NEW YORK:
THE IOT SECURITY & BLOCKCHAIN HOTBED

BROUGHT TO YOU BY

IoT Security Summit

Blockchain 360

Contents

Page 3:
New York as a hotbed for IoT security

Page 5:
Scaling blockchain to solve the IoT cybersecurity crisis

Page 7:
4 ways blockchain could help enhance IoT security

Page 8:
Upcoming IoT regulations and laws: How to survive and stay compliant

---

Your 15% discount to attend IoT Security Summit & Blockchain360

We value our online community, and we'd love for you to join us at IoT Security Summit or Blockchain360 in New York this October. As a "thank you" for downloading our content, we're delighted to offer you a **15% discount** on your conference pass!

Claiming your discount is easy. When you're ready, click on the button below, select a ticket, then add it to your basket—VIP code **IOTSEC15** (IoT Security Summit) or **BLOCK15** (Blockchain360) will be automatically applied before you check out.

IOT SECURITY SUMMIT: BOOK NOW

BLOCKCHAIN360: BOOK NOW

The State of IoT Security & Blockchain in 2017

A recent Ponemon Institute survey revealed that 75% of security professionals expect an IoT-enabled data breach or DDoS attack to occur within their organization in the next two years, while 94% said such an incident would be catastrophic.

The need for stringent cybersecurity has now been widely acknowledged, yet many executives and security professionals still feel helpless. There has never been a more important time for the industry to gather and strategize their next steps for security.

And there's no better place to do so than New York. Read on to discover how a pool of strong cybersecurity talent and significant financial backing has transformed New York City into a focal point for Internet of Things security and development.

Our report also brings you commentary on scaling blockchain to suit IoT security demands, the benefits of blockchain as a cybersecurity tool, and implementing and surviving upcoming IoT security regulations.

This report is brought to you by IoT Security Summit and Blockchain360, two industry events collocated in New York this October. We're bringing NYC a two-day cybersecurity and digital ledger showcase like no other, featuring:

Thomas Braun,
Chief Information Security Officer,
United Nations

David Hahn,
Chief Information Security Officer,
Hearst

Vijay Vedanabhatla,
Principal Security Architect,
UPS

Martin Lehofer,
Blockchain Head of Research Group Systems Integration,
Siemens

Anil John,
Program Manager, Identity Management & Privacy Research, Cyber Security Division,
Department of Homeland Security

Thien La,
Chief Information Security Officer,
Wellmark Blue Cross Blue Shield

See more IoT Security Summit speakers

See more Blockchain360 speakers

NEW YORK STEPS UP AS A HOTBED FOR IOT SECURITY

The Internet of Things (IoT) as an industry has exploded, but with technological advancement comes the need for improved security for both businesses and consumers.

Since the days of Stuxnet, cybersecurity has become a key component in the successful implementation of technology-related product strategies, whether it be for traditional PCs, mobile devices, IoT security systems or consumer products.

According to Cisco, 50 billion interconnected IoT devices are expected to be in use by 2020. However, it is only in recent years that technology vendors have attempted to create protocols and standards for smart device security.

While solutions are being researched and developed, such as the use of blockchain technology—more commonly associated with virtual currency—to combat the exploit and compromise of IoT devices, this emerging field needs a talent pool to tap into, as well as cities in which experts can collaborate on new, security-focused IoT research.

New York, with an estimated population of just under 20 million and roughly 30% of the population educated to degree level or higher, has emerged as a pinnacle area for IoT security in recent years.

According to the Compass Global Startup Ecosystem Report, New York was the second hottest city for startups to begin their journeys in 2015, coming just behind Silicon Valley.

An analysis released in the same year by New York State Comptroller Thomas DiNapoli, suggested that job growth in high-tech industries was able to grow four times faster than the city's economy during the economic recovery period.

Angel investors are often hot on the trail of new, exciting technology startups, and the New York local government is just as keen. The NYC Mayor's Office of Tech + Innovation has invested hundreds of millions of dollars into IoT, smart city and broadband projects over the past few years alone.

