Cyber Risks in the IoT and Industry 4.0 IIoT Landscape

A guide to managing cybersecurity vulnerabilities tied to IoT integration.

Gallagher

Insurance | Risk Management | Consulting

Contents

Headlines

ESCALATING CYBERTHREATS IN A HYBRID WORK MODEL

- Multiple industries and sectors in Canada are adapting their operations using internet of things (IoT) devices to analyze data, integrate the supply chain and reduce time to market.
- Canada's IoT market is predicted to reach $19.08 billion in 2023[1] and expected to exceed $32 billion by 2028, with industrial IoT (IIoT) currently forming roughly one-third of the Canadian IoT market.
- Cyber attack on IoT devices and connected ecosystems are on the rise. The number of IoT cyber attacks worldwide amounted to over 112 million in 2022,[1] with the volume of attacks predicted to grow further.
- Almost 20% of organizations[14] have detected attacks on their IoT systems/devices since 2019, and roughly one-third of chief information security officer (CISO) confident that their information security can reliably assess and mitigate IoT risk(s).

EXECUTIVE SUMMARY

The rising volume of cyber attacks covering data breaches, ransomware attacks and intellectual property theft in Canada have become a pressing concern for corporate organizations and business operators. According to a 2023 survey conducted by Benefits Canada,[1] 62% of Canadian employers are now using a hybrid working model with some hot-desking or working remotely across multiple offices, locations and countries.

The confluence of technology, connectivity and a scattered workforce presents a range of risks and operational challenges for individuals and companies in the hybrid and work-from-anywhere model.

For individuals:

- Reliance on personal devices, public Wi-Fi and cloud technologies create opportunities for hackers to obtain sensitive data.
- Phishing and malware pose hazards to personal and professional data for remote workers.
- Blurred personal and professional environments on shared devices are susceptible to online dangers.

For organizations and business operators:

- Flexible and remote work arrangements increase the exposure to cyber danger.
- Using personal devices and a decentralized workforce create new entry points for cyberthreats.
- Relying on personal network usage and not securing remote access endangers cybersecurity.

Cybersecurity risks have been elevated further by mobile working practices. As employees flip between home/office/on-demand workspaces, data breaches, interception of private information and unauthorized network access increases the vulnerability to multiple cyber attack vectors.

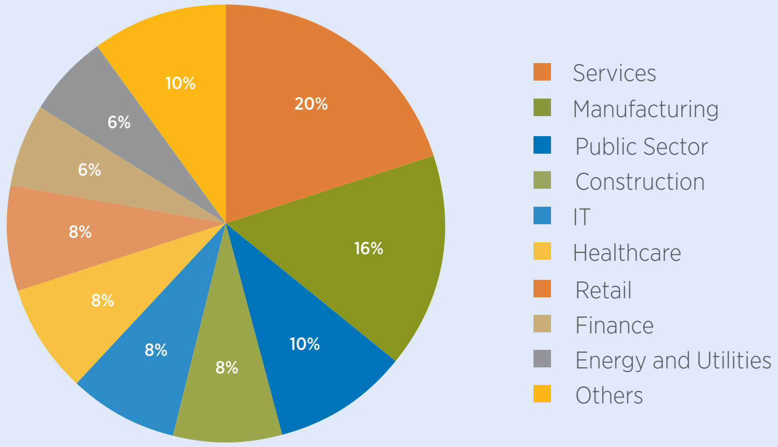
Section 1: Risk Landscape

Context

The Canadian cyberthreat landscape is rapidly evolving as the drive towards multi-industry digitization continues. Interconnected software and platforms, and a growing use case for internet-of-things (IoT) and operational technology (OT) devices, has motivated cyberthreat actors to disrupt business operations. The scope and scale of cyber attack events also challenges public safety and national security. In 2023/24 the complexity of managing IoT and IIoT platforms requires deeper investment—technical skills and technology response—to deliver a holistic and sustainable cybersecurity defence solution.

