VIEWPOINT

ARTHUR D LITTLE
2022

SUCCESSFULLY MANAGING IOT CYBERSECURITY RISKS

The importance of a holistic framework to protect your business

We are currently witnessing an enormous increase in both industrial and consumer Internet of Things (IoT) deployments across a range of sectors, from smart mobility to industrial uses. However, this growth is not being matched by a corresponding focus on IoT security, dramatically increasing risk for businesses across their ecosystems and supply chains. As a path forward, this Viewpoint outlines a holistic framework and approach to successfully manage the IoT cybersecurity challenge.

AUTHORS

Philipp Mudersbach

Tim Christoph

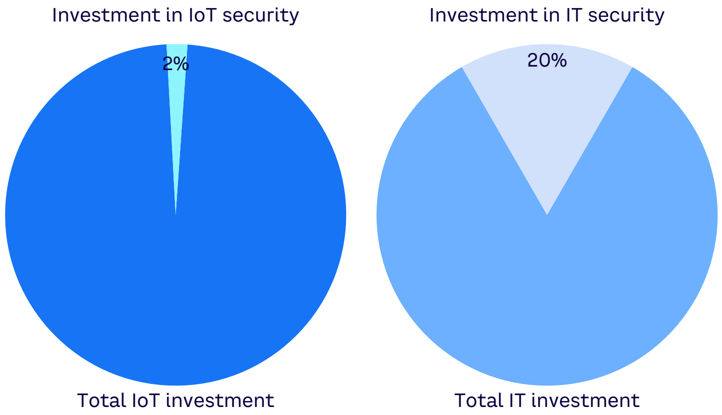
Moritz Kandt

GROWING IMPORTANCE OF IOT SECURITY

By extending the use of smart, connected devices to collect data and monitor processes, the IoT enables transformational change across consumer and industrial uses. (In industrial contexts, the IoT is usually called the Industrial Internet of Things [IIoT]. However, because cybersecurity is equally relevant for both industrial and consumer use cases, in this Viewpoint we use "IoT" to describe both areas.) It delivers higher efficiency, greater innovation, and allows new ways of working and connecting to customers. Its impact is being felt across all industries, including smart agriculture, smart homes, education, industry, healthcare, retail, mobility, grid/energy, government, and smart cities. Using IoT sensors to monitor vaccine cold chains during the pandemic is a prime example of the benefits the technology can provide (see Appendix).

Demonstrating the pervasiveness of the trend, a recent International Data Corporation study estimates IoT spending will top US $1 trillion in 2022. And Statista predicts the market size for industrial IoT applications alone will reach $111 billion by 2025. However, this expansion brings increased cybersecurity risks. IoT adds a substantial number of new end points for organizations to protect, many of which may be out of the direct control of a company's IT team. Moreover, IoT devices tend to be deeply interconnected, creating a greater risk of cyberattacks spreading from them throughout the company network. At the same time, organizations face an overall rise in cyberattacks — both from private individuals and state actors — that are increasing in complexity. Whether the objective is espionage, extortion through ransomware, or simply to cause malicious damage, these groups will always target the easiest way into an organization. Therefore, businesses must take a forward-looking approach that protects them both now and in the future.

Figure 1. Relative spend on IT and IoT security



Source: Arthur D. Little, "Hiscox Cyber Readiness Report 2021," IDC, Statista

Currently, IoT represents a weak point due to a combination of underinvestment, the complexity of technology, and unclear security responsibilities. For example:

- Cybersecurity makes up about 20% of a normal IT budget, but less than 2% of IoT budgets (see Figure 1). This underinvestment in cybersecurity prevention opens the door for attackers to infiltrate a company's equipment.
- IoT ecosystems normally contain a large number of disparate devices, often deployed externally to company networks or in areas traditionally run by operational technology (OT) rather than IT teams, such as factory control systems. All such devices can pose severe security risks.
- Responsibilities for IoT security can be blurred between IT, OT, and external providers, leading to a piecemeal approach. This undermines the holistic response required to effectively prevent cybersecurity attacks that normally cross over internal organizational boundaries.

Consequently, companies need both to invest more and take a whole ecosystem approach to IoT security risks. As we define it, the IoT ecosystem consists of every device and service connected to the IoT network. It includes internal and external devices/services, all of which must be protected from a range of risks — from online attacks to physical threats and the consequences of human behavior and actions. This is broader than traditional cybersecurity. As such, organizations need to look beyond their own firewalls to understand risks, manage threats, and ensure ongoing secure operations.