"Technology is critical to New York's place as a 21st Century city," NY Mayor Bill de Blasio says. "Not just because tech brings lots of investment and jobs but because successful cities have always thrived on the disruption new technology brings."

However, according to Mike Joyce, Client Partner at Citrusbyte, it is a combination of factors which make New York an appealing area for security-related firms, in particular, to set up shop and flourish.

Not only does the city have the financial muscle of some of the largest banks and investors in the world close by, but there is a high density of tech talent due to the local government's emphasis on promoting STEM skills and programs, alongside countless technology and Fortune 500 companies which have picked the city as their home.

According to the Cybersecurity Ventures top 500 cybersecurity companies to watch report, 23 of the strongest players in the field, including IBM Security, Knoll, Bayshore Networks, Fireglass, Booz Allen and Varonis, call New York their home.

Booz Allen, for example, offers enterprise security solutions to protect

systems ranging from business to industrial control, IoT, and the military.

Varonis, also based in the area, has recently worked with the city of San Diego to implement a data security solution to protect thousands of mobile and smart, connected devices, alongside roughly 40,000 network endpoints.

Knoll offers "smart solutions for a connected world," ranging from compliance advice to security solutions, while Bayshore focuses on protecting the Industrial Internet, IoT and embedded systems.

IBM Security offers security solutions ranging from IoT to mobile security and operations response.

There is also evidence of mergers and acquisitions around the area which has the potential to strengthen the IoT security field.

Honeywell has been eyeing up the IoT security field of late and acquired NY-based IoT and industrial security firm Nextnine earlier this year, while Cisco's acquisition of NY-based Jasper in 2016 for $1.4 billion was aimed at solutions for managing and securing IoT devices through the cloud.

"[The acquisition] has the possibility to provide meaningful security solutions," Joyce says. "It's not going to be easy or quick, but Cisco has a great history of pulling these kinds of acquisitions off."

There is financial backing, serious interest from investors and technology firms alike, and governmental support for IoT security research and development—but challenges for pushing the industry forward lie ahead.

IoT cybersecurity solutions are not mature enough to be considered an ecosystem in themselves, and as an industry in its infancy, colleges and vendors need to train up the next generation of cybersecurity professionals to pick up the slack for IoT technologies.

Innovation centers do, however, have a part to play in ensuring New York continues as a hotbed of IoT security-related activity. These kinds of labs are commonplace in New York, and recently, the State University of New York at Albany received a federal grant to launch a new cybersecurity center.

The startup ideas, concepts and prototypes for IoT security solutions may all be there in the melting pot of New York talent, but there can be difficulties in bringing ideas to market and then implementing them successfully.

"Quite a few large companies run Innovation centers within the NYC area," Joyce says. "These innovation labs are tightly coupled with existing

enterprises—and the timeline of going from idea to production is greatly reduced compared to a typical startup."

Citrusbyte says there are some platforms being developed which are making implementation easier, including leveraging blockchain ledgers, clientless VPN systems, and the emergence of marketplaces which specialize in configuration purchases and SIM-based security.

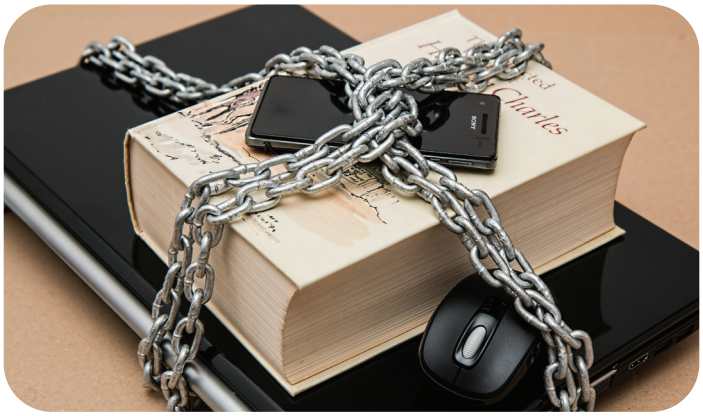
"I would say that the industry is generally lacking implementation experience," Joyce commented. "We have implemented quite a few meaningful production systems of which IoT is one small piece. Most customers that we've worked with are great at producing proofs of concept, but they really need help with the implementation details."