In 2022 IoT/OT cyber attacks in Canada targeted multiple industries and sectors:

IoT Cyber Attack by Industry Sector (%)

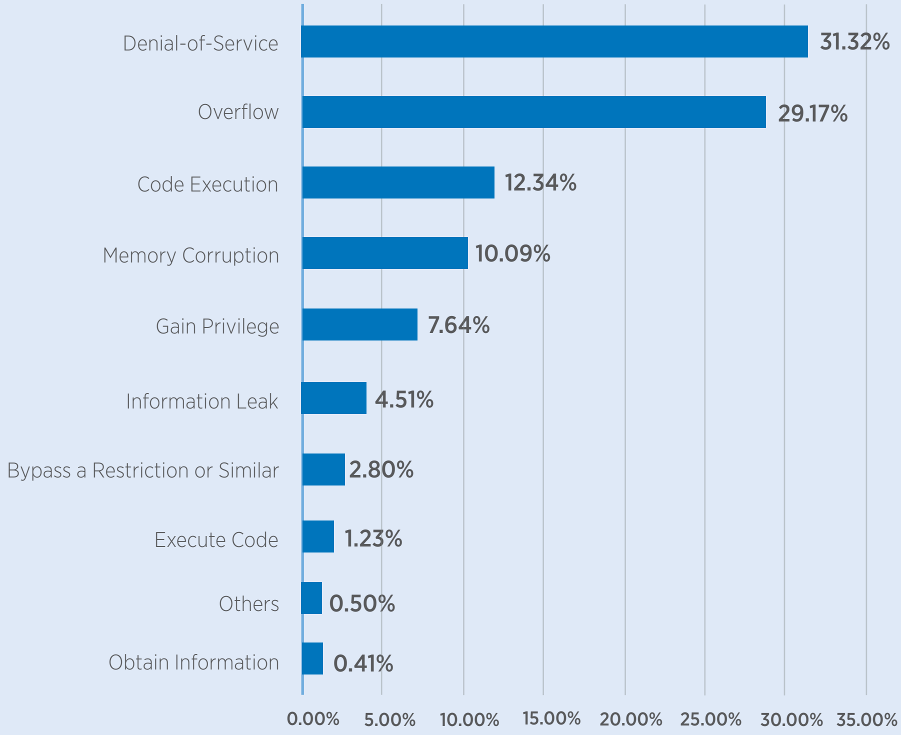


Source: Statista—Cybercrime in Canada Statistics (2022)

From an IoT perspective, any internet-enabled device is vulnerable to being hacked and exploited. As organizations embrace the efficiencies and data enabled by IoT devices, cyberthreat actors are stepping up their efforts by targeting sensitive data, using malware and phishing attacks to exploit network vulnerabilities and disrupt productivity.

Weak authentication remains a serious IoT security concern, with many devices having inadequate security controls in place. While Zero Trust and multifactor authentication look set to become an industry norm, cyber defence teams are focusing their attention on tighter data security, stronger default passwords and improved cyber risk management practices.

According to Bitdefender's 2022 IoT Security Landscape report,[11] the outcome and motivation of an IoT attack involves one or a number of variables:



