How to Overcome IoT Security Concerns

A report in the IoT InfoBrief Series, Sponsored by Bell | May 2017

IDC
Analyze the Future

Manage Risk, Don't Avoid It

Fifty-two percent of medium and large Canadian organizations have already adopted Internet of Things (IoT) solutions in order to gain benefits such as reduced costs and improved customer experiences. What is preventing the other 48% from jumping on the bandwagon?

IDC research shows that the second highest concern for Canadian IoT deployments is security. Every week brings news of cybersecurity crises. IoT is increasingly both the target and the distribution mechanism for hackers.

Is the threat from connected smart devices a reason to avoid IoT? No.

IDC strongly believes the answer is that **organizations need to manage risk, not avoid it.** The potential of IoT to improve efficiency and productivity, and create new revenue streams and business models is too compelling to be overshadowed by security concerns that can be effectively mitigated. Adopting and following security best practices will guard IoT initiatives against security threats.

IoT Security Vulnerabilities

How does IoT change the security equation? The table below highlights some key vulnerabilities that differ from traditional IT security issues. This report highlights best practices to address these IoT vulnerabilities.

Endpoints and Devices

Endpoint and devices are:

- Physically available: In-person attacks are possible.
- Computationally lightweight: It's more difficult to enforce encryption requirements.
- Promiscuous by nature: They are designed to "talk" with each other. This chatter means devices may be attacked from other devices in the IoT "daisy chain."

Network

IoT solutions rely on connectivity. Unlike legacy M2M/SCADA solutions, IoT solutions:

- Use public or private networks that are linked to core business applications.
- Can operate outside of traditional firewalls.
- May transmit information that should be encrypted as it moves through the network.
- Can make it harder for network administrators to catch or flag rogue devices or behaviour.

Data and Applications

The crucial element is the underlying data being transmitted from endpoints to internal systems and databases. Vulnerabilities include:

- Authentication attacks in which user names or passwords are guessed through automated trial and error processes.
- Outdated database and application versions and patches.
- Lack of ongoing monitoring.
- Failure to encrypt data.

Endpoint and Device Security Best Practices

Price reductions in connected sensors and modules are one of the key reasons IoT has risen in prominence over the last few years. Canadian businesses need to focus on securing them while capturing the benefits that IoT brings.

- **Ensure that IoT endpoints have policies to enforce password configurations.** The sheer scale of connected devices being shipped globally (30 billion devices in 2020 worldwide) means the manufacturers' default password settings will be known to hackers. Implementation plans need to ensure configurations are routinely updated and devices authenticated using unique, dynamically generated keys. There should never be default passwords or unprotected connected devices. Use tamper-resistant hardware such as SIMs to store identity, authentication, and authorizations.
- **Use a respected third party, such as a mobile network operator, to conduct end-to-end device certification before deployment to enhance security.** Some providers combine device and network services authentication and encryption. Non-registered devices are ignored and security is built around only authenticated devices.

As edge devices are taken out of service, erase all the sensitive data on them. Ideally, use the IoT platform software to remotely decommission, providing an auditable trail.

- **Enable ongoing device monitoring and management.** Companies need to proactively monitor device configuration changes, authentication attempts, and inbound communications to catch threatening actions and upgrade devices. IoT management platforms allow customers to monitor endpoints. Some IoT platforms automatically send alerts if a SIM is moved to a rogue device, enabling the client to shut down the SIM.
- **Regularly audit connected devices.** Organizations need to know how many devices they have, what those devices are, where they are, and when they have last been used.
- **Avoid devices that offer unnecessary capabilities to support their core service and function.** Having edge devices with unneeded incremental functions — whether cameras, microphones, or other options — introduces unanticipated vulnerabilities.
- **Plan for decommissioning.** As edge devices are taken out of service, erase all the sensitive data on them. Ideally, use the IoT platform software to remotely decommission, providing an auditable trail.

Don't count on "security through obscurity." The idea of hiding in the vastness of the internet simply doesn't work. There are search engines such as Shodan.io that let anyone search for connected physical devices from baby monitors to industrial control systems (ICS). Devices will be found and exploited, so obscurity is not a feasible approach.

Network Security Best Practices

The network will play a critical role in the detection, response, access, and policy enforcement for enterprise IoT.

