

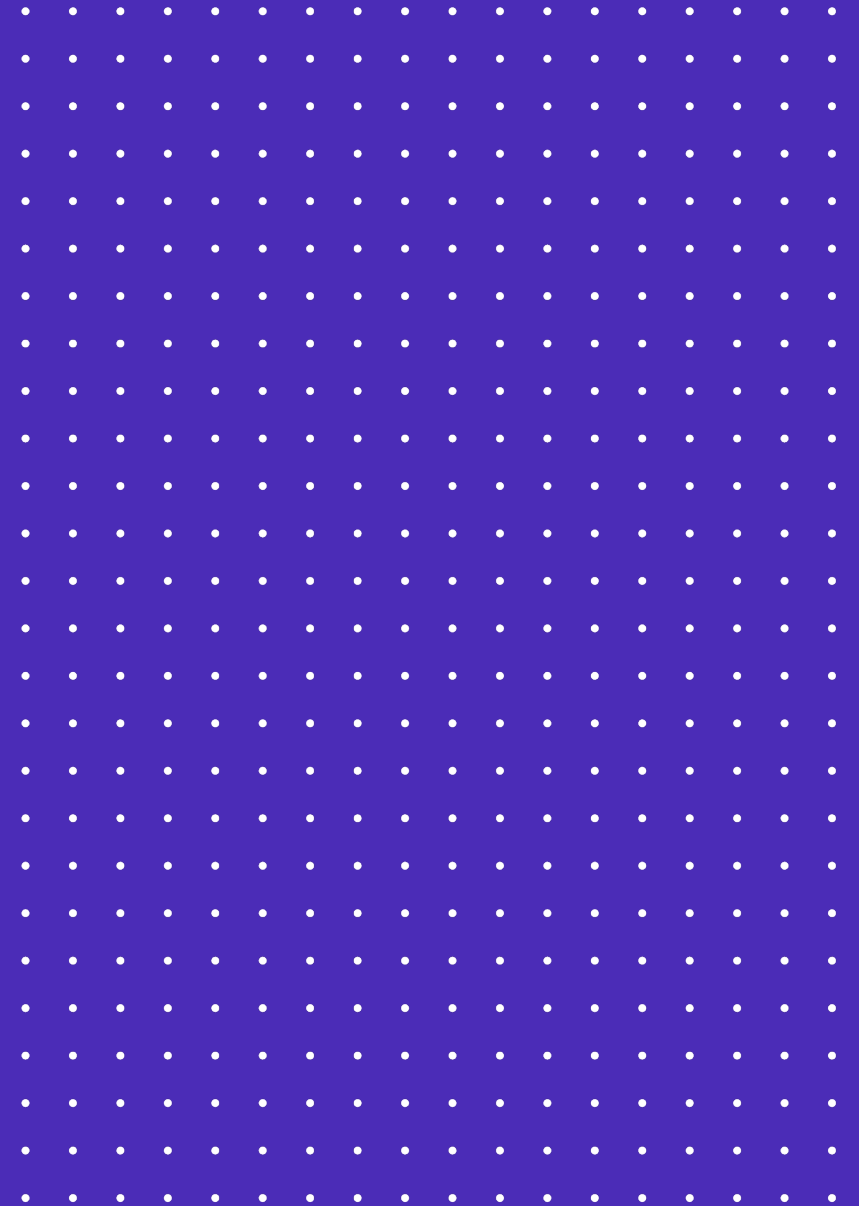
# Master Class: Cybersecurity and Direct Selling

