Security Call to Action
Preparing for The Internet of Things

High performance. Delivered.
Executive Summary

The Internet of Things (IoT) makes many innovative business models and applications possible, but with cybersecurity breaches increasingly in the headlines, it could also expose industries and consumers to new security and privacy issues.

The IoT, which consists of every type of Internet-connected device, including those used in health, vehicles, finance, defense and industry, is becoming an attractive target for cyber-attackers. According to the US Department of Homeland Security, the energy sector has faced the most intensive bombardment from attackers due to the severe impact a successful breach would have on people's daily lives. But all areas of the Internet of Things—including the Industrial Internet—are under attack, including IoT networks in telecommunications, transportation, pipelines, and refineries, as well as those in power generation, transmission and distribution.

Consequently, awareness of cybersecurity threats and incidents is also increasing. For example, respondents to recent World Economic Forum research say that vulnerability to cyber-attacks is their most important IoT-related concern, followed closely by privacy breaches of personal data. Given this growing awareness, the dominant question on the minds of business and government leaders is the same: what do we need to do to secure the IoT? The most challenging aspects of this question involve the IoT’s sheer expanse and the diversity of industries and use cases that it embraces, which means that no “silver bullet” for securing it exists. The security and privacy requirements in industry, transportation, health and commercial implementations each have very specific and differing security needs. What's more, these needs often conflict—a problem amplified by growing pressure to reduce costs and settle on single solutions.

The unstoppable momentum of the IoT revolution also poses a significant challenge to businesses, which will have to find ways to protect their networks on the run. Because the Internet itself remains at risk, leaders cannot assume that the IoT will be secure any time soon. Instead, they will have to adapt their thinking concerning security to reflect current realities. We believe companies and governments need to create resilient and agile security solutions. Embedded into products and processes, these solutions will monitor threats and operational states, triggering appropriate responses to detect cyber-attacks before they can cause damage.
The Internet of Things (IoT) is already a reality

According to Gartner, the number of connected devices (excluding PCs, smartphones and tablets) will reach 26 billion units by 2020. Suppliers of IoT products and services will generate incremental revenues exceeding $300 billion.\(^3\)

While the IoT may seem brand new, a number of industries already have high levels of experience in the field (Figure 1).

Retailers have employed connected devices for years to introduce new products and services in their efforts to enhance capabilities and boost customer reach. Consumers are using connected health and fitness devices to monitor and exchange exercise statistics and vital signs. Homes are also becoming more intelligent with the emergence of expanding varieties of smart appliances.

Likewise, industrial players already have significant experience using the IoT to support their supply chains and equipment. Unlike its other manifestations, the industrial IoT includes industrial control processes such as supervisory control and data acquisition (SCADA) systems that control everything from robotic painting and welding systems that assemble cars, to machinery that generates electricity, refines oil and distributes natural gas. In these cases, control systems extract data from a mesh network of sensors and devices to make decisions without human intervention. Inevitably, many future
industrial processes will become even more reliant on the precision that software controls can provide, and companies will increasingly seek the cost savings made possible by the automation of previously labor-intensive processes.4,5

As a result, the Industrial Internet of things is changing how industries operate, as seen in Figure 2.

Figure 2: Extended reach of the Internet of Things
Intelligent connected devices are now a fact of life. In commerce, manufacturing, health, retail and transportation they control much of the world’s critical infrastructure. However, the security requirements and priorities of each area require detailed understanding. For example, an organization that has a combination of IT and operational technology (OT) may discover that its security requirements and governance mechanisms conflict. The implementation of effective IoT security requires a detailed understanding of the assets to be protected and the security mechanisms employed. For example, the operational and security requirements in the production of oil and gas differ significantly from those in connected retail or in the connected vehicle. Without sufficient attention to the security needs of the IoT, things can quickly go catastrophically wrong, as the following scenarios suggest.

Scenario #1: Industrial Control Systems
Many industrial control systems (ICS) in use today employ highly intricate and precise mechanisms that automate complex industrial processes. Operating and controlling physical machinery via software gives cyber-attackers rich targets to exploit. By altering control settings or sensor values, they could disrupt production or severely damage equipment. In the worst case, an attack could result in the physical destruction of machinery or even loss of life. For instance, the Stuxnet worm used such techniques to destroy more than 1,000 uranium enrichment centrifuges at Natanz in Iran between 2007 and 2010. Stuxnet has gained notoriety as the first true cyber weapon, and unfortunately, it provides hackers with a rich reference guide for developing increasingly sophisticated ICS attack mechanisms.