With government backing for technology, strong universities, startup network support and a range of security and enterprise companies in the area, it is no wonder New York has become a hotspot for the emerging IoT security field.

In cybersecurity, it is often the network which must be given the most attention. In the case of New York, it is also the network of enterprise players, inventors and investors which make the area such a promising base for the IoT security industry.

Charlie Osborne, IoT Institute

SCALING BLOCKCHAIN TO SOLVE THE IOT CYBERSECURITY CRISIS



Blockchain has the potential to become key to protecting Internet of Things (IoT) devices, and learning how to scale it properly is critical.

When the concept of connected devices first began to form, leaping from the mobility arena into the consumer and business markets with a sudden influx of "smart" products ranging from lighting to personal cloud systems and security cameras, the novelty caught many an eye.

However, vendors en masse did not take security seriously.

Hardly a week goes by now without us hearing of the latest successful exploit or attack against IoT and connected devices, whether it be hackable jeeps, air conditioning systems which cause business blackouts, or smart medical device tampering.

Shodan, the world's first search engine for Internet-connected devices, can be used to find and watch vulnerable and open security cameras and the Mirai botnet, which launched a record-breaking 620 Gbps botnet attack against the website of renowned security expert Brian Krebs last year, was able to do so by enslaving millions of vulnerable IoT devices.

Research agency Gartner predicts that 20.4 billion connected devices will be in use by 2020. If billions of these devices are left vulnerable, personal and corporate security will be placed at risk.

However, there may be a solution for the IoT industry in the form of technology originally designed for cryptocurrency.

Blockchain is a digital ledger which distributes information across nodes in a network. By design, the blockchain is decentralized and records both data and activity transparently.

While originally intended for cryptocurrency, vendors are exploring how this technology can be used in other fields, including cybersecurity.

The decentralized nature of the blockchain offers security benefits as there is no single centralized hub where data is stored; instead, the information being transmitted through the chain is linked to a number of nodes, all of which use cryptographic signatures to secure data.

In order to compromise a network, cyberattackers would need to take out the majority of nodes in a chain simultaneously, which is time-consuming and difficult.

Emily Ratliff, engineering manager of security at Canonical explains that decentralization is important as "attackers have to defeat the security of many nodes and not just the centralized system."

"In practice, this usually results in better security although there is debate over whether many nodes are weakly defended and susceptible to the same automated attack versus a centralized system with security at the highest level," Ratliff says.

Due to blockchain's architecture, malicious events also are recorded for all to see and cannot be wiped from a system after compromise. Therefore, suspicious activity is visible and more likely to be shut down.

With so much data baked in, enterprise players will be able to see with full clarity product cycles, security implementation, suspicious activity, compliance and more, which in turn promotes trust and accountability in a security solution.

Travis Biehn, technical strategist at Synopsys, noted that many enterprise players are already working with blockchain, such as the Linux Foundation's HyperLedger project and the Enterprise forks of Ethereum.

"Most of these platforms are being developed and used to provide for distributed immutable append-only ledgers," Biehn says. "What once had to be an opaque feed from a trusted source can now be a shared data structure between participating members."

However, the blockchain, if used in IoT security applications, would need to be scalable to make them viable for the enterprise. Such scalability is not limited to the number of nodes in a network, but rather the latency and throughput over time.

There are a number of approaches to scaling blockchain. The first is "sharding" the blockchain network, which breaks the network into smaller groups of nodes that work locally, as well as altogether.

A second approach is using solutions such as IOTA, which uses a technique called a "tangle" that scales performance levels in line with the number of nodes in a network.

"Using this technique means the IOTA network is not constrained by the current performance issues that other networks are encountering," Joe Pindar, director of product strategy at the Data Protection Office, Gemalto explained.

In addition, there is the notion of dynamic trust. According to Shaan Mulchandani, security director and blockchain Lead at Aricent, this requires a minimum number of nodes with "established credibility," tied to the longevity of a node, participants it accepts and the recorded history of any poor behavior or bad actions.