November 18, 2021

Michael Weinberger

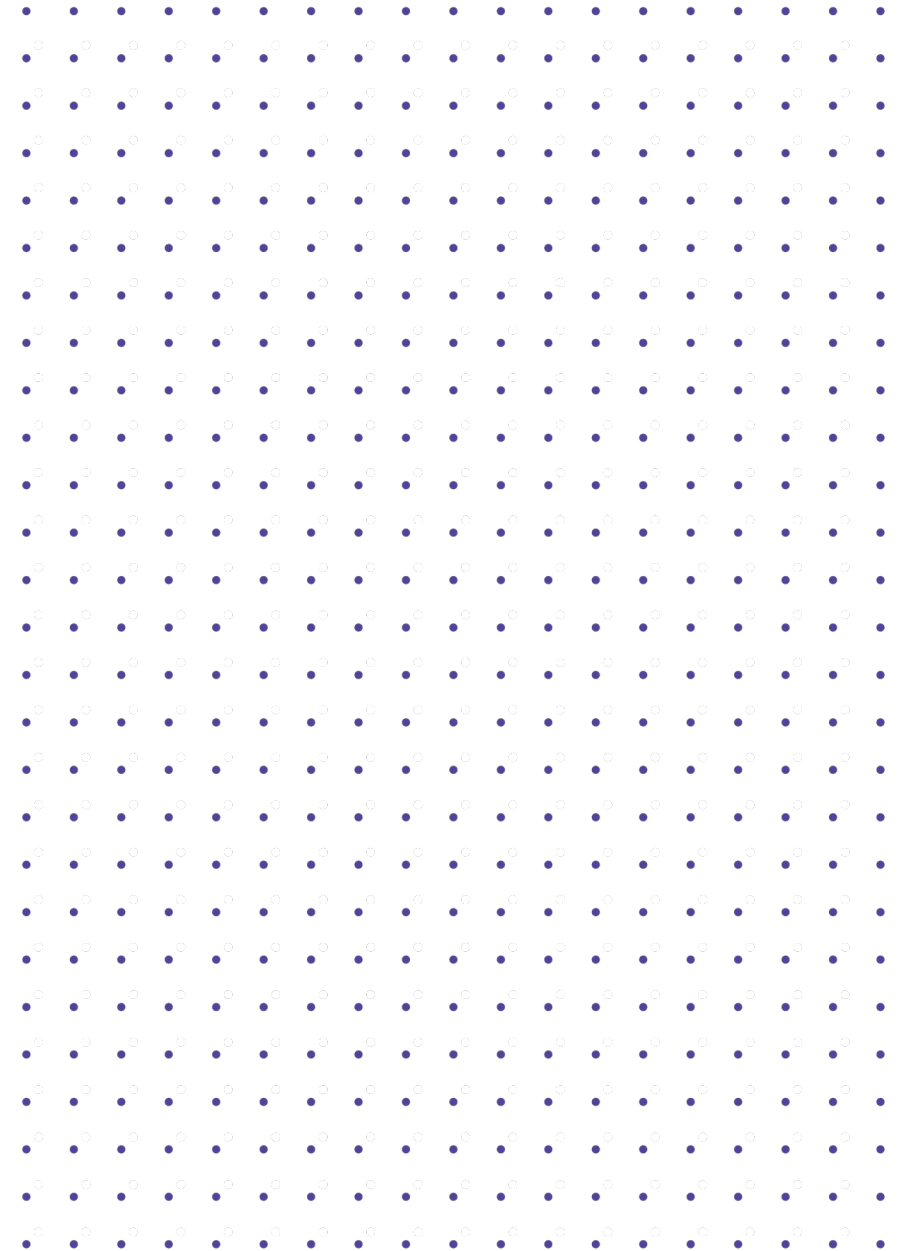
Peter Dillon

**SISKINDS** | The law firm



# Roadmap

- About Us (and you)
- Why Cybersecurity is important for the MLM industry
- Basic Types of Cyber Attacks
- The Cyber Kill Chain
- ABCs of Cyber-Response
- Preparation and Protection