We are already seeing cyberattacks that use IoT hardware to target consumers as well as organizations, including the following examples:

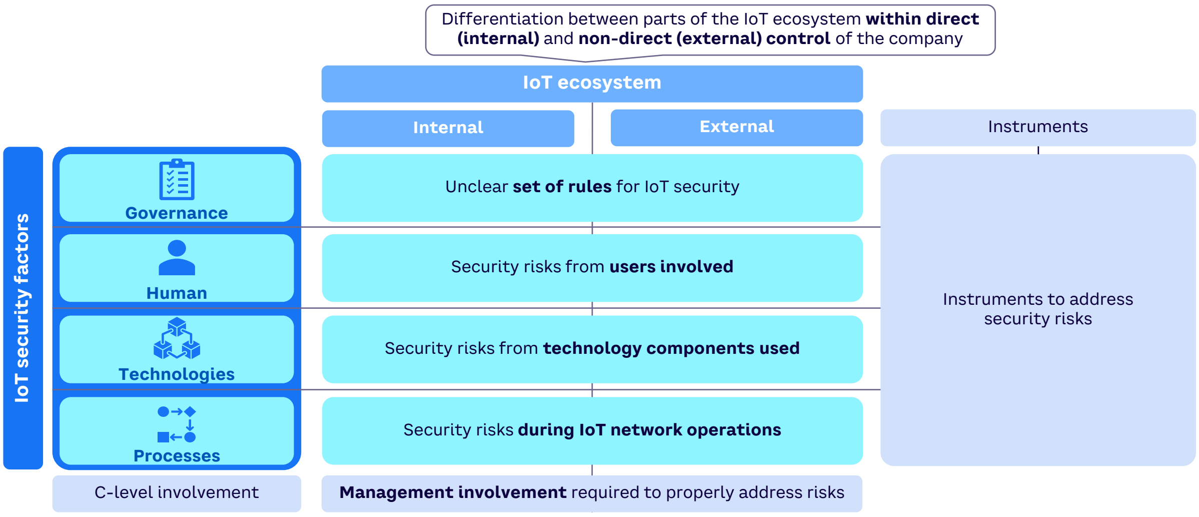
- **Ring.** Amazon-owned smart home company Ring provides a range of connected devices, from video doorbells to security cameras and alarms. It suffered a hack when criminals exploited weak, recycled, and default security credentials to access live feeds from the cameras around customers' homes. Hackers were even able to communicate remotely using the devices' integrated microphones and speakers, harassing customers in some cases. In addition to causing customer distress and reputational damage, Ring is currently the target of ongoing legal actions, including a class-action lawsuit for $5 million.
- **Oldsmar water supply.** In Oldsmar, Florida, USA, an intruder was able to hack into the system that controls the town's water supply using remote-monitoring software and then boosted the level of sodium hydroxide (lye) in the water supply to 100 times higher than normal. While the change was detected and cancelled by an operator before it went into effect, the potential consequences for public health were catastrophic — lye poisoning can cause burns, vomiting, severe pain, and bleeding.

A FRAMEWORK FOR HOLISTIC IOT SECURITY

Given the increasing importance of IoT to business operations, the time to act on security is now. However, organizations should not only invest more in IoT security. Unless this spending is coupled with the right IoT security risk management, it will potentially be wasted.

Based on ADL's Cybersecurity Matrix, outlined in a previous Viewpoint (see "Being Concerned Is Not Enough"), we have developed the IoT Risk Assessment Framework (see Figure 2) with a specific focus on risks related to an organization's IoT devices. By applying the holistic framework, companies can understand and mitigate risks across their IoT ecosystem. The framework distinguishes between internal and external activities and requires organizations to understand and include areas that are outside their direct control or influence, such as external service providers and partners across the supply chain. Often, companies focus only on the areas of the ecosystem within their direct influence, failing to account for risks from external service providers.

Figure 2. IoT Risk Assessment Framework


Differentiation between parts of the IoT ecosystem **within direct (internal)** and **non-direct (external) control** of the company
IoT ecosystem
Internal
External
Instruments
IoT security factors
Governance
Human
Technologies
Processes
Unclear **set of rules** for IoT security
Security risks from **users involved**
Security risks from **technology components used**
Security risks **during IoT network operations**
Instruments to address security risks
C-level involvement
Management involvement required to properly address risks

Note: Codeveloped with Infinity Grey Ltd. on the basis of its Cyber Maturity Model and embedded Enterprise Cybersecurity Architecture Framework.
Source: Arthur D. Little

The framework covers four different factors as part of a company's operational readiness to handle cybersecurity risks (see Figure 3):

1. **Governance** — unclear rules and governance structures that hamper the safe use of IoT devices. For example, unaligned policies between internal and external IoT devices.
2. **Human** — security risks caused by human error or malicious activity. For example, not all internal/external staff may have received sufficient training to work securely with IoT devices.
3. **Technology** — security risks from issues with hardware, software, and services. Often companies are unaware of external risks within bought-in hardware or services due to a lack of detailed due diligence. Similarly, the growing number of IoT devices used within production technology may not be known to IT or may not be managed under existing security policies.
4. **Processes** — security risks caused by poor processes within the operation of the IoT network. Issues arise particularly when processes span different parts of the business and/or involve external providers.