By limiting the numbers of new participants and hopefully keeping bad actors out of transactions, scalable solutions can still root themselves in the concept of Probably Byzantine Fault Tolerance (PBFT), but they will not require all nodes to validate all transactions, improving speed and scale.

For validation and security functions on a scalable blockchain system, so-called "oracles" can also be utilized.

Oracles can provide underlying code, still tied to the blockchain, which can improve security, compatibility and interoperability for IoT devices on the network.

"It is obvious that this brings about a larger network, which would be more secure by making 51% of attacks, or takedown of processing capability in geo-constrained or geo-centralized areas by cutting power supplies, more improbable," Mulchandani says.

Lastly, IoT security solutions utilizing the blockchain can be modeled on current designs which construe them as a system-of-systems or network-of-network in itself, such as in Smart City networks or tired Industrial IoT platforms.

"This is conducive to using plasma-like techniques, which essentially allow for blockchains within blockchains," Mulchandani says. "In this way, decentralized security can be accomplished within a single organization's IoT network/deployments, or in ecosystems like smart cities that consist of smaller networks."

Scalability problems affect public networks such as Bitcoin and Ethereum due to issues such as Bitcoin's block limit and Ethereum's gas limit.

When everyone can write and the network is used as an anchor, bloating may also occur. Public networks such as Bitcoin must also validate every transaction and accommodate the slowest nodes, but with IoT networks, these problems can be sidestepped.

"This is unacceptable when it comes to IoT networks, which often consist of low-power, low-storage devices," Mulchandani noted. "[IoT] networks will mostly be private (or pseudo-private), and highly process or governance-driven. This implies that networks can be reasonably immune to bloating, and that nodes are at least on-boarded in a secure fashion."

According to Ratliff, there is no "inherent limitations" to blockchain which prevents scaling, as long as analysts anticipate the required scale to effectively run security solutions and build out the solution accordingly.

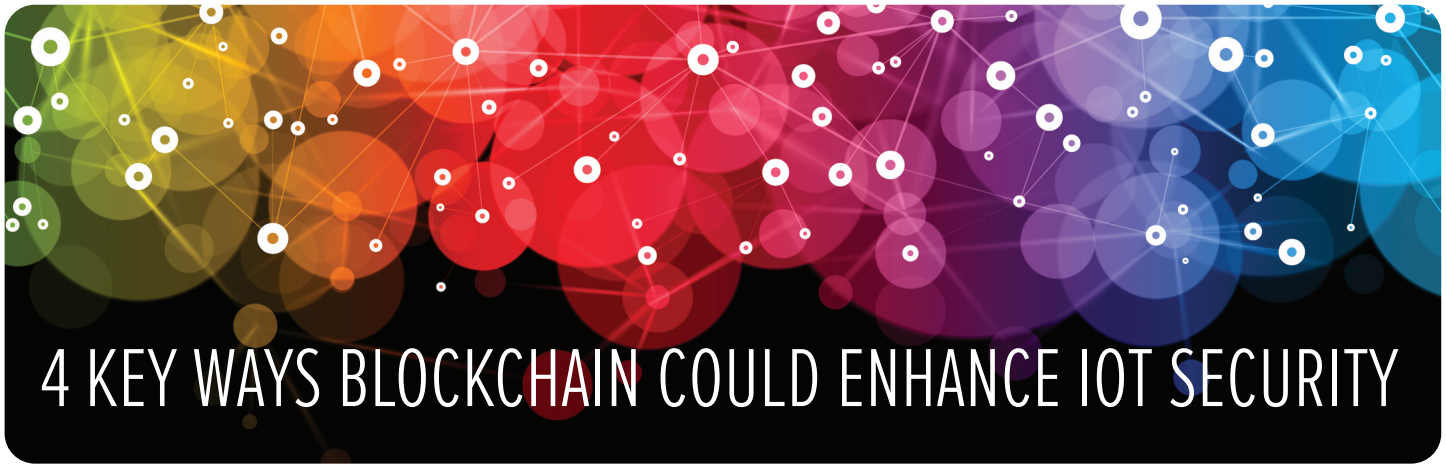
"The biggest challenges associated with deploying blockchain in a security solution is that the questions of motivation and energy consumption will need to be clearly answered up front otherwise the solution will fail," the executive warned.