# About Us

**Full service law firm headquartered in  
London, Ontario**

**Offices in:**

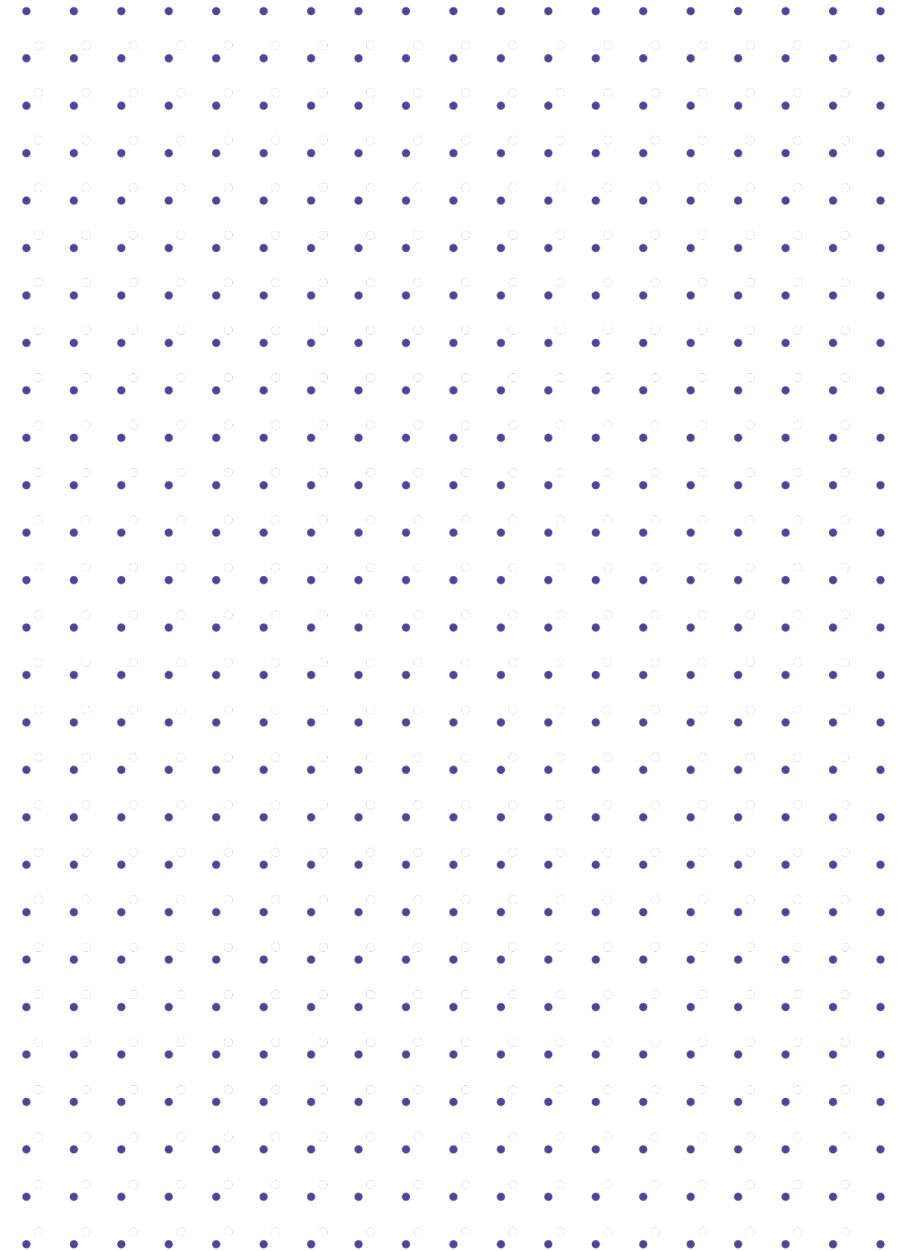
Toronto

Sarnia

Quebec City

**Over 80 lawyers working in over 25  
specialized practice areas**

**SISKINDS** | The law firm



# Peter Dillion

## Partner & Chief Privacy Officer

Called to the Bar in Ontario and  
New York State

Certified Breach Coach

Certified Data Protection  
Officer (IBITG)

EU GDPR Certified by the  
Chartered Institute of  
Information Security



# Michael Weinberger

## Associate

Called to the Bar in Ontario

Holds a Masters of Law and Finance

Practice Focuses on Direct Selling and MLM Industry

Fluent in Spanish, French, German



# Involvement in the Direct Selling Industry

- New Member of Canadian DSA
- Advising Direct Sales Clients since the 1990s
- Advise MLMs both large and small