While the high impact of a successful attack on an ICS attracts hackers, attackers can also exploit other interesting vulnerabilities. For example, the huge scale of large ICS—particularly those involved in critical infrastructure production—makes them extremely expensive to put in place, which is why they often have design lives of up to 20 or more years. Unlike in the enterprise, it is probable that many components in an existing (i.e. brown field) ICS deployment will be old and potentially unable to support current best-practice security mechanisms. Additionally, the need for high availability in order to avoid halting production—particularly with systems running critical infrastructure—can have a negative impact on the expected incident response time. If security staff discover a serious loophole in a plant’s security system, it’s often impossible to update the production systems with an approved patch (if one is available at all) without hurting production. Technicians often have to schedule maintenance windows for upgrading systems many months in advance to avoid outages, so the resulting potentially sluggish response times, coupled with the possible high impact of a successful cyber-attack, make ICS very attractive targets.

Scenario #2: Connected Vehicles
The connected vehicle has arrived. Research firm IHS Automotive estimates that globally, 23 million cars currently connect to the Internet in some capacity. By 2020 that figure is expected to rise to 152 million. The automotive industry has long embraced computerized systems in the form of electronic control units (ECUs) to monitor and control engine performance and exhaust emissions via sensors and actuators. The ECU has also improved vehicle safety through software controlled systems for traction control, anti-lock brakes, electronic stability control, seatbelt pre-tensioners and, of course, airbag deployment.

Inevitably, the mobile communications revolution has extended into the vehicle, with driver entertainment systems now integrating seamlessly with cellular devices. Today’s Internet-connected cars download music, movies, maps, congestion alerts and tourist information, as well as provide email and web browsing capabilities.

With an abundance of connectivity options and integrated control systems currently part of the modern vehicle, manufacturers are becoming aware of the need to secure these systems—particularly with the introduction of over-the-air upgrades to the devices that control the actual operation of the vehicle. For example, electric vehicle maker Tesla has revealed that it can diagnose vehicle faults and send software upgrades to those vehicles when safe to do so (e.g., when parked). To do this it employs mechanisms very similar to those used to
upgrade mobile phone software over the air. This approach has already enabled it to avoid an expensive recall. When engineers discovered that a fault with the vehicle charger mechanism could cause a vehicle fire, Tesla simply upgraded nearly 30,000 vehicles over the air to remedy the error.10

The benefits of such a system to the manufacturer and owner have to be tempered with the potential for misuse by an attacker. If a cyber-attacker gains access to vehicle systems, it could potentially introduce malicious software or settings, and the consequences could be fatal (e.g., engine or anti-lock brake failure). Such incidents could also cause severe financial and brand damage to the car manufacturer.

Scenario #3: Unmanned Aerial Vehicles

An increasing array of organizations is planning to use unmanned aerial vehicles (UAVs) or drones to collect data on hard-to-reach or highly dangerous areas and to support law enforcement. The military has long used UAVs to perform reconnaissance and attack missions where the use of manned vehicles proves too dangerous, or where the small noise and radar footprint of the UAV allows covert action.

The increasingly sophisticated UAVs available on the commercial market have opened opportunities for drones to be used to survey farmland or to inspect industrial complexes. However, the ability to equip drones with high-resolution cameras and to fly them covertly has introduced new privacy concerns. The increasing payload capabilities of UAVs also enables new security threats—armed with explosives or guns, commercial UAVs could conceivably become tools for attacks.

Even assuming peaceful use cases, the drone system, if not carefully engineered for security, can itself be vulnerable to attack. A successful attack on a drone’s command and control system could pose a threat in the event of an intentional crash. An attacker could also compromise a drone’s navigation system and effectively steal it, or take control of it to generate negative publicity for the operator.