- **Keep your IoT solutions on distinct networks from the core internal network.** There's no reason for the building's HVAC units to be on the same network as your firm's payments or financial systems. Devices deployed on internal networks or private clouds have more protection against attacks, but still require strict authentication and restricted access to common communications ports (TCP, FTP, etc.) to secure against inappropriate employee access. Partition your networks to keep key processes separate. Public wireless networks (cellular) offer robust security and isolate your IoT solution, limiting exposure in the event of a breach.
- **Consider using a private access point name (APN) and authorized universal integrated circuit cards (UICC or SIM).** This will decrease the threat surface compared with relying on the public internet.

Devices deployed on internal networks or private clouds have more protection against attacks, but still require strict authentication and restricted access.

- **Implement wireless monitoring solutions** that discover the endpoints, determine whether they are legitimate, shadow, or hostile, and then track them within a specified location so they can be deactivated or recovered. This is very similar to deploying enterprise mobility management solutions for smartphone and tablet deployments. IoT platform software like Jasper can have automated alerts if the international mobile equipment identity (IMEI) number changes, so network administrators can investigate and deactivate the UICC as needed. Monitoring solutions can be deployed by IT or outsourced to third parties that can monitor devices 24 x 7.
- **Deploy edge firewall solutions** to manage communications between an intelligent system and its upstream components on the internet.
- **Ensure strong encryption for in-flight data.** In addition to Secure Socket Layer/ Transport Layer Security Protocol (SSL/TLS) used with an IP server connection, cellular networks and devices add a further layer of security.
- **Consider the duration of connectivity.** Do endpoints need to be connected to the internet 24 x 7 x 365? This exposes the system to greater ongoing risks than batch- or exception-based communications. Consider using network controls to limit the time of day or duration of connectivity.
- **Restrict common communications ports.** By closing down ports that devices can connect to (e.g., TCP, FTP, etc.), it reduces the threat surface that hackers can target.

Monitor and control local communications among servers and storage.

Server and Storage Best Practices

Server and storage components can vary greatly depending on the IoT use case. These components may also be local, in datacentres, at a service provider location, or in a service provider's cloud.

- **Activate server and storage identification and authentication.** Increasingly, hardware comes with identification and authentication tools which just need to be activated and used. Repurposing legacy equipment can lead to issues in this regard.
- **Deploy application control solutions to "harden" servers and storage solutions.** These solutions apply to systems that are receiving the data from sensors and devices at the local level or from the internet.
- **Consider building on cloud PaaS and IaaS.** IDC expects an install base of more than 30 billion connected endpoints by 2020. Cloud allows organizations to deal with the variable workloads from these devices but more importantly it provides an architecture that has the scalability and flexibility crucial for the deluge of data.
- **Adopt "next-generation security" approaches.** IT needs to move away from using a static but constantly updated database of threats toward using algorithmic and/or machine learning based approaches.

Attackers often target servers and storage because of the large amount of information they house.

Database Security Best Practices

IoT solutions generate significant amounts of data. For example, Bombardier's new C Series jetliner uses Pratt & Whitney engines with 5,000 sensors, generating up to 10 gigabytes per second. Organizations need to focus on securing their databases, data warehouses, and data lakes.

- **Evaluate the value of your data** to potential attackers and prioritize your security investments accordingly. Mission-critical data or deeply sensitive information like financials, research and development, or customer data needs to be protected to a higher extent.
- **Encrypt any data at rest to ensure confidentiality** and that the information can only be read by appropriate parties. This typically means leveraging solutions your organization is already using.
- **Make it impossible to compromise administrator credentials and other default IDs.** Traditional attacks such as phishing will target these identities in order to take control of databases and applications.
- **Engage in dynamic testing** prior to going live in order to expose (and fix) exploitable vulnerabilities, including SQL injection, cross-site scripting, and cross-site request forgery attacks.
- **Undertake intensive monitoring of file system integrity, subtle system processes, and employee behaviours.** Antimalware and targeted detection technologies are adding behavioural analysis capabilities to identify advanced malware designed to evade signature-based defences. Consider cloud-based IoT solutions that offer enhanced security and monitoring allowing internal IT resources to focus on their core competencies.

Applications Security Best Practices

Enterprise applications are both systems of action and of record. That is, they can be used to do things and then to create documentation of those actions. As a result, it is critical to ensure their confidentiality, integrity, and availability.