# What some of our partners say:

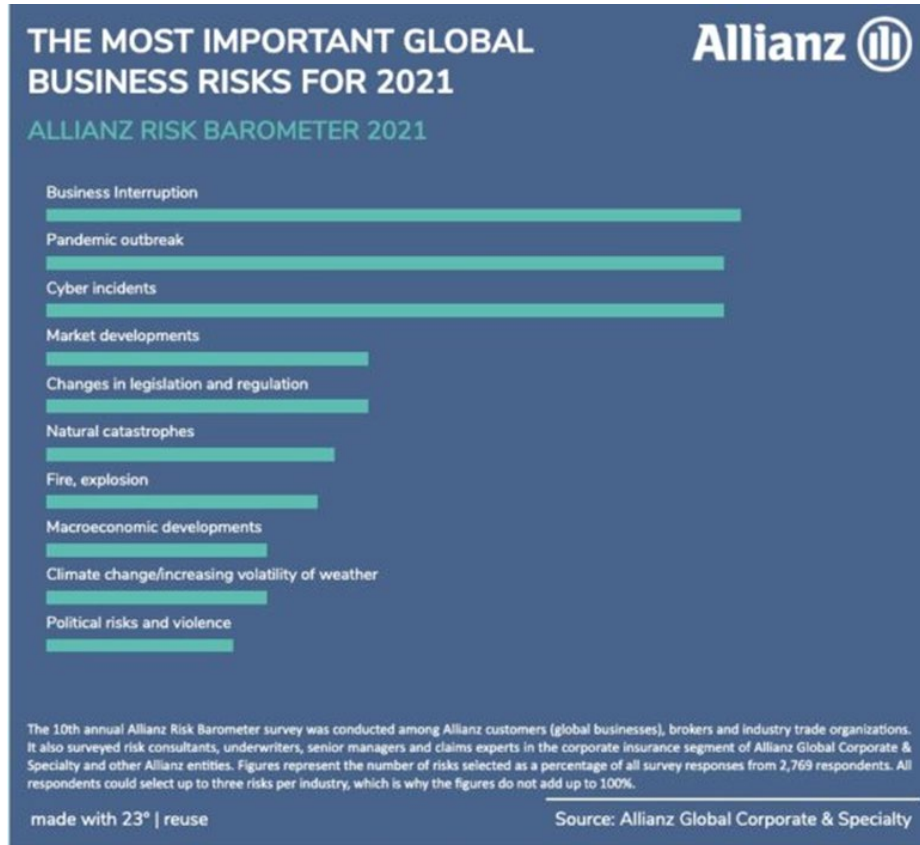


*Without reservation, I can say that Michael's perspicacity and detail orientation in the thorny and bureaucratic world of network marketing jurisprudence would be an asset to any organization entering the space.*

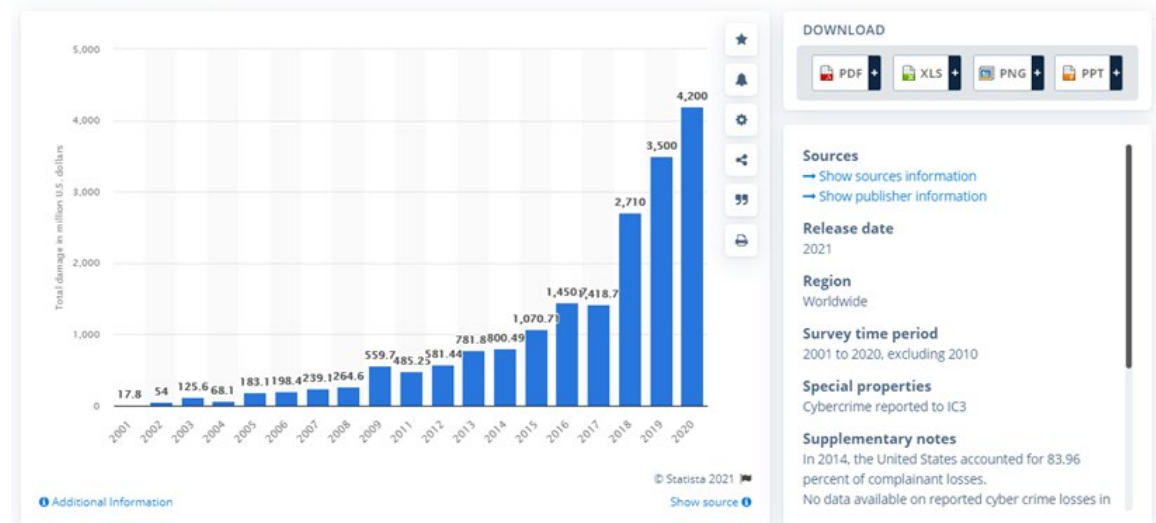
**Kenton Engel, Vice President of Compliance for New U Life**



# Why are We Here?



Amount of monetary damage caused by reported cyber crime to the IC3 from 2001 to 2020  
(in million U.S. dollars)





# The Direct Selling Industry

## Arbonne MLM data breach exposes user passwords, personal info

By **Sergiu Gatlan**

May 26, 2020 05:29 PM 0



International multi-level marketing (MLM) firm Arbonne International exposed the personal information and credentials of thousands after its internal systems were breached by an unauthorized party last month.