Firms including IBM, Sensify, Cisco, Bosch, Gemalto and Aricent are all working on blockchain-related IoT security solutions. However, vendors must tread cautiously.

Blockchain has the potential to improve the security of IoT devices in both small and vast ecosystems, but there are potential pitfalls if implementation is rushed.

"Aside from supply chain promises, and possibly some applications in code updates, we see IoT platforms that might leverage blockchain technology actually make the problems worse," Biehn says. "A combination of IoT devices which can't really be trusted, implementing new technology like blockchain, for unfamiliar applications can only result in more damaging cyber-security headaches in the future."

Charlie Osborne, IoT Institute



4 KEY WAYS BLOCKCHAIN COULD ENHANCE IOT SECURITY

For organizations interested and investing in IoT, connecting devices are just the beginning.

It's not just reliable connectivity and storage they need. It's not just a standardized communication model to process billions (perhaps trillions of) microtransactions between devices. It's not just efficiencies and cost reductions to support sustained service business models (over product business models).

One of the single most important enablers of IoT adoption is trust: the ability for all stakeholders to trust that objects, infrastructure, people and data are as secure as possible.

Although blockchain is but one of many tools in the broader landscape of digital transformation, its potential to enhance security is notable. Below are four ways blockchain technologies or applications could help augment IoT security.

Decentralized structure

The most immediate potential security-related benefit blockchain offers IoT is its inherent decentralized architecture. A blockchain is a peer-to-peer communication model where transaction information is distributed and immutably recorded across all nodes on the network. Whether private or public blockchain architectures, there is no single centralized hub.

What this means is that the penetration or failure of any single node will not cause the broader network to collapse. If a malicious actor wishes to take down a network that runs on such a consensus model, they must penetrate at least 51% of the nodes on the network—often a far costlier and logistically unfeasible option than any potential reward would justify.

Authentication and access

Another security enhancement made possible by blockchain's very architecture is the difficulty and transparency that renders tampering with data riskier to exposure.

In traditional IT architectures, once a hacker penetrates a firewall, account, system, or other defense, "they're in". That is, once they've broken in, what tampering takes place often goes unnoticed and is rarely recorded. In a blockchain architecture, any transaction involving the data is recorded on the ledger across all nodes, for all to see. Transactions aren't just financial; any action created by the participant in the system is a transaction event. This means that any and all malicious activities, especially those with real impact, would be visible and potentially attributable.

Cryptographic standards

While not new or unique to blockchain, cryptography and digital signatures—which are an inherent part of blockchain architecture—offer an embedded layer of security compared to traditional database architectures. All transaction data must be cryptographically secured using encryption and digital signatures.

Furthermore, research and development supporting cryptographic standards, smart contracts and related technologies underlie the development of the entire blockchain market given their relevance to identity authentication and privacy protection.

Supply chain transparency

Blockchain impacts a number of use cases across the supply chain, some of which could potentially enhance security of IoT devices.

Given the technology's distributed, immutable and transactional nature, many organizations are looking at blockchain for tracking provenance, as a product travels through each phase of its lifecycle. From registering parts, sourcing, pricing, location, environmental data, interactions with each party, ownership, compliance, counterfeit and so on, what is opaque and fragmented today would effectively have visibility and accountability "baked in" with every interaction. From a security standpoint, this could be relevant in times of product recall, fraud or dangerous counterfeit, assessment of security patches or updates, even outreach to end users in the event something has been compromised.

While no single technology, blockchain or otherwise, will ever be the "silver bullet" for securing our physical and digital worlds, a distributed, immutable ledger technology may help address or enhance various vulnerable spots in the network.

It's reasonable to assert that if blockchain is implemented at scale, it could be a true breakthrough in security technology because the architecture allows users to trust the result that the network provides, even if some of the participants in the network are malicious actors.

The notion that in a world of constant and increasingly sophisticated cybercrime, we can have a reliable and resilient network infrastructure (even if some of the players are corrupt) is a revolution in trust enabled by technology.