- **Update and patch software as soon as possible.** IT threats are spreading faster than responses, making companies that delay applying updates more vulnerable. Consider adopting cloud-based solutions in which the provider continually monitors and updates its applications, freeing IT resources from this task.
- **Limit employee access to systems outside of their role and requirements.** One of the simplest attack vectors is to use employee IDs from unrelated departments to access more critical roles, thereby moving up the ladder of corporate vulnerabilities. Companies need to secure their applications by role in order to prevent this daisy-chain style attack.
- **Establish logical isolation by process.** Modern connected machines, whether cars or manufacturing equipment, are complex, interdependent systems with thousands of sensors and actuators. Software design needs to isolate different processes so that a breach in the infotainment systems cannot be expanded into an attack on the drivetrain or steering components.
- **Investigate the security maturity of your key IoT suppliers.** If an objective, comprehensive assessment is beyond the capabilities of your IT and procurement teams, then select consultants with the experience, scope, and ability to assess the security vulnerabilities of your IoT solutions.

Additional Security Best Practices

1 Make Security Everyone's Responsibility

Line of business funds 60% of IoT projects in Canada. Yet these business leaders want to leave security solely up to the IT department. As business strategy embraces connected solutions, line-of-business leaders need to step up and embrace their responsibility to integrate security by design into the products and processes, which means funding staff and technologies to do so. Business leaders are the best suited to understand their regulatory environment, the relative value of their data, and the industry-specific operational risks of a breach. Whether they like it or not, security is now an important part of the job for Canadian business executives.

2 Change Your Security Approach

Security is in a constant state of evolution. Over the past 10 to 15 years, the industry has changed from focusing on "securing the perimeter" to prevent an attack, to a practice of quickly "detecting the enemies amongst us" and recovering when a breach occurs. This switch is crucial for organizations launching IoT initiatives, but the good news is that it reflects the overall drive for improved resiliency in the tech sector and especially the cybersecurity world.

3 Deploy Multiple Solutions

There is no silver bullet to secure IoT systems, meaning that IoT risks cannot be successfully addressed by a single security product. IDC recommends deploying multiple layers of security solutions to proactively manage risk with IoT. Consider whether your organization should deploy the following:

- Communications encryption to protect the communications between the intelligent systems and the management systems. Often these communications are more sensitive since they might include aggregated information, sensitive management reports, or control channel data.
- Edge firewall to manage communications between an intelligent system and its upstream components on the internet.
- IoT security gateway to provide combined security capabilities such as filters, detection, and encryption to local systems.

IoT intrusion detection to monitor the local communications among system components and identify inappropriate devices or sensors. These solutions maintain state tables to track devices and recognize anomalous communications. They may require custom devices that decode protocols and analyze the network traffic accordingly.

4 Consider Managed Security Services

It is increasingly common for Canadian firms to turn to a qualified third party to cope with security burdens. Many organizations do not have the experience, time, or budget to deal with the evolving threat landscape. There is an increasing number of industrial control systems (ICS) zero-day vulnerabilities (flaws unknown to the software provider) being published online. Retaining qualified cybersecurity staff is an ever-more common problem for Canadian businesses.

Managed security services providers can either assist or take over securing systems and networks completely. These providers have more highly trained resources and tools which can detect and defend against an attack faster than most organizations. Using managed security services to assist with IoT deployments can improve security while freeing up IT staff for more strategic initiatives.

There are widely recognized guidelines to align your IoT's security controls and processes such as ISO/IEC 27001:2013, ISO 27018, the US Federal Risk and Authorization Management Program (FedRAMP), and the NIST Cybersecurity framework. **Organizations should benchmark their own efforts or choose certified vendors to build in security from the outset.**

Manage IoT Security Concerns Through Proactive Response

IoT introduces new vulnerabilities, but organizations can manage these by:

1. Identifying vulnerabilities (physical and virtual) in endpoints, networks, databases, and applications
2. Implementing technologies, policies, and procedures that reduce identified vulnerabilities, and keeping these current
3. Proactively monitoring all the layers in their stack to detect threat and breaches

Canadian businesses aren't abandoning email, web servers, or social media technologies just because of the security threat they pose. The Internet of Things needs to be considered in the same light — the benefits and value are too great to ignore because of cybersecurity concerns that can be addressed with the right technology, processes, and partners.

To learn more about IoT security best practices, contact a Bell Business Representative now or visit www.bell.ca/IOT