Valeriy Shevchenko

1K Followers   About

Follow 

Sign in [Get started](#) 

## How I hacked millionaires accounts in MLM company

 **Valeriy Shevchenko** Nov 2, 2017 · 7 min read



OFFICE OF THE VERMONT ATTORNEY GENERAL  
TJ Donovan, Vermont Attorney General

[HOME](#)
[ABOUT](#)
[FOR CONSUMERS](#)
[IN THE COMMUNITY](#)
[OPEN GOVERNMENT](#)
[NEWS/MEDIA](#)
[CONTACT PAGE](#)

Security Breaches > Herbalife International of America Notice of Data Breach to Consumers

## Herbalife International of America Notice of Data Breach to Consumers

© FEBRUARY 23, 2007



500 West Olympic Blvd., Suite 4  
Los Angeles, CA 90015

February 23, 2021

G3271-LS2-0000002 T50001 P001 \*\*\*\*\*MIXED AAC  
SAMPLE A SAMPLE-LS2  
APT 123  
123 ANY ST  
ANYTOWN FRN ZIP  
COUNTRY  
+-----+-----+-----+-----+-----+-----+



News Editorial **Security** Privacy Crypto Cloud Resources ▾ Tools ▾ Reviews ▾

Follow ▾ 🔍

If you purchase via links on our site, we may receive **affiliate commissions**

[Home](#) » [Security](#)

## 30,000+ Italian sales agents' personal data, IDs leaked by MLM company that distributes wellness products

by Edvardas Mikalauskas · 16 June 2020 · 5



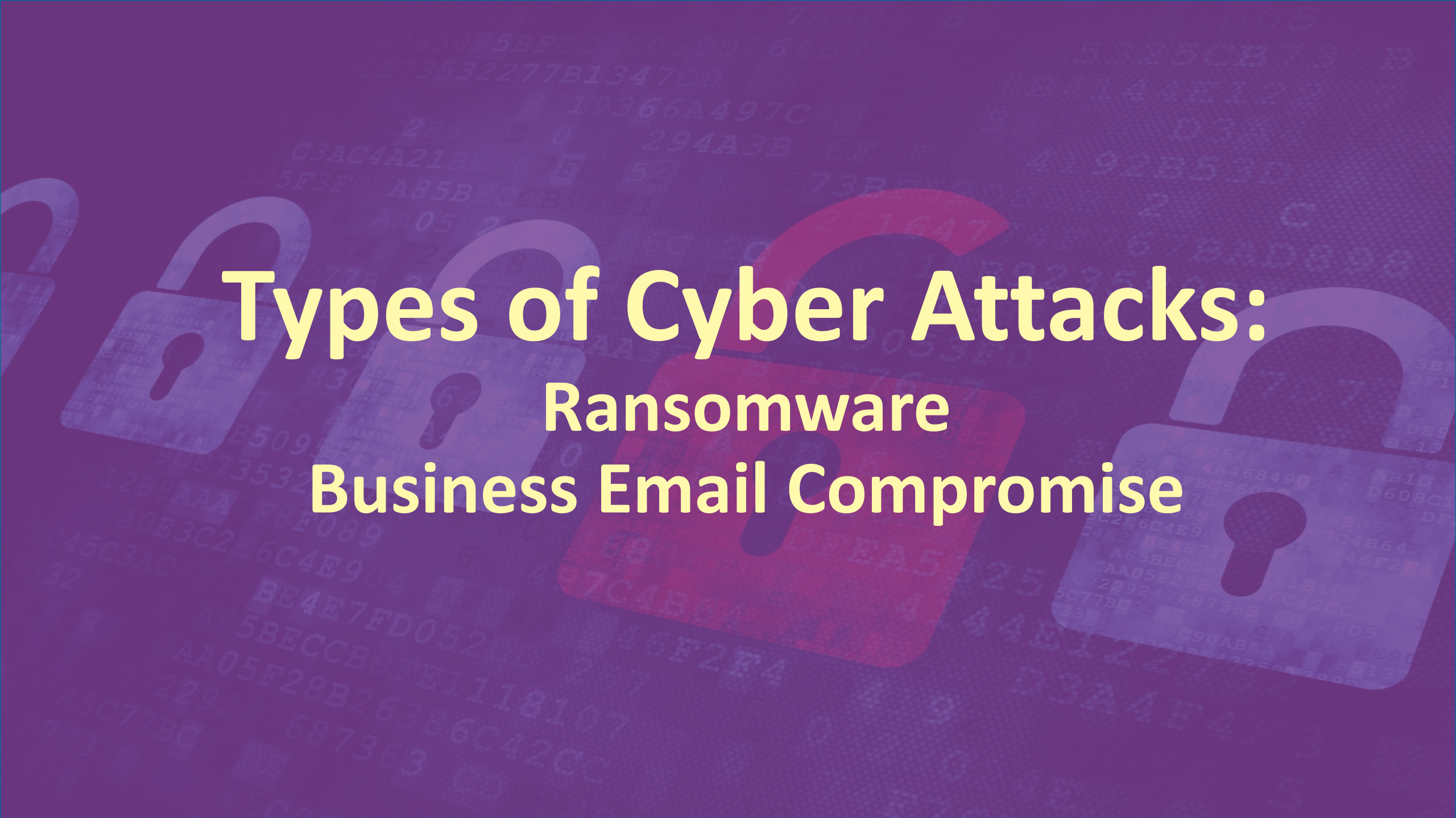
### Editor's choice



**SISKINDS** | The law firm

# Why is this so important?

- People Business
- Trust
- PIPEDA is going to “get real”
- Average cost of a data breach is \$4,000,000