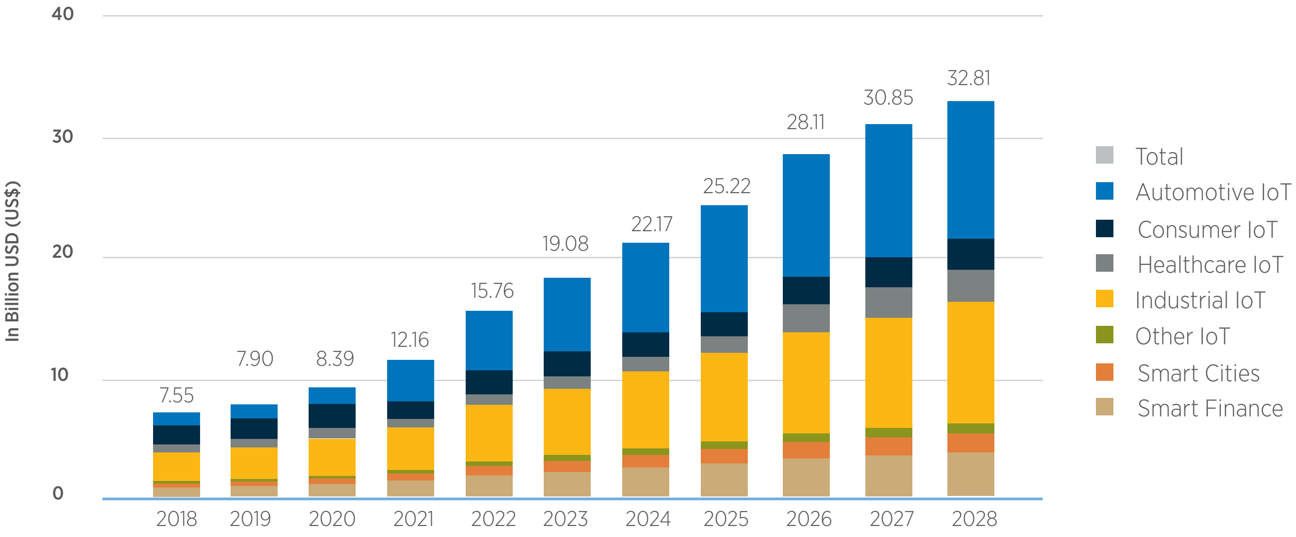
Source: Bitdefender.com—IoT Security Landscape Report (2023)

RISK #1: SMART FACTORIES (IIOT/OT) TO CUSTOMER (IOT)

Canada has emerged in recent years as an IoT leader with a projected market volume of 32.80 billion by 2028.[1] With the rapidly growing number of IoT devices collecting and transferring data, increased convergence and interconnectivity has led to IIoT becoming a pervasive force across industries and sectors, and a key driver of Canada's economic growth plans.

IIoT[15] enabled smart factories (Industry 4.0) leverage technology and data to optimize operations—helping to eliminate unplanned downtime, enhancing decision making and managing supply chain logistics. Cyberthreat actors understand the critical role industry plays in global supply chains and the financial impact of disrupted operations impacting multiple sectors.

Organizations using IoT-generated data to deliver efficiencies and get closer to the end customer are now able to activate a quick fix for identified issues and production bottlenecks before the customer is aware that problem exists. IoT data can also be used to analyze buying patterns and inform production planning.



Source: Bitdefender.com—IoT Security Landscape Report (2023)

Embedding technology into physical objects and the increasing ease of utilizing complex data and 'real time' communication across devices, many industries are exploring and unlocking new use-cases to power growth opportunities and business process improvements. Critical sectors like healthcare, transport, automotive and financial services are connecting infrastructure, supply chain and linking data with service. As always there are pros and cons associated with this.

RISK #2: SCALE OF CYBERSECURITY INVESTMENT OUTPACED BY RAPID DIGITIZATION

With continued including inflation, geo-economic trade tensions, restricted access to investment capital and higher cost of borrowing, business critical programs including cyber defence have been increasingly re-prioritized and funding reduced. Experienced cybersecurity and data risk specialists are harder to come by and command higher salaries.

When developing budgets for cybersecurity, CIOs and risk managers are facing two divergent priorities—1) maintaining operations with tighter cost controls; 2) the pressing need to fund programs that enable longer term operating performance and sustainability, including cybersecurity.

The implementation of IIoT technology targeting operating cost reduction introduces increased cyber risk exposure and vulnerability to attack. Pricing of cybersecurity products and services has also increased while installing new IoT devices rarely involves a 'plug and play' experience, generally requiring operating system updates and/or replacing legacy equipment and machinery to provide adequate data security. The challenge of balancing risk, cost and security with responding to the pace of change will remain on the CTO's agenda for the foreseeable future.

