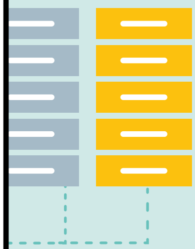
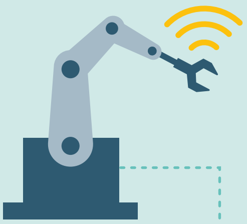
Can IoT win the war on security?



While the Consumer Internet of Things industry calls for stronger security, the Industrial Internet of Things is meeting the challenge.



– AUTHOR: Chris Coffey –

Too many Internet of Things (IoT) devices lack intrinsic security. In a connected world, all it takes is one vulnerable device to bring down an entire network of machines.

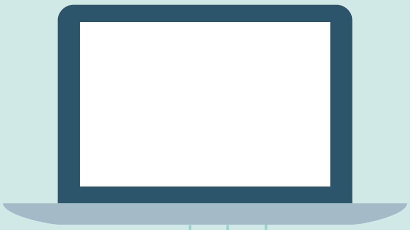
As you can imagine, this weakness in the IoT heightens fear within supply chain systems, especially in the manufacturing world. Asset-intensive organisations facing the threat of cargo loss, theft, damage and piracy can't afford to complicate operations by opening the door to sophisticated cybercrime.

However, there's no reason to believe information and operational blindness are costs of doing business in 2018. IoT adoption is growing in both the public and private sectors, impacting all areas of business where asset-rich enterprises operate. According to the International Data Corporation, "The IoT use-cases that are expected to attract the largest investments in 2017 include manufacturing operations ($105 billion), freight monitoring ($50 billion), and production asset management ($45 billion)."[1]

Maersk Line, the world's largest container shipping company, uses real-time IoT data to optimise route planning and asset utilisation, track intermodal freight, predict equipment failure, and minimise performance variations. By leveraging the power of the IoT, Maersk reports that the company has saved millions of dollars in operational costs.[2]

Lost production is easier to recover than your reputation. If you're ready to embark on the IoT journey, you'll discover that the IoT can provide you with an ability to cost-effectively balance real-time visibility, security and convenience.

First published in Assets, the magazine for Members of the IAM. August 2018



Act I: Ready?

Recent online articles describe the IoT as a security crisis. Is there no effective way to secure vehicles, assets and cargo?

There is a better way. Risk exposure haunts the entire IoT industry, but much of what gets published on IoT security breaches relates to the Consumer IoT (CIoT), not the Industrial IoT (IIoT). That's not always clear to the reader, and this is where the waters get muddy. To better understand the content covering IoT security vulnerabilities, you need to be familiar with the devices and attacks being written about.

Take IoT botnets, for example. The notorious IoT botnets making headlines are attacks on consumer-grade devices. These attacks target, infect, and hijack consumer devices, such as smart cameras and routers, which are shipped and sold with default usernames and passwords.[3] These login credentials are published and searchable online. If the customer doesn't change the default username and password, cybercriminals can recruit that IoT device for their botnet army of machines.

Act II: Aim...

Fortunately, unlike the CIoT, the IIoT hasn't been plagued by successful exploits.

But it hasn't been ironclad either. According to Verizon's 2017 Data Breach Investigations Report, the manufacturing and transportation industries faced their fair share of malware attacks, DDoS (Distributed Denial of Service), and cyber-espionage in 2016.[4]

This shouldn't deter asset-intensive organisations from digital transformation, though. Trusted IIoT managed service providers emphasise and offer rigorous security architecture for companies that lack the in-house experience or expertise needed to protect IIoT data.

Besides, the technology available to you is also available to your competitors. Companies that avoid or delay IIoT adoption risk losing talented employees, partners, market share, customer loyalty, revenue and competitive advantages. To compete in today's global economy, companies in the logistics space need better ways to improve service delivery, maintain equipment, and monitor assets moving through supply chains.

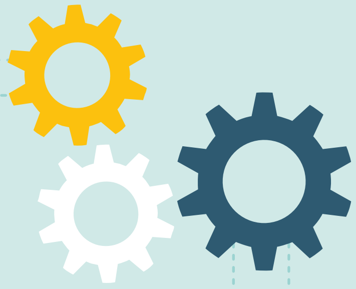
The IIoT can help you reach these new levels. To maximise value from the IIoT, your IoT technology partner must provide real-time data, analytics, advanced reporting, and intuitive applications. However, these functionalities must be secured across four different layers: Device, Network, Cloud, and Application.

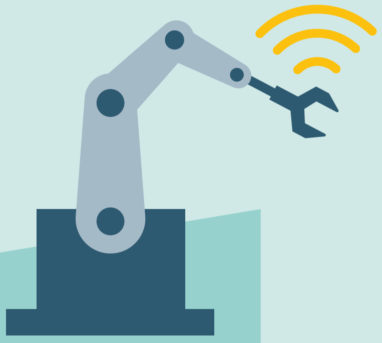
Device Layer: the hardware component of your IIoT solution. IIoT hardware includes devices that monitor asset location, vehicle movement and health, cargo temperature, and machine diagnostics. These devices should allow over-the-air firmware and configuration updates to maintain their software lifecycle. They must also be robust and ruggedised for durability. A growing number of devices are meeting military specifications for durability, Federal Information Processing Standard (FIPS) 140 requirements for tamper-resistance against physical attacks, and cryptographic algorithms to protect data stored on devices and in transport.