The background is a solid purple color. It features several large, stylized padlocks in shades of blue and red. Overlaid on this are numerous strings of hexadecimal code (e.g., 5325CB73, 19366A497C, 294A3B) in a light blue or white font, scattered across the image.

# Types of Cyber Attacks:

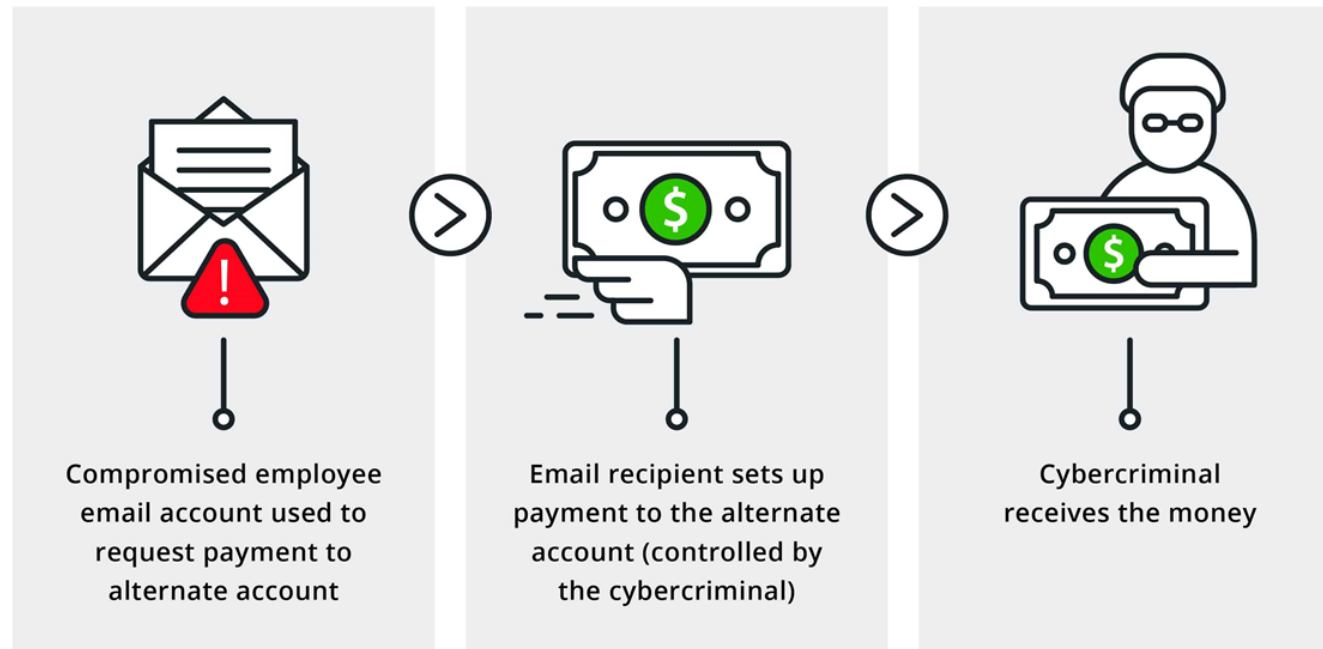
- Ransomware
- Business Email Compromise



# Ransomware



# Business Email Compromise



# The Cyber Kill Chain

The background of the slide is a solid purple color. On the right side, there is a faint, light-colored graphic. It consists of a network diagram with several nodes connected by lines, forming a circular shape. In the center of this network is a stylized padlock icon, suggesting a focus on security and cyber threats.

