C VISION INTERNATIONAL

AGENDA

The Future of Cybersecurity

CISO Think Tank

SPEAKERS



Ben Sapiro
Head of Technology Risk & CISO
Canada Life



Emma Christy Peel
Director Information Security- Governance
Gap Inc.



Jeff Moore
Chief Product Security Officer
Drager



Steve Magowan
VP - Cyber Security
BlackBerry



Arif Hameed
CISO
C&R Software



Iain Paterson
CISO
WELL Health Technologies Corp.



David Masson
Director of Enterprise Security
Darktrace Holdings Limited



Octavia Howell
CISO
Equifax Canada



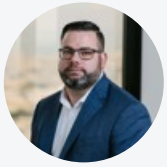
Samer Adi
CISO
Ontario Securities Commission



Michael Gross
Manager, Cybersecurity Intelligence
Cleveland Clinic



Steve Zalewski
Former CISO
Levi Strauss & Company



Garrett Weber
VP - Worldwide Sales Engineering
Salt Security



Rob Knoblauch
Deputy CISO & VP Global Security Services
Scotiabank



Robert Smith
Field CISO
Noname Security



Jeff Moore
CISO
Gap Inc.



Michael Gross
CEO
Engrossed Advisory

Click Here to Register

August 24, 2022

Eastern Time

Welcome & Registration

12:00 PM-1:15 PM

KEYNOTE

Third Party Security – We need to support our suppliers

1:15 PM-1:50 PM

Managing third party risk must be a core competency for security teams because our businesses depend more and more on third parties. There is no clearer alignment for security with business value than third party risk management. To manage third party risk well we need to do more than asks questions, we need to enable our suppliers. To enable our means we need to understand them and some of the problems we face as a profession in assessing the security around third parties.

SPEAKER



Ben Sapiro

Head of Technology Risk & CISO

Canada Life

PANEL

Ransomware/Extortionware

1:55 PM-2:50 PM

CISOs face a huge headache trying to understand how to know when they were attacked, what data attackers have corrupted? How quickly can they recover from the attack? And do they have to pay a ransom to get the data back?
Ransomware remains a significant challenge for companies, not simply because it has become ubiquitous, but also because of the significant impact a single ransomware attack may have on a company and every other company or customer that relies on that company.
Cybersecurity and risk management have always been vital for the flow of any business. However, the current condition of the global supply chain makes it exceptionally vulnerable to severe damage from an attack more so than usual. When the supply chain is barely getting by, criminals are more likely to assume they have leverage over businesses. A ransomware attacker may be more brazen and exercise higher demands than they might have a few years ago.

CHAIR



Steve Zalewski
Former CISO
Levi Strauss & Company

PANELISTS



Iain Paterson
CISO
WELL Health Technologies Corp.



Octavia Howell
CISO
Equifax Canada



Michael Gross
Manager, Cybersecurity Intelligence
Cleveland Clinic



Robert Smith
Field CISO
Noname Security

Networking Break

2:50 PM-3:05 PM

FIRESIDE CHAT

3:05 PM-4:00 PM

Guarding the Doors: Navigating 3rd Party Risk

As organizations expand their third-party ecosystem, many are challenged with executing core activities that are critical to operations, risk profiles, and compliance posture without compromising the quality of data collection, evaluation, and mitigation measures increasingly outsourcing business activities to 3rd-party vendors. It is critical for an organization to be vigilant when selecting the right 3rd-party vendor with the appropriate security posture, as many vendors are hosting, processing and transmitting sensitive regulatory information with unrestrained access to our IT assets. At the highest level, third-party incidents can result in reputational damage, non-compliance, or even criminal activity, which can negatively impact earnings and shareholder value. To address this challenge, many organizations are investing in technology to support vendor risk management. Technology isn't the entire answer to managing third-party risk, however the right technology or collection of technologies, coupled with optimal processes, can enable organizations to bridge the gap.

CHAIR



Steve Zalewski
Former CISO
Levi Strauss & Company

SPEAKERS



Steve Magowan
VP - Cyber Security
BlackBerry



Samer Adi
CISO
Ontario Securities Commission

DISRUPTOR

4:05 PM-4:20 PM

How AI Can Think like an Attacker

Outside agents today are using more automation, targeting external providers and shadow IT, and taking advantage of new techniques in their campaigns. As threats change, security approaches need to evolve to manage risk so you can minimize downtime, compromises, and incidents. In this session, learn how the evolution of security gives you unparalleled visibility into the parts of your business that are exposed to the outside world, allowing your security team to proactively identify vulnerabilities before an event takes place. This "outside in" perspective can help you to identify issues before they put your business at risk.

SPEAKER



David Masson
Director of Enterprise Security
Darktrace Holdings Limited

Networking Break

4:20 PM-4:35 PM

The explosion of API Security

4:35 PM-4:55 PM

How do CISOs get the most out of APIs while limiting the risk? 20 years ago the motives for hackers were website defacement and getting your name on all those defacements. That was the point of hacking. Now, it's all about monetizing the data you can steal.
Just as cloud computing initially seeped into organizations under the cloak of shadow IT, application programming interface (API) adoption has often followed an organic, inexact, and unaudited path. IT leaders know they are benefiting from APIs, internal, via third parties, and often outwardly exposed. They just don't know where they are, how much they support key services, and how they're being used, or abused!
In this session we will discuss if APIs are meant to be exposed, and discuss if the startups API software companies are ready for the explosion.

SPEAKER



Steve Zalewski
Former CISO
Levi Strauss & Company

PANEL

The Greatest Fears?

5:00 PM-5:55 PM

The biggest fear is not the technology, it is the potential of human error that could expose your organization to a cyberattack. The majority of CISOs agree that an employee carelessly falling victim to a phishing scam is the most likely cause of a security breach. Most also agree that they will not be able to reduce the level of employee disregard for information security. How do we guard against human error without limiting employee efficiency and productivity?

CHAIR



Steve Zalewski
Former CISO
Levi Strauss & Company

PANELISTS



Emma Christy Peel
Director Information Security- Governance
Gap Inc.



Jeff Moore
Chief Product Security Officer
Drager



Arif Hameed
CISO
C&R Software



Rob Knoblauch
Deputy CISO & VP Global Security Services
Scotiabank

Closing Remarks

5:55 PM-6:00 PM

Cocktail Hour

6:00 PM-7:00 PM

TOGETHER WITH