“

Manufacturing operators in Canada can access cyber hygiene information that identifies improvement areas including MFA, EDR tools and O365. One major challenge is the percentage of Canada’s production output delivered by outdated machinery and technology. While these systems may still deliver the required output and quality level, they often don’t connect to new(er) operating systems.

Bringing everything up to speed requires significant capital investment. Replacing machines, robots and tech platforms often requires multimillion-dollar investment to upgrade production software to adequately secure the network.

The problem/challenge is readily understood. Organizations can’t make a wholesale investment at the click of a button to upgrade every single machine to become insurable. The net result is some manufacturers opting out of purchasing cyber insurance and some insurers declining to write insurance for manufacturers unable to upgrade their network where it is viewed as high loss exposure—cyber and business interruption being two of the primary risks, along with lost income.”

Dan Lewis

Director, Cyber Practice—Canada

RISK #3: CONNECTED ECOSYSTEMS EXPAND THE ATTACK SURFACE

Where IoT systems controlling physical operations converge with third-party applications and sensors, the IOT/OT attack surface expands significantly. Security cameras, door locks, and alarm systems provide multiple entry points for hackers to access data and exploit back-end systems. Robust monitoring and maintenance of physical and digital convergence points has elevated to a business critical risk.

IT/OT convergence minus a robust data and network security layer presents an opportunity for hackers to exploit IT access points or cloud vectors, and there are now more known vulnerabilities impacting IoT devices than IT platforms able to effectively combat them.

The risk profile of IoT systems has become more complex when compared to the traditional information technology (IT) threat landscape. Data breaches are becoming more complex and not always instantly evident as threat actors collate information to target IoT attacks to maximize disruption and financial reward.

RISK #4: PHYSICAL SECURITY RISK

IIoT/OT integration and monitoring network connections between digital assets and physical assets continues to be a major concern for cybersecurity teams. While digital assets offer cyber attack entry points for targeting industrial plants and production lines, hackers can exploit physical equipment and machinery, causing unplanned production downtime and machinery malfunction including material changes to specifications and machine settings. The scope, scale of the attack and costs associated with physical security breaches are significant.

