regulations that govern our cyber activities.

Law enforcement and ISACs
We need to identify the government agencies that we are required to disclose the information to as well as Information Sharing and Analysis Centers (ISACs) we can share information with and what type of information we can safely share.

Recommendation summary

- Publish cybersecurity requirements
- Limit data collection and define retention period
- Use of cloud-based technology encouraged
- Identify qualified service providers
- Supply chain management

Learning management system

A successful eLearning platform owes it success to a good learning management system and effective authoring tools. LMS is a collection of software applications for the administration, documentation, tracking, reporting and delivery of educational courses, training programs, or learning and development programs. Without the support of an LMS, it will be almost impossible to properly administer and track a digital course.

Authoring tools
Two prevailing authoring tools dominate the eLearning market at this time:

- Articulate Storyline
- Adobe Captivate

LMS choices

Most LMS use one of the above two authoring tools while incorporating other document formats such as pdf eBooks, text, graphics and videos. Here is a list of the top LMS as published by elearningindustry.com: Top 20 LMS

About the author…

Carmel C. Tse is the operator of iPass Driving School, a CAA ADSN school in Ontario. He is a licensed Ontario driving instructor (classroom and in-car). He holds a Higher Education Teaching Certificate from the Harvard Derek Bok Center for Teaching and Learning and a post-graduate Cybersecurity Certificate from the Harvard VPAL. He is a certified system integrator in the newspaper industry and has extensive knowledge in Content Management Systems (CMS) and Learning Management Systems (LMS).

Tel: +1 519-673-7333 | **Email:** ctse@qint.com