# Recon



Reconnaissance



# Weaponization



Weaponization

# Delivery



Delivery

# Exploitation



Exploitation

# Installation



Installation

# Command & Control



Command & control

# Exfiltration



Actions on objectives

# What To Do if You Detect a Cyber Incident



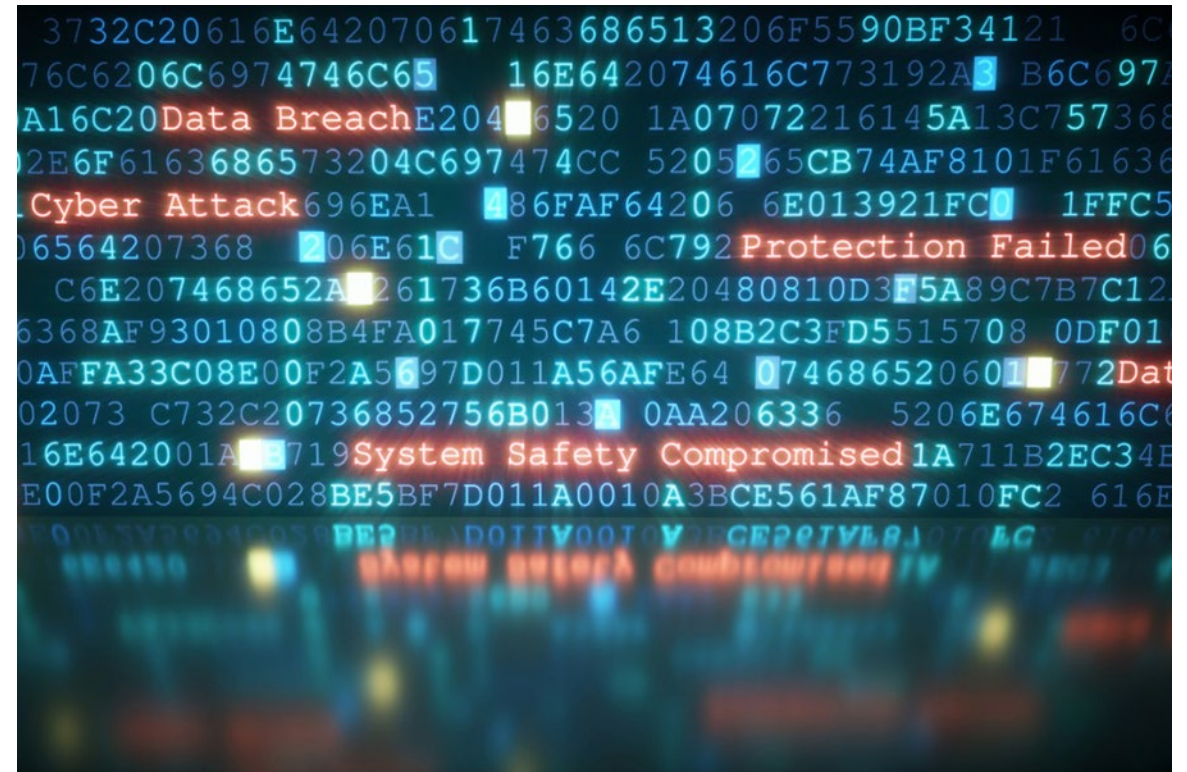


# Required Notifications?

- Three reasons to notify
  - Law
  - Contract
  - Insurance
- Who should notify?
  - The Controller must make the notification

# Who had the Incident?

- Corporate?
- Leader?
- Both?
- Does it matter in the end?



# Corporate Breach-Example: Microsoft Sharepoint Hacked

- Corporate to Downline
- Corporate to Consumer
- Corporate to Employee
- To Suppliers
  - When was the last time you reviewed your DPA?
- To Insurers
- To Regulators
- To Parent company

# Leader and Participants

- Leader to Corporate
- Leader to Downline
- Leader to Consumer
- Leader to Regulator

# Which Jurisdiction?

- Canada?
  - Which province?
- USA?
  - Which State?
  - CCPA?
- EU?
  - Notification twice? Natürlich in Deutschland
- Global? Even where not allowed?

# Engage legal counsel experienced with data breach management

- We have experience with midsize and publicly traded companies
- Canada's only certified Breach Coaches
- Pre-established relationships

# Commence record taking

- The time and date of all discussions and key decisions should be documented throughout the event. The role of this record keeper should be identified in your Incident Response Plan (“IRP”).



# Activate the Incident Response Team

- All members of the Incident Response Team (“IRT”) should be notified using one or more of the contact methods identified in your IRP.

# Engage forensics

- The containment, eradication and recovery phases of the incident require the involvement of a skilled forensics team from the outset.

# Secure the premises

- If there is a defined area where the data breach occurred, it should be secured to prevent unauthorized access and the loss of any evidence. At the same time, a Command Centre for the IRT should be established and secured.