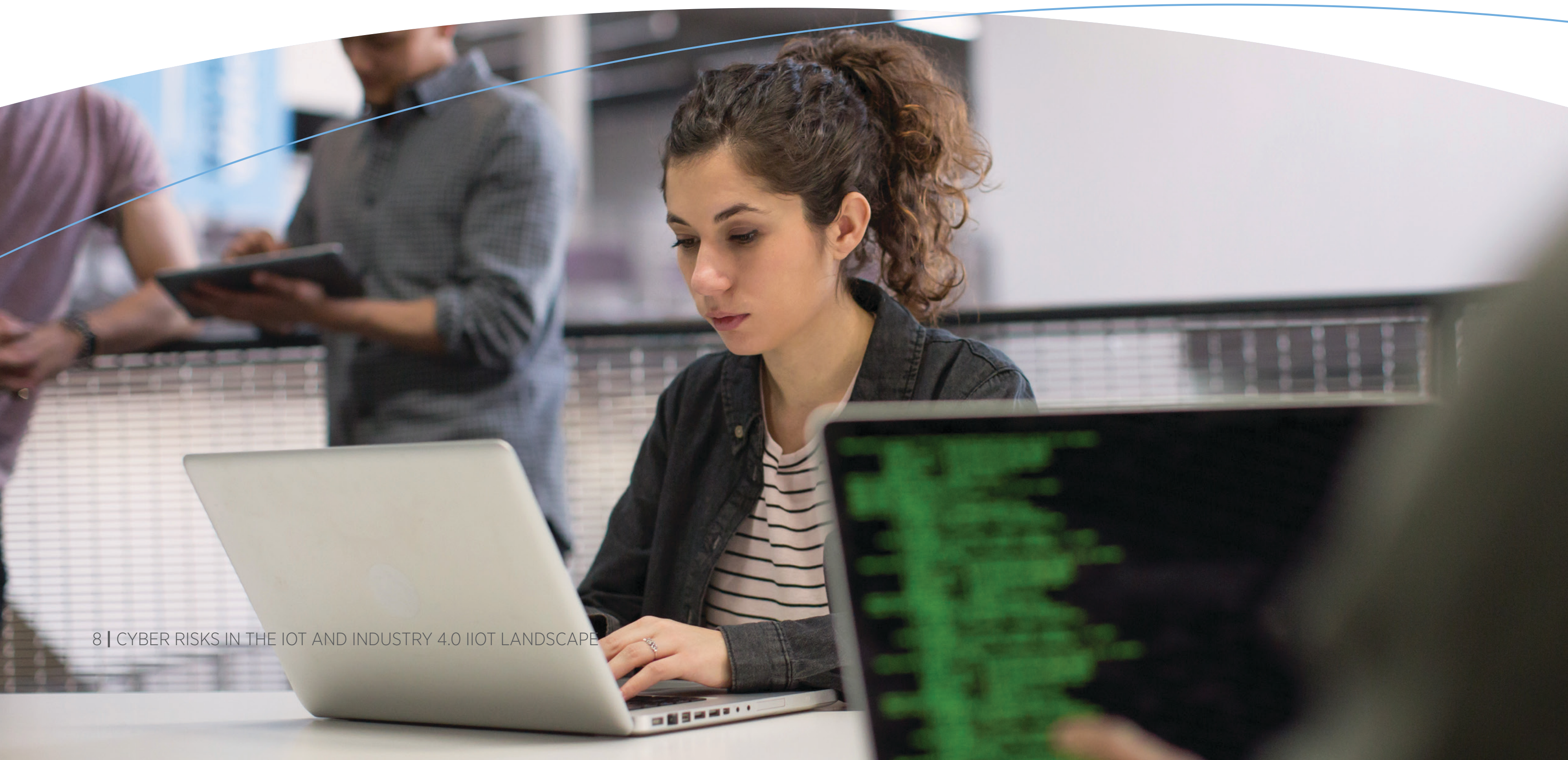
“

Cyber attackers love industrial plants and manufacturing businesses because they’re one of the few industries that if you get ransomware on that network, it quite literally has a minute by minute revenue impact.

As one example, for a manufacturer producing car parts a growing concern in Industry 4.0 is a hacker changing the tolerance or specification of a part being made. Extrapolate that out to a million widgets that are shipped off to BMW or Jaguar Land Rover, they arrive and the team realize that they’re 3 millimeters out. As well as the significant cost of replacing and re-shipping the incorrect part, the big issue is not knowing that the product was wrong in the first place.

A manufacturer can utilize Shodan, an IIoT website that pulls together all of the industrial control systems by brand, and sets out the identified cyber attacks on those systems. For example, Siemens technology has a dedicated section on Shodan listing all of the Siemens connected plants that are vulnerable right now”

Johnty Mongan
Global Head of Cyber Risk Management—Gallagher



RISK #5: PRIVACY CONCERNS

The volume and scope of data held on IoT platforms and the growing number of ransomware attacks is significant cause for concern. Stricter data privacy laws and regulatory governance have placed increased pressure on cybersecurity teams to protect sensitive data and understand the consequences should they fail to do so. Despite the growing sophistication of devices and Zero Trust protocols, data privacy concerns appear to be growing.

Data access permissions included in third party vendor contracts, where data collected from organizations is used to support continuous improvement efforts, has the potential to provide inside information on production processes and commercial position. The general lack of visibility of the data collected and transmitted by IoT devices, and the potential to use this data to track and profile individuals is particularly concerning in terms of commercial IP, medical information and financial data. Tighter vendor due diligence, including close review of data access permissions within contracts, needs to become industry standard practice.