Network Layer: network connectivity, which enables data transport between your IIoT device and cloud, server, or hybrid storage. The most popular communication protocol for IIoT deployments is 3G/4G cellular connectivity. Other common communication protocols you might hear mentioned include Wi-Fi, satellite, Zigbee, and LoRaWan. The major wireless carriers provide end-to-end encryption security for every IIoT device that connects to their wireless networks. Connectivity for the other communication protocols can also be secured through data service centres like Amazon Web Services, or with other solutions such as a virtual private network (VPN).

Cloud Layer: a managed service of virtual servers that allow you to gather, store, aggregate, and analyse IIoT data. Cloud services should be scalable, secure and compartmentalised. Scalable architecture allows you to dynamically access data storage when needed. Also, for maximum security, the cloud layer of your IIoT solution should give you the ability to compartmentalise and control who has access to your data and what they can see.

Application Layer: software applications that contextualise and visualise IIoT data on desktop and mobile devices. Bringing IIoT data over the internet and into the hands of users requires multiple layers of security. First, your application must provide strong credential management to prevent the exploitation of weak usernames and passwords. Second, security protocols must tightly govern user roles and permissions. Applications should control each user's ability to view, create, edit and delete data, as well as provide a hierarchy that sets permissions from object- to field-level.





Act III: Fire!

The IIoT has ushered in a new era in secure data management. With the IIoT, asset-intensive companies are positioned to use actionable data for reducing costs and increasing profitability.

The City of Burleson's industry-leading asset monitoring units connect to their vehicles' OBD-II (onboard diagnostics) ports, capturing a stream of real-time data that includes date, time, location, speed, hard braking, aggressive acceleration, odometer, engine hours, and ignition on/off status.

"We've also built a scorecard system based on different metrics that scores the value of each asset, each year," said Aaron Russell, Director of Public Works, City of Burleson. "Now, we generate a list for asset replacement versus saying 'we'll just keep a vehicle or asset for seven years'. We save quite a bit of money off [this scorecard system]."[5]

Similarly, motor carriers and construction companies are empowering fleet and maintenance managers with IIoT devices to improve logistics operations. GPS trackers can simultaneously monitor movement and engine diagnostics. The data gathered from these devices can help reduce heavy equipment theft, miles driven, wasteful idling, poor driving behaviours, late deliveries, and costly vehicle breakdowns.[6]

In Flagstaff, Arizona, the Northern Arizona Intergovernmental Public Transit Authority (NAIPTA) relies on an IoT-enabled transit asset management solution to help transport millions of riders per year.[7] Because of the IIoT, NAIPTA is now capturing about 85 per cent of the work the facilities team is performing at each stop. This is data that can now be used to make smarter decisions to be a more efficient organisation. Also, when the city planning department wants to develop new bus stops along a new route, this data can be used to plan for costs and resources with more accuracy.

The IIoT industry is aware and ahead of the game regarding security concerns. The risk has been minimised, and the biggest risk is not doing anything and falling behind.

References

1. IDC: Worldwide spending on the Internet of Things forecast to reach nearly $1.4 trillion in 2021, according to new IDC spending guide idc.com/getdoc.jsp?containerId=prUS42799917
2. Maersk: Smart containers listen and talk maersk.com/stories/smart-containers-listen-and-talk
3. Krebs on Security: Who is Anna-Senpai, the Mirai Worm author? krebsonsecurity.com/2017/01/who-is-anna-senpai-the-mirai-worm-author/
4. Verizon: Verizon's 2017 data breach investigations report verizonenterprise.com/verizon-insights-lab/dbir/
5. ThingTech: ThingTech connects City of Burleson, Texas to the Internet of Things thingtech.com/blog/2018/01/18/2018-1-4-thingtech-connects-city-of-burleson-texas-to-the-internet-of-things/
6. ThingTech: Aubrey Silvey Enterprises prevents heavy equipment theft with real-time asset tracking thingtech.com/blog/2017/12/06/2017-12-6-aubrey-silvey-enterprises-prevents-heavy-equipment-theft-with-real-time-asset-tracking/
7. ThingTech: NAIPTA relies on ThingTech to transport millions of riders per year thingtech.com/blog/2018/02/01/2018-1-30-naipta-relies-on-thingtech-to-transport-millions-of-riders-per-year-case-study/

About the author

Chris Coffey is an award-winning IoT marketer, and chief storyteller at ThingTech. Chris oversees demand generation strategies that integrate content development, events, email campaigns, newsletters, social media, custom webpage design and digital advertising. If you want to improve your ability to securely pinpoint, prevent, and predict operational errors, contact Chris at ThingTech: thingtech.com/contact-us/