Agenda | The CYBER Exchange

CHANGE POINT INTELLIGENCE

7:30 am
8:15 am

REGISTRATION OPENS ALONG WITH BREAKFAST SERVICE

8:15 am
8:30 am

WELCOME AND OPENING ADDRESS

Greg Padovani
Chief Operating Officer
NFP Canada

8:30 am
9:30 am

A REVIEW OF PRIVACY LEGISLATION, RECENT NETWORK SECURITY, DATA AND PRIVACY (CYBER) LIABILITY LOSSES, EMERGING TRENDS AND LESSONS LEARNT

Actual cyber breaches that organizations have encountered will be discussed; the impacts of 1st party costs such as IT forensics, data identification, recovery and restoration, legal fees, the cost of identify and financial fraud monitoring along with the cost of breach notification. The impacts of 3rd party costs such as civil litigation, regulatory investigations, and contractual costs associated with when a breach occurs will also be discussed.

Mandatory breach notification under Canada's Federal Personal Information Protection and Electronic Documents Act (PIPEDA) came into force on November 1, 2018. The national mandatory breach notification rules include a mandatory requirement for organizations to give notice to affected individuals and to the Office of the Federal Privacy Commissioner about data breaches where it is reasonable to believe that a breach creates a "real risk of significant harm to any individual". Our panel will outline what this means for your organization and what you should be doing in response to this new legislation

The General Data Protection Regulation (GDPR) came into effect on May 25, 2018 and this EU privacy legislation imposes stricter requirements than its predecessor, the Data Privacy Directive, and unlike that instrument it is not open to interpretation by National Governments, and its shock-waves will travel beyond EU borders.

The GDPR will affect Canadian organization's more than expected as several clauses do not align with Canadian law, for example data portability, data use and consent mandate to name a few. Our panel will outline what it means to Canadian organizations and what you should be doing now as the legislation is already in place.

9:30 am
10:30 am

A REVIEW OF CEO FRAUD, HOW IT OCCURS? WHY IT CONTINUES TO OCCUR? RECENT LOSSES AND WHAT CAN BE DONE TO PREVENT FINANCIAL LOSS FOR YOUR ORGANIZATION FROM THIS THREAT VECTOR?

CEO fraud, also referred to as "business email compromise and cyber fraud"; prevention, response and recovery will be discussed. The focus of the presentation will centre on how deception and manipulation are used to trick CEO's, CFO's and organizations into fraudulent electronic wire / funds transfers or the disclosure of confidential, personal or financial information. The consequences of this fraud, along with real loss examples of successful types of CEO fraud will be discussed along with steps an organization can take to prevent such fraud

10:30 am
10:45 am

NETWORKING BREAK

10:45 am
11:45 am

PAYMENT CARD INDUSTRY (PCI) DATA SECURITY STANDARDS (DSS), WHAT YOU DON'T KNOW WILL COST YOUR BUSINESS IN FIRST-PARTY COST ASSESSMENTS, FINES, CHARGES AND LOST CUSTOMERS AND POSSIBLY THIRD-PARTY LITIGATION; RECENT LOSSES WILL BE DISCUSSED AS WELL AS WHAT TO DO WHEN A BREACH OCCURS?

Payment Card Industry Data Security Standards (PCI DSS) will be discussed, including your contractual responsibilities, the audit of your security standards at your cost, fines and industry penalties, and the costs of identify and financial fraud and credit card monitoring when your customers credit cards have been stolen and re-sold on the Dark Web. Learn about recent Canadian credit card losses as well as what to do when a breach occurs.

11:45 am
1:00 pm

LUNCH AND KEYNOTE PRESENTATION ON RANSOMWARE

Ransomware has morphed from a painful financial loss to a bankrupting business interruption. Our featured speaker at the "The Hamilton Cyber Exchange", along with her firm has responded to hundreds of ransomware attacks globally. "A Walk-through of an Actual Ransomware Case" will be featured in which you will witness the value of advisory services on the likelihood of remediation and the ability to recover from back-ups.

As part of the negotiation process, she will explain how her team of malware experts review all decryption tools for additional malware designed to create a secondary attack, or escalate the current attack, and to confirm that the decryption keys work. Regardless of whether the ransom is paid in bitcoin or another crypto-currency, her team of forensic experts will determine if there was any actual theft of confidential information during the attack as well as confirm that the network has been fully remediated.

1:00 pm
2:00 pm

WE HAVE BEEN BREACHED, NOW WHAT?

Do we have a Breach Response Plan? Has it ever been tested? Is our "Tiger Team" ready to respond? Are our IT vendors ready and able to resolve our breach? These are just a handful of the questions that your Board of Directors will be posing your management and IT teams in the event of a breach, and why? because the financial integrity of your business is now on the line and you are vulnerable!

Our panel of experts will discuss the impact of having and not having a Breach Response Plan, the need for a Breach Coach and access to top tier IT forensic experts on every threat vector known, share actual breach successes and failures as well as walk you through incident response service agreements, specifically forensics investigation, data processing, analysis of the incident, vulnerability scans, and dark web investigation to name of few of the key elements that you will need to address in the event your organization has been breached.

2:00 pm
2:30 pm

NETWORKING BREAK

2:30 pm
3:30 pm

NETWORK SECURITY, DATA AND PRIVACY (CYBER) LIABILITY INSURANCE, THE INSURANCE MARKET PERSPECTIVE

Network security, data and privacy liability insurance also known as "Cyber Liability Insurance" has grown dramatically as an additional Board of Director and Company based solution to first party and third-party company losses in the event of a security, data or privacy breach. The evolution of the market place has meant more meaningful coverage is now available for all of the current threat vectors facing Canadian Companies today. Our panel of insurance experts will discuss current coverage grants, where and under which insurance policies coverage applies, and the lessons learnt from paid insurance losses to date.

3:30 pm
4:30 pm

NETWORK SECURITY, DATA AND PRIVACY (CYBER) LIABILITY, THE BUYER'S PERSPECTIVE

Our panel of senior executives will address the merit of employee security training and awareness, penetration testing and vulnerability assessments, how they interact with IT and the Board of Directors in dealing with the liability risks associated with network security, data and privacy liability as well as how they handle breaches.

"Cyber Liability Insurance" will also be discussed; its merits, strengths, weaknesses and where and how it plays a role in the risk management strategies of our panel of executives. Finally, you will hear about the overlaps and gaps in coverage, the need to coordinate coverage's and to keep pace with the evolution of the insurance coverage provided.

4:30 pm
4:45 pm

CONFERENCE WRAP UP AND CLOSING REMARKS

Adam Briklyn
President and Chief Executive Officer
Professional Risk Underwriters Inc.