Section 2: Risk Analysis

RISK #1: CYBERSECURITY RISKS IN IOT

As Canadian organizations continue to evolve, enhance and digitize production, a growing number of sectors and services will become prime targets for hackers. Vulnerable IoT devices are subject to a myriad of risks and sophisticated attacks carried out by hackers with malicious intent, and attacks are becoming more coordinated and informed by dark web forums offering tools, knowledge and capability.

IOT CYBER ATTACK IS PERPETRATED IN A NUMBER OF WAYS, INCLUDING:

Malware

Hackers use malware (malicious software) to take control of a network to extract data and/or disrupt critical software and system infrastructure.

Phishing

Hackers run highly targeted email or social media campaigns where they lure and trick people into providing sensitive information.

Advanced Persistent Threats (APTs)

Hackers access data and/or a system for extended time periods to source information to assist with planning a cyber attack.

Ransomware

A type of malware that locks a victim's data or device and threatens to keep it locked unless the victim pays a ransom amount. Double extortion ransomware takes this further, where the hacker exfiltrates and encrypts data and then demands a ransom for both the decryption key and prevention of data leakage.

Trojans

Malware disguised within legitimate software and/or files. Once installed, the trojan enables remote access to the host computer, subjecting the host computer to a variety of destructive or undesired activities.

Spyware

Hackers hide malware inside documents, music, movies and other files, and lure people to download it onto their devices—smartphone, smart-TV, smart watches, for example. Hidden inside operating systems, spyware pulls in and then shares sensitive information without the authority or knowledge of the owner.

DDoS Attacks

Distributed denial-of-service (DDoS) is one of the most used attacks on IoT systems where hackers disrupt the normal functioning of a network by flooding it with excessive requests using botnets.

RISK #2: SERVICE DISRUPTION, PRODUCTION DOWNTIME

Recent industry reporting suggests that IoT devices are being subjected to a growing number of cyberthreats. These typically result in the theft of confidential data, the launch of DDoS attacks, and more.

The most infamous in recent times is Mirai, IoT specific malware used in 2016 to launch targeted attacks on Twitter, Reddit, CNN, Netflix and The Guardian, causing widespread disruption and reputational challenges while highlighting the scope and scale of major cyber attack events.

Concerns of government backed, politically motivated cyber attacks are high among policy makers and industry leaders due to the potential economic and geopolitical turmoil these events could create. These threats have become particularly prevalent in the energy sector as well as manufacturing production lines.

RISK #3: IOT LIFECYCLE MANAGEMENT

Tracking and replacing out-of-date technology to maintain data security is a central pillar of cyber defence strategy.

Legacy IoT sensors capture real-time data and have become high-value targets for attackers aiming to compromise IoT networks and launch lateral data breaches across networks. Many organizations are unaware that IoT devices have an expiry date and consumers are not alerted to the dangers of continuing to use unpatched firmware, with countless outdated connected devices waiting to be infiltrated by opportunistic attackers.

Devices running unsupported operating systems often can't be secured or updated, with the risk of a device becoming "bricked" if an attacker compromises one and it can't be quickly patched. Extending Zero Trust to IoT is challenging on a number of front, as the endpoints vary and the environment is dynamic and filled with legacy devices.

Industrywide standards are urgently needed to regulate IoT device maintenance and security.

RISK #4: THE 'I' BLIND SPOTS IN THE IOT LANDSCAPE

IoT devices become a security liability when connected to the internet, with a growing number of cases of an IP address being pinged from outside the company by hackers looking to identify points of network vulnerability. Most legacy IoT devices weren't designed with security as the #1 priority, lacking the option to automate firmware updates and patches. The primary issue is that traditional vulnerability management tools do not scan past the operating system.

