Cybersecurity Trend Predictions

2023 and Beyond

2/24/2023

Dan Deganutti

SVP & GM Canada

- Serving Canada 22+ Years
- 5 CyberSecurity Vendor entries to market
- 6 Years at BeyondTrust (2016 Vintage)
- 650+ Canadian Clients

- (Real) Football & Good espresso are my passions. My family too.

BeyondTrust

Mission Statement:

We protect identities, stop threats, and deliver dynamic access to empower and secure a work-from-anywhere world.

BeyondTrust

Company Overview

1,500+ Employees

20 Countries

2003 Founded

Market Leader

Ranked as a PAM leader by Gartner, Forrester, and KuppingerCole

Global Presence

~20k customers in 100+ countries and extensive partner network

Integrated Platform

Unified platform with seamless third-party integrations

Broadest Portfolio

Best-in-class identity and privileged access solutions

Customer Driven

90%+ gross retention and exceptional customer support and success

Technology Pioneers

Heritage of innovation with 75+ patents and commitment to R&D

Headquarters	**Atlanta, GA | USA**
Global Offices	**USA, CANADA, EMEIA, APJ**
Privately Held	**Francisco Partners & Clearlake Capital**

Canadian Headquarters	**Halifax, NS**
Canadian Employees	**360+**
Canadian Customers	**650+**

Cybersecurity Trends for 2023

1. **Negative, Zero, and Positive Trust**

   Implementation transformation with positive and negative implications

2. **Camera-Based Malware is here. Say "Cheese"!**

   Prepare for the first of many exploits that challenge smart cameras

3. **Reputation for Ransom: the rise of ransome-vaporware**

   Extortion based on the threat of publicizing a fictional breach

4. **The Foundation of MFA Invincibility Fails**

   expect new attack vectors that target and bypass MFA strategies

5. **Cyber Uninsurability is the New Normal**

   More businesses will face the stark realization that they are not cyber insurable

6. **The Latest Concert Hack: Wearable Risk Surfaces & Hackable E-Waste**

   expect threat actors to wreak havoc on venues that use these enhancements

7. **Compliance conflicts are brewing**

   Diverging standards, best practices, and security frameworks will lead to conflict

8. **The Death of the Personal Password**

   Non-password-based authentication will spell the end of the personal password

9. **De-Funding of Cyber Terrorists Becomes Law**

   A new approach to defend against ransomware and stop the funding of terrorists: ban ransomware payouts

10. **Cloud Camouflage is Confronted**

    Expect a push for transparency and visibility into the security operations of cloud providers

11. **Social Engineering in the Cloud**

    Attackers will level more social engineering attacks at employers and organizations across the cloud

12. **Unfederated Identities to Infinity and Beyond**

    Expect an expansion of the identity model that includes unfederated models

11. **OT Gets Smarter, Converges with IT**

    Attack vectors for basic Operational Technology will expand based on similar exploits that target IT

14. **Headline Breaches Move to Second-Page News**

    Audience fatigue and lack of interest will cause news of breaches to be buried deeper

15. **A Record-"Breaching" Year**

    2023 will smash records in the direct and indirect cost of breaches to businesses

Cybersecurity Trends for 2023

3

Reputation for Ransom: the rise of ransome-vaporware

Extortion based on the threat of publicizing a fictional breach

Cybersecurity Trends for 2023

4

The Foundation of MFA Invincibility Fails

expect new attack vectors that target and bypass MFA strategies

Cybersecurity Trends for 2023

5

Cyber Uninsurability is the New Normal

More businesses will face the stark realization that they are not cyber insurable

Cybersecurity Trends for 2023

6

The Latest Concert Hack: Wearable Risk Surfaces & Hackable E-Waste

expect threat actors to wreak havoc on venues that use these enhancements

Cybersecurity Trends for 2023

9

De-Funding of Cyber Terrorists Becomes Law

A new approach to defend against ransomware and stop the funding of terrorists: ban ransomware payouts

Cybersecurity Trends for the Remainder of the Decade

1. **Battery Software Revolution**

   Security of the software used for power management will be needed to prevent tampering from causing a catastrophic event

2. **Hackers take automobiles off-roading and off-line**

   Expect the hacking of automobiles to substantially increase

3. **More "Lights Out" Cyberattacks**

   Increasing cyberattacks on energy production and distribution will lead to power outages, fuel shortages, and heating or cooling resource depletion

4. **Evolving from Technology Recycling to Upcycling**

   The recycling of technology will move from destruction to repurposing

5. **The Emergence of "One You"**

   In the next 3-5 years, millions of people will start operating with a single, centralized digital identity

6. **Personal Data Loss Tsunami**

   A massive amount of personal data will vanish because no one is tending to subscriptions

7. **Default Accounts Go Extinct**

   we may finally witness the much overdue extinction of the default accounts and associated secrets

8. **ICS-based Attacks become more Cost-Effective**

   Attacks on industrial control systems will rise as targeted tools increase their profitability

9. **Election Hackers Double Down to Destabilize Democracies**

   Expect cyberattacks on the election process to intensify

10. **The Arrival of the Unforeseen Attack Vector**

    At least one entirely new class of attack vector will emerge and raise the bar for cybersecurity

Thank You

beyondtrust.com