Jess Groopman, Independent Industry Analyst & IoT Advisor

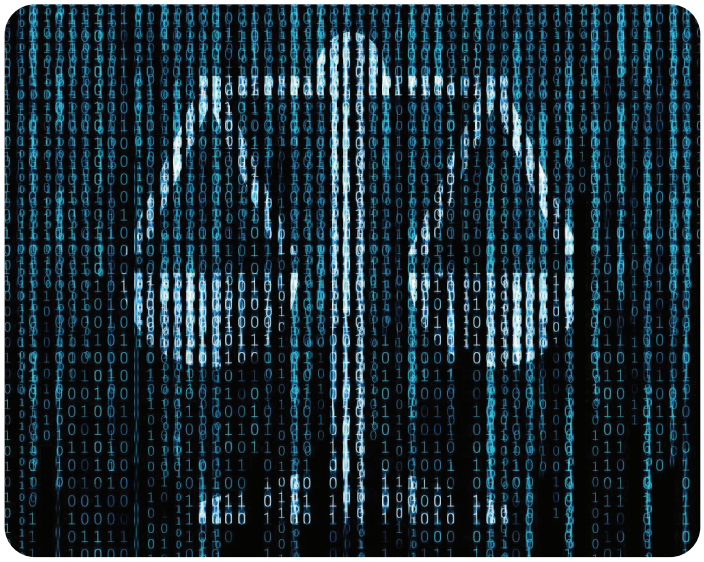
UPCOMING IOT REGULATIONS AND LAWS: HOW TO SURVIVE AND STAY COMPLIANT

Despite its origin as a marketing buzzword, there's no question that the uptake of network-connected devices that interface with the physical world as sensors and actuators, better known as the Internet of Things, has grown dramatically. As the uptake of IoT has increased, the number of calls for meaningful IoT regulations and laws has grown in parallel.

IoT devices have also enveloped the segment known as industrial control systems that has been a mainstay of manufacturing, power generation and delivery, water systems, and a wide variety of other industrial applications for decades. While the industries those devices supported may have been subject to a wide array of safety, environmental and sometimes cybersecurity regulations, the devices themselves were regulated indirectly, if at all. If the purchasers of those devices were in regulated industries, such as electric power delivery, healthcare or financial services, they were obligated to ensure that the devices they purchased, when combined with their own people, processes and technology, provided adequate security.

As the Internet of Things market has exploded beyond the traditional industrial control and medical device market, there has been increased interest in directly regulating the devices themselves now that technically unsavvy consumers are in the mix.

For example, U.S. Sens. Edward J. Markey (D-Mass.) and Richard Blumenthal (D-Conn.) have proposed the Security and Privacy in Your Car (SPY Car) Act to address security and privacy protection in automobiles. While this and similar legislation have yet to gain much traction, it is likely that the media attention over recent cyberattacks involving IoT devices will eventually force legislative or regulatory action at the state or federal level, particularly if the cyberattack leads to death or serious injury. Consequently, it is important that the industry strives to both influence and respond to the likely changes in the legal landscape.



There are some potential pitfalls that Internet of Things regulations can bring while noting that the life safety issues for many IoT devices mean that IoT regulations of some sort will likely be needed. However, the goal should be to regulate lightly where possible, and recognize that a heavy-handed approach can stifle innovation and limit options for the many small companies that simply don't have the resources to respond to endless data calls or onerous documentation requirements.

Instead, I propose 10 common-sense steps regulators can take to protect consumers while maintaining a light touch:

1.Regulators should prioritize investigations based on the likely number of victims and the severity of the impact that could result from a breach.

2. Investigations should be structured to leverage automation wherever possible by using industry standard questions for cybersecurity controls and minimize the need for lawyers and auditors to be engaged to answer the questions.

3. Regulators should regularly report on the efforts they have made to reduce the cost for companies to respond to regulatory inquiries, including providing estimates on the expected costs to respond.

4. Expedited review by federal courts should be available for investigative targets to challenge overly onerous costs of responding to an inquiry.

5. Regulators should provide testing scripts and sample investigative questions on their web site that can be incorporated into cybersecurity scanning and governance, risk and compliance (GRC) products to encourage more automation.