# Stop additional data loss

- Containment of the incident includes such measures as: disabling the network switch port to which a particular system is connected; blocking access to malicious network resources such as IP's (at the firewall) and domain source specific URLs; temporarily locking a user account under the control of an intruder; disabling system services or software that an adversary is exploiting; and shutting down all Wi-Fi connections. Note that all machines should be left powered on , in order to preserve any cached memory. Reset the passwords of employee and customer accounts, to prevent takeovers, in order reduce the value of exfiltrated data on the black market and make data buyers and traders lose confidence in the seller.

# Continue record-keeping

- Secure all logs, audits, notes, documentation and any other evidence that has or is gathered during the incident with appropriate identification marks, securing the chain of custody for future prosecution or litigation. All relevant system security/event/IDS logs should be maintained. Provide notice to your ISP or MSP that they preserve and maintain all logs.

# Interview key persons

- As part of the record-keeping process, all parties involved in the incident should be interviewed from time to time to gather their observations and input.

# Consider notification requirements

- Provincial and federal laws impose notification obligations to various governmental offices, the affected data subjects, and law enforcement and other agencies. Because of the short notification periods provided for under these laws, your legal obligations to disclose need to be assessed early on, and that assessment should be constantly updated.



# Assess priorities and risks

- Based on what you know at this point regarding your systems, the extent of the breach, the nature of the breach and other factors, priorities need to be established and other aspects of your response, including communications, need to be progressed.

# Advise your insurer

- If you have cyber insurance coverage, your broker or insurance company representative should be notified at the outset. This ensures that the response is conducted in accordance with the best practices established by the insurer.

# Notify law enforcement

- Law enforcement agencies are increasing their level of cooperation and information sharing. This means that information about the particular threat actor may be known to the police, which may assist the forensics team. In some instances, decryption keys for ransomware are known to law enforcement agencies who can then share that information. In the event of a criminal prosecution, law enforcement can insist assist with preservation and storage of evidence.

# How to Prepare

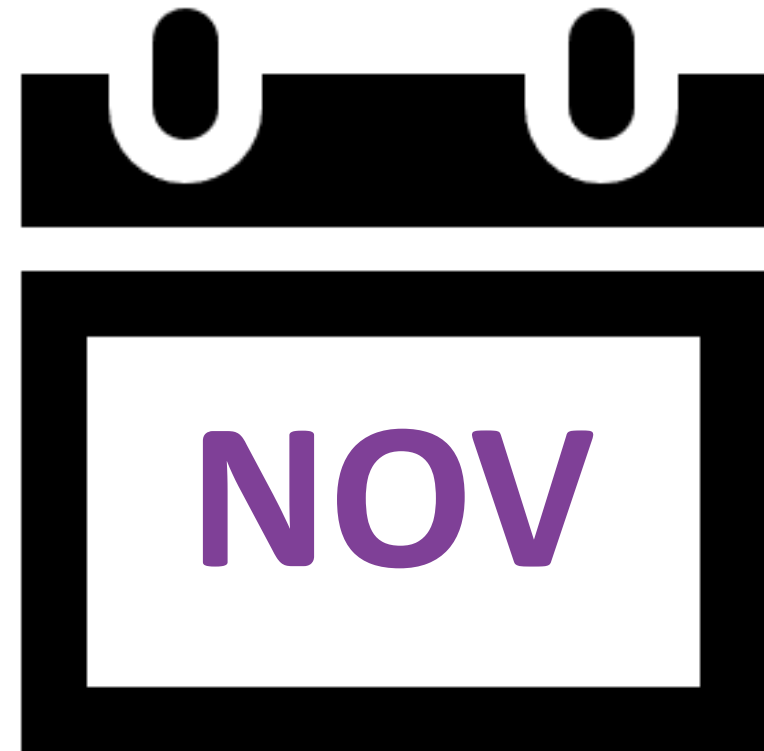


VIRUS ALERT

`x[i].getElementsByTagName("title").childNodes`

# Data Collection

- Reduce collection where able
- Limit collection
- Why full DOB? Month Only





# Incident Response Team (IRT)



# Penetration Testing



# Preventative Steps

- Password policies
- Multi-factor authentication
- Encryption
- Backups
- Training Modules for the field
- Training for Leaders
- Tabletop Exercise





# Contact Us



**Peter Dillon,**  
Head of Technology and  
Cyber Security Group

Email:

[peter.dillon@siskinds.com](mailto:peter.dillon@siskinds.com)

Phone: 519-660-7818



**Michael Weinberger**  
Direct Sales Lawyer

Email:

[michael.weinberger@siskinds.com](mailto:michael.weinberger@siskinds.com)

Phone: 519-660-7843