Closing internet blind spots in IoT sensors is essential to resolve unmanaged or unsupported legacy systems. With greater visibility and analysis across IT and OT systems, cybersecurity teams can quickly identify and address problems before threat actors exploit them.

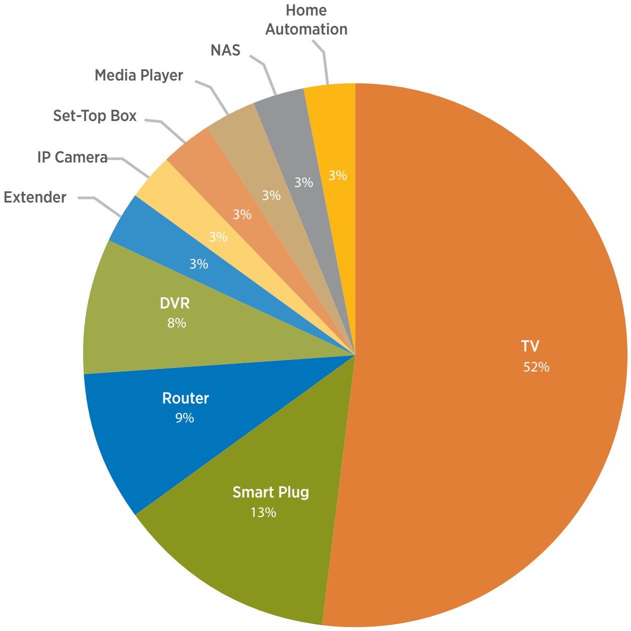
RISK #5: VULNERABLE DEVICES AND ATTACK SURFACE AREAS OF IOT

The attack surface of an IoT environment can be generally divided into three groups. Any security loopholes in them will lead to a fatal security incident.

- **Devices**: Threat actors looking for vulnerabilities in memory chips, firmware, physical/web interfaces and network servers are able to take advantage of insecure device-settings, components, and irregular system updates. Depending on the industry and application, a patch is not always available to close security gaps.
- **Communication channels**: Hackers targeting communication/data channels that connect IoT components can impact the entire system, making it easier for hackers to execute DDoS, phishing and spoofing.
- **Applications and software**: A prize target for hackers seeking to exploit sensitive information and user credentials using malware to cripple an entire system/platform.

Attack surfaces can change due to the nature of devices and the motivation behind individual attacks. For example, the IIoT attack surface is more focused on a) endpoints and legacy devices, b) vulnerable systems, c) proprietary software, and d) communication platforms.

According to the Bitdefender's IoT Security Landscape report, the most vulnerable IoT devices in 2022 were:



Statistics source: www.bitdefender.com/files/News/CaseStudies/study/429/2023-IoT-Security-Landscape-Report.pdf

Section 3: Will Iot Related Cyber Events Become the Norm or Will Defence Adapt Faster?

IoT/IIoT/OT cybersecurity has reached a critical point and the challenge now facing Canadian business operators is how to stay one step ahead.

With IoT attacks predicted to double by 2025 and the rapid pace of digitization transforming the industrial landscape with IoT, 5G, Cloud networks and digital supply chain integration becoming the norm, industry is more vulnerable to cyber attack, and defence strategy needs to step up to the challenge.

The evolution of the BYOD workplace further increases the cyberthreat landscape, and the convergence between business and householder data networks across multiple devices evolves, with roughly 43 billion active IoT-connected devices predicted to be communicating and transferring data worldwide by 2025. And the more interconnected devices become, the greater the cyber risk exposure becomes.

Accelerated implementation of Zero Trust security frameworks for IoT devices on remote and hybrid cloud environments as well as the security of data accessed by supply chain partners are two of the key priorities for IIoT cyber risk mitigation strategy.