BUSINESS SHOULD ENFORCE IOT SECURITY FACTORS THROUGH CLEAR SERVICE-LEVEL AGREEMENTS

Strong C-level involvement must underpin the framework. This requires alignment at the board level between IT and OT so that IoT security factors cover all connected devices. Responsibilities, security standards, and approaches must be set out clearly and standardized across IT and OT. The aim is to create holistic, transparent IT/OT environments across the business so that all assets connected to the network are covered by guidelines. Business should enforce IoT security factors through clear service-level agreements and manage those factors through an overall IT/OT security council that involves all stakeholders.

Figure 3. IoT Risk Assessment Framework, with examples

		IoT ecosystem		
		Internal	External	Instruments
IoT security factors	Governance	• Unclear set of rules for local IoT network • Governance structure lacks defined roles and responsibilities related to IoT cybersecurity	• No agreed rules with service provider • External standards differ vastly to internal standards	Rulebook with standard and clear roles (e.g., security architect)
	Human	• Employee gives unintentional access to network • Employee does not properly configure or set up IoT network	• Inconsistent data availability creates opportunities for external threats • Communication errors lead to network connections being interrupted	Training, building risk culture, raising awareness with partners, such as through contractual terms
	Technologies	• Owned devices use unsecure protocols to communicate • Access to the network through another protocol (e.g., Bluetooth)	• Rented IoT platform solution (PaaS) is hacked • Software update is either improperly executed or contains security flaws	Defined requirements (e.g., ISO), audits
	Processes	• Inconsistent data availability creates opportunities for external threats • Communication errors lead to network connections being interrupted	• Communication protocol to external interface not deployed correctly • Due to low service-level agreements, fixing errors takes too long within daily operations	Monitoring, process audits
	C-level involvement	CIO, CTO, COO, CEO		Regular risk meetings

Source: Arthur D. Little

THE ASSESSMENT PROCESS

In a complex environment, with multiple internal and external players, implementing an effective IoT security framework can appear challenging. Organizations have the choice between standards from ISO, IEC, or the US National Institute of Standards and Technology (NIST). Among the options, ADL recommends adopting the NIST framework due to its more holistic approach and easier mapping. The approach must be comprehensive, following NIST's five-stage model:

1. **Identify.** Create an inventory of all network-connected IoT devices across the business and in use by external providers within the supply chain. Create a full asset register, identifying and logging potential risks, including possible future risks. Determine where are the strengths and potential weaknesses. Confirm that suppliers meet security standards (e.g., ISO) within their own operations and ensure all employees are properly qualified and certified.
2. **Protect.** Put in place the governance, controls, and training to mitigate risk and ensure security. Begin with the most pressing weaknesses to ensure major issues are covered quickly. Implement safeguards around access control, data security, and information protection — inside and outside the organization. Run regular awareness training with all relevant employees and contractors, including simulated attacks.
3. **Detect.** Develop and implement full security monitoring across the ecosystem, including OT and external providers. Focus on clear processes to detect anomalies and events, with well-understood escalations to named individuals.
4. **Respond.** Have a full plan in place to launch immediate responses in the event an IoT security attack is detected. This should include both internal and external communication and actions to be taken across the ecosystem. Responses should be frequently tested and subject to a process of continuous improvement.
5. **Recover.** Develop and implement appropriate activities to maintain plans for resilience and restore any services that are impaired due to IoT security breaches. Recovery plans should include short-term mitigations to reduce business disruption, and longer-term improvements to the human, technology, and process parts of the framework.

> IMPLEMENTING AN EFFECTIVE IOT SECURITY FRAMEWORK CAN APPEAR CHALLENGING

CONCLUSION

PUTTING SECURITY FIRST FOR IOT

SECURITY IS CURRENTLY A LOW PRIORITY, PUTTING COMPANIES AT RISK

The clear benefits of the IoT are driving massive growth and investment in the technology, particularly in industrial and supply chain scenarios. However, security is currently a low priority, putting companies at risk. Organizations therefore need to focus on:

1. **Creating a comprehensive IoT security framework** that spans the ecosystem and includes OT alongside traditional IT.
2. **Covering more than just technology** to incorporate the risks from people, processes, and governance.
3. **Understanding the roles** of both the internal and external parts of the ecosystem, through a holistic view of the entire IoT estate.
4. **Enforcing standards** through C-level involvement.

Taking this approach will help unleash the benefits of IoT while ensuring secure, uninterrupted operations.