6. Regulators should offer clear and concise safe harbor options that impose a higher burden on regulators to demonstrate that cybersecurity practices were unreasonable if the options are leveraged (e.g., regular use of static/dynamic analysis for code review, two-factor authentication, application whitelisting, removal of admin rights from user workstations).

7. For sector specific regulators, guidance based on the use cases for IoT and the expected controls for those use cases should be provided to ensure that an appropriate cost-benefit analysis, which includes externalities, can be performed.

8. Regulators should provide examples of breach investigations, without naming the target, where companies were found to have behaved reasonably and no enforcement action was taken.

9.Regulators should incorporate the supply chain into their investigations so that accountability can be appropriately assigned.

10.Regulators should be required to harmonize their cybersecurity guidance and determinations of reasonableness across all sector and non-sector specific agencies regulating similar practices.

But even in the unlikely event that all these recommendations are adopted, IoT manufacturers, integrators and end-users may need to alter their practices and tighten cybersecurity and privacy controls for their products. Below are some examples of steps these groups can take to minimize scrutiny from regulators and avoid legal judgment should a cybersecurity attack occur.

Know what data you are collecting and why

For many IoT devices, their primary job is to collect data about the physical world using a variety of sensor technology. Much of this data is fairly innocuous information derived from the weather, traffic, speed, air pressure and other phenomena. However, once this data is connected to a person, the privacy advocates and associated regulatory agencies get involved.

Ultimately, data points like heart rate and electricity usage are aren't as useful for treatment or billing purposes unless connected to a person, but that doesn't mean that the identity of the relevant person needs to be stored on the device. Using concepts like tokenization, the device can simply report its sensor data and its serial number to a centralized data source that can be better secured. Moreover, for many device manufacturers, the fact that the device doesn't even have the requisite fields for storing that personal data means that the responsibility for any privacy violations would reside elsewhere.

Know where your device will be used and how it can be abused

Product liability law has long held manufacturers responsible for harms arising from both legitimate uses of a product as well as the product's foreseeable misuses. For example, a chair is meant for sitting, but a common misuse is as a makeshift stepladder. Manufacturers are expected to build that into their safety considerations.

Similarly, setup instructions for an IoT device may remind owners to change the default password on their devices but not force that change, even though it is well known that most consumers don't change those default passwords. As Bruce Schneier notes, much of the damage arising from the recent Mirai botnet attack could have been avoided if either the manufacturer or the consumer had taken efforts to secure their devices, which in many cases meant either changing the default password or requiring such a change before activating the network interface.

Know the potential impacts of cybersecurity attacks individually and in aggregate

One of the blessings and curses of IoT is that a device becomes more useful when it is networked with many others. For example, a single sensor

embedded in the road doesn't offer much help for people wanting traffic status, but when thousands are linked together, drivers, traffic engineers and government officials can derive a wealth of knowledge.

However, the networking of thousands of homogeneous devices means that a cyberattack infiltrating one can quickly spread to others, creating harms not envisioned individually, such as the denial-of-service attacks caused by the Mirai botnet. And it's a sure bet that regulators are going to target the biggest networks first, particularly where the damage is likely to be significant.

Build in mechanisms to automate the documentation of cybersecurity controls

Increasingly, the biggest challenges manufacturers and end-customers have with cybersecurity compliance is not in implementing the appropriate controls but in proving to auditors and regulators that those controls exist. By automating that documentation in conjunction with appropriate cybersecurity standards and IoT regulations, organizations can save a lot of money and potentially generate more sales to customers with their own compliance obligations.

Watch the supply chain

In our global economy of just-in-time manufacturing, parts can come from a different part of the world depending upon the day of the week. If we're not careful, our end-products can wind up filled with counterfeit or manipulated components. Moreover, most software is comprised of a significant amount of third-party code coming from open-source repositories (for example, the Linux operating system or an Apache web server) or commercial libraries.