The solution rests on robust prevention and sustained investment in defence—securing IoT points of convergence, monitoring legacy devices, using data analytics as part of an early issue detection strategy, and strategic investment in robust cyber risk management. Coordinated action and partnership at a cross-industry level. Applying IoT data to enable risk managers and CTOs to analyze and model their cyber exposure profile, having a deeper understanding of systemic risk(s) for specific industries and setting out clear(er) expectations and embedding risk management processes for the application of technology will help organizations to move forward with increased confidence.

CITATIONS

[1] IoT and IIoT growth in Canada Internet of Things - Canada | Statista Market Forecast
[2] Revenue in the consumer IoT market in Canada Consumer IoT - Canada | Statista Market Forecast
[3] Global IIoT market Global industrial Internet of Things market size 2028 | Statista
[4] Cyber attack on IoT worldwide Annual number of IoT attacks global 2022 | Statista
[5] Organizations detecting attacks on IoT devices/systems IoT Security Primer: Challenges and Emerging Practices (gartner.com)
[6] Growth of IoT market in Canada Internet of Things - Canada | Statista Market Forecast
[7] IoT Revenue by segment Internet of Things - Canada | Statista Market Forecast
[8] Worldwide IoT attacks Monthly number of IoT attacks global 2022 | Statista
[9] Mirai botnet hack DDoS attacks on Dyn - Wikipedia
[10] Outcome of IoT attacks 2023-IoT-Security-Landscape-Report.pdf (bitdefender.com)
[11] Most vulnerable IoT devices in 2022 https://www.bitdefender.com/files/News/CaseStudies/study/429/2023-IoT-Security-Landscape-Report.pdf
[12] OWASP recommendations on IoT security OWASP Internet of Things | OWASP Foundation
[13] shodan.io Shodan Search Engine Shodan is the world's first search engine for Internet-connected devices and a search engine for the Internet of Everything
[14] Gartner. IoT Security Primer: Challenges and Emerging Practices (2020)
[15] What is IIoT? Sap.https://www.sap.com/uk/products/scm/industry-4-0/what-is-iiot.html

In one of the most infamous IoT hacks, the Mirai botnet hack, hackers used a botnet of IoT devices and managed to cripple important servers and brought huge sections of internet down. Twitter, Reddit, CNN and Netflix were affected by this attack. According to reports, hackers managed to execute this large-scale attack through a botnet which infected many internet-connected devices—such as printers, cameras, residential gateways with malware.

Connect With Us

To find out more about any of our services, please get in touch with:

Cyber Practice
CyberRM@ajg.com

Gallagher

Insurance | Risk Management | Consulting

AJG.com/ca **The Gallagher Way.** Since 1927.

Arthur J. Gallagher Canada Limited ("Gallagher") provides insurance, risk management and consultation services for our clients in response to both known and unknown risk exposures. When providing analysis and recommendations regarding potential insurance coverage, potential claims and/or operational strategy in response to national emergencies (including health crises), we do so from an insurance/risk management perspective, and offer broad information about risk mitigation, loss control strategy and potential claim exposures. We have prepared this commentary and other news alerts for general informational purposes only and the material is not intended to be, nor should it be interpreted as, legal or client-specific risk management advice. General insurance descriptions contained herein do not include complete insurance policy definitions, terms and/or conditions, and should not be relied on for coverage interpretation. The information may not include current governmental or insurance developments, is provided without knowledge of the individual recipient's industry or specific business or coverage circumstances, and in no way reflects or promises to provide insurance coverage outcomes that only insurance carriers control.

Gallagher publications may contain links to non-Gallagher websites that are created and controlled by other organizations. We claim no responsibility for the content of any linked website, or any link contained therein. The inclusion of any link does not imply endorsement by Gallagher, as we have no responsibility for information referenced in material owned and controlled by other parties. Gallagher strongly encourages you to review any separate terms of use and privacy policies governing use of these third party websites and resources.

Insurance brokerage and related services to be provided by Arthur J. Gallagher Canada Limited and its affiliates and/or subsidiaries.