APPENDIX — IOT SECURITY IN VACCINE COLD CHAIN

The COVID-19 pandemic and subsequent vaccine rollouts have demonstrated the importance of IoT in the pharma cold chain — and the risks that require identification and mitigation. Put simply, if many vaccines exceed certain temperatures or are damaged en route, they lose effectiveness, putting lives at risk. Thus, the cold chain cannot be interrupted. It's a perfect example of how the IoT security framework can work across the supply chain ecosystem.

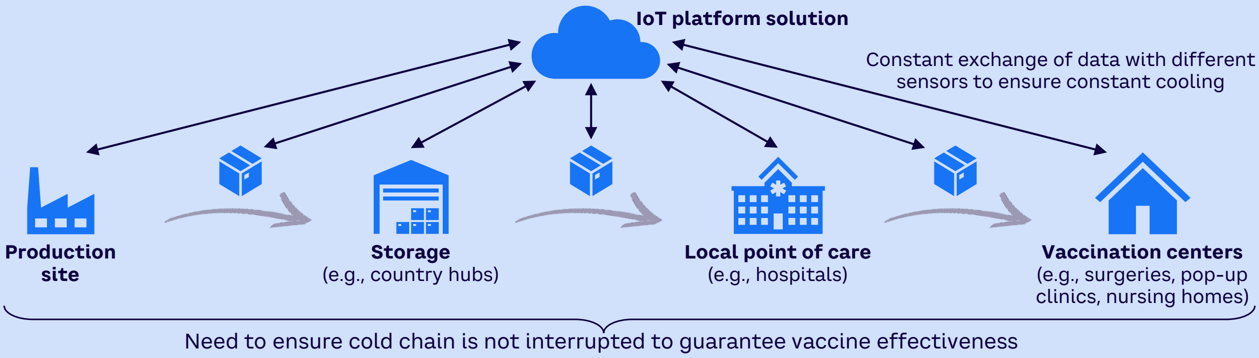
The pharma cold chain is complex and involves multiple players and locations (see Figure A). It stretches from the vaccine production site to storage facilities (potentially in other countries), to the local point of care (e.g., hospitals), and to vaccination centers (e.g., surgeries, pop-up clinics, and care homes). It involves a diverse mix of people from multiple organizations — from production employees to drivers/couriers at logistics companies and medical staff at hospitals/clinics.

The vaccine's condition is monitored by IoT sensors in its packaging, which relay information to a cloud-based IoT monitoring platform. Data is then shared with the organizations responsible for vaccine rollouts — whether health providers, governments, or the pharmaceutical company itself. Potential issues, along with mitigations, may include the following factors:

- **Governance.** Imprecise cybersecurity responsibilities prevent the sustainable implementation of cybersecurity standards across the supply chain. Ensure clear responsibilities by establishing an overarching governance structure and formalized rules that include all relevant ecosystem partners.
- **Human.** An employee at a production site connects cooling sensors to an unsecure network or a delivery driver leaves a truck door open, enabling physical access to tamper with sensors. Prevent this by training employees on the proper use of sensors, backed up by specific rules and a defined emergency plan.
- **Technology.** Internally, legacy systems connected to the IoT network are not properly protected, or externally, the monitoring solution suffers a security breach. Guard against such risks through an IT security audit of the whole ecosystem, including external providers, before the vaccine rollout begins.
- **Process.** Inconsistent data transfer can occur during the handover between the production facility and transportation stage of the process. Issues may also occur in plane cooling systems during flights. Regular process audits that bring together relevant ecosystem partners can identify such risks, enabling their prevention.

To enable success, all these factors must be enforced and underpinned by C-level involvement. Regular risk meetings should identify emerging issues and continuously improve the framework to safeguard the cold chain. While this example model covers the pharma cold chain, it applies equally to other industries, particularly those with complex, IoT-controlled supply chains.

Figure A. The vaccine cold chain


IoT platform solution
Constant exchange of data with different sensors to ensure constant cooling
Production site
Storage (e.g., country hubs)
Local point of care (e.g., hospitals)
Vaccination centers (e.g., surgeries, pop-up clinics, nursing homes)
Need to ensure cold chain is not interrupted to guarantee vaccine effectiveness

Source: Arthur D. Little

Arthur D. Little has been at the forefront of innovation since 1886. We are an acknowledged thought leader in linking strategy, innovation and transformation in technology-intensive and converging industries. We navigate our clients through changing business ecosystems to uncover new growth opportunities. We enable our clients to build innovation capabilities and transform their organizations.

Our consultants have strong practical industry experience combined with excellent knowledge of key trends and dynamics. ADL is present in the most important business centers around the world. We are proud to serve most of the Fortune 1000 companies, in addition to other leading firms and public sector organizations.

For further information, please visit www.adlittle.com.

Copyright © Arthur D. Little – 2022. All rights reserved.