The good news is that there are lots of eyeballs to notice those vulnerabilities and hopefully get them patched quickly. The bad news is that once incorporated into an IoT's software stack, many manufacturers don't keep track of vulnerability alerts and patches tied to those third-party libraries. It also makes those products an easy target for regulators as often a simple scan can find those vulnerabilities. While locating malicious code in a custom-built microprocessor isn't easy, confirming that you have the latest version of Debian Linux shouldn't be that difficult.

Taking the above actions is no guarantee that regulators will stay off your back, but it will hopefully make the regulatory process less onerous and may reduce the likelihood of a major breach of customer information or physical harm, which is what will get a regulator's attention.

Gib Sorebo, Chief Cybersecurity Strategist,
Leidos & IoT Security Summit speaker

IoT Security Summit

October 23-24, 2017
InterContinental Times Square, New York City

Co-located with:

Blockchain 360

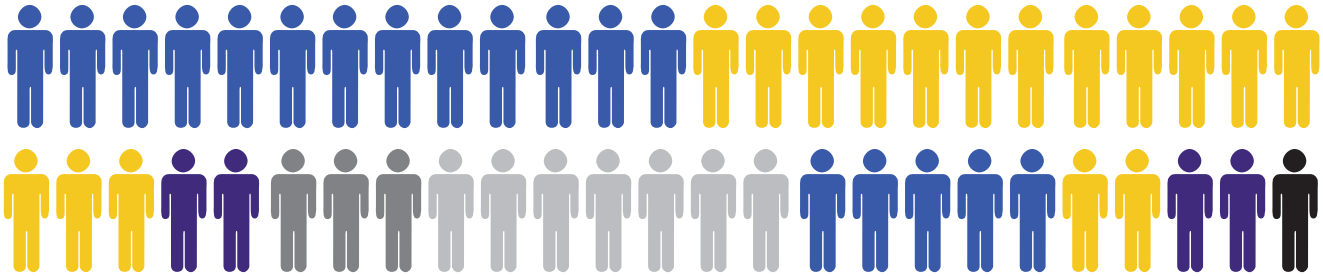
Cloud Security Summit

500+ Attendees Across All 3 Events

80+ Speakers

30+ Exhibitors, Sponsors & Startups

MEET SECURITY EXPERTS AND DECISION MAKERS



- CXO/VP **26%**
- Director/ Manager **29%**
- Business Strategy **5%**
- Business Development/Account Manager **6%**
- Engineer/Developer/ Architect **15%**
- Research/Analyst **11%**
- Media **3.5%**
- Consultant/Expert **4%**
- Other **0.5%**

COVERING KEY TOPICS
SURROUNDING THE VITAL ISSUE OF SECURITY:

- Workforce Preparation for Security Challenges
- Value of Penetration Testing
- Vendor Collaboration to Secure IoT
- Standards & Interoperability
- Protection Against Large Scale IoT Exploitation
- Securing Consumer and Industrial IoT
- Data & Devices Security Use Cases
- DDoS attacks and Ransomware
- Securing IoT Network Infrastructure
- Privacy and Big Data
- AI to Improve IoT Security
- Blockchain for Security

BOOK NOW & SAVE 15%
(WITH CODE IOTSEC15)

Blockchain 360

October 23-24, 2017,
Intercontinental, New York City

Co-located with:

IoT Security Summit

Cloud Security Summit

500+ Attendees across all 3 events

80+ Speakers

30+ sponsors, exhibitors & startups

ATTRACTING A QUALITY TECHNICAL AUDIENCE

- Software Engineers & Architects
- Enterprise CTOs and CIOs
- Law Firms and Privacy Professionals
- Tech Giants
- System Integrators
- Blockchain Platform Providers
- Startups
- Investors

KEY TOPICS INCLUDE:

- Getting Started With Blockchain
- Value Creation with Blockchain
- Blockchain Startup and IoT Partnership
- Blockchain for IoT Identity Asset Management
- Use Cases in Supply Chain, Energy & More
- Challenges in Scaling Blockchain for IoT
- Data Analytics for Blockchain Computing Network
- Ethereum vs. Hyperledger for IoT
- Scalable and Secure Enterprise Application
- Applications & Use Cases in Deployment
- Shaping the Future of Blockchain

BOOK NOW & SAVE 15%
(WITH CODE BLOCK15)