Scenario #4: Connected Retail

The IoT has energized new value generation opportunities within businesses. The emergence of cloud computing makes plays such as platform-as-a-service (PaaS) and software-as-a-service (SaaS) realities. Enterprises can now achieve bold new economies by paying only for the resources that they use, when they use them. The IoT has enabled the enterprise to connect with suppliers and customers intimately—and the emergence of sophisticated cloud big data analytics helps firms to understand more about their clients and consumers, which in turn allows them to predict trends and offer personalized services based on their behavior. Retailers have never understood more about their consumers than they do right now—but what does this mean for consumer privacy? Traditional IP, bank account or transaction details are no longer the only information companies need to safeguard from misuse. Entities can now analyze and potentially misuse information related to consumer spending behavior, location, and even biometric information.
Understanding threats to the IOT

Given the potential threats, IT and security executives need to focus on the security aspects of IoT and integrate them with processes and lifecycle schedules. Figure 3 depicts a high-level IoT architecture that connects what were once isolated technology components across domains.\(^{11,12}\) The threat vectors that hackers use will depend on their motives, skills and the levels of difficulty they encounter. The following offers a simplified view of how an attacker could target each component in the IoT.\(^{11}\)

### Applications

The cyber-attacker can exploit a number of weaknesses in the application domain, many of which are the result of poor security awareness by the users. For instance, simple, easy-to-guess or default passwords make it easy to gain access to devices and accounts. Likewise, sending unencrypted confidential information makes it easy for an attacker to collect information through “sniffing” or eavesdropping. Increasingly, hackers are using sophisticated social engineering attacks to trick unsuspecting employees or users into revealing confidential information.

### Network

Network domain attacks might focus on the core network infrastructure and the access network. Attacks could exploit vulnerabilities in protocols, impersonate devices or involve the insertion of rogue devices, leading to unauthorized network access. Attackers can also exploit the error information used by engineers to debug systems to identify what information technicians do and do not monitor, and to determine network topologies, device identities and information flows.

### Devices and Equipment

Attacks typically target connected devices and equipment such as supervisory control and data acquisition (SCADA) systems, sensors or household appliances. Many such devices depend on hard-coded access keys, making them vulnerable to brute-force attacks and spoofing.
As the scope of the IoT evolves, consumers and enterprises alike may have trouble keeping up with security threats. The following examples highlight some of the security challenges organizations may face.

**Operational security**

The IoT embraces the cyber world and the physical world at the same time. Security models that have been established within the enterprise do not typically fit well with the requirements of the physical world and of operational technology—and yet the undeniable economic benefits of connected devices and interconnected systems compel these two worlds to converge.

For example, the security and safety requirements in the OT domain for oil production are very different from those seen in connected retail. However, since an oil producer must sell its oil, it will require business-supporting IT mechanisms for retail and billing activities, as well as traditional business systems for email, documentation, HR, finances and so on.

Companies can assess the security tensions between the IT and OT domains by using the “CIA triad,” which focuses on information confidentiality, integrity and availability. Within the IT domain, organizations can protect the confidentiality and integrity of information at the expense of system availability—although there is the risk that with an increasing number of mobile OS and hardware platforms to support, insufficient testing prior to patch deployment can result in broken applications and disgruntled customers. Companies might also roll out maintenance activities for security upgrades at short notice, interrupting service availability to patch machines or systems.

Within the OT domain, production availability is paramount, and some may argue that with very little confidential information to protect, they can sacrifice confidentiality to protect the availability of production. However, we believe such an argument is too simplistic. In fact, it is not true that no confidential information exists in the OT domain. The manufacture of specialized lubricants, pharmaceutical products—or even soft drinks—all have manufacturer-specific blends and ingredients designed to provide a competitive edge. Sophisticated spyware attacks such as Dragonfly, a multi-stage attack that apparently targets pharmaceuticals companies, have increased in recent years to gain covert access to IP and other confidential information within the OT domain. Although the IT domain has different characteristics to OT, availability is also important there; video conferencing or streaming services are good examples of where companies must protect availability and latency. Unreliable service will quickly result in a loss of business no matter how secure the confidential information streamed is. In both the IT and OT domains, the integrity of information is essential. Just as with industrial control systems, where the guarantee of data integrity underpins information availability, the IT domain has many examples of use cases, such as trading platforms, which cannot provide a service unless the integrity of data is ensured.
The complex operational and security interactions and associated tensions between IT and OT domains mean that organizations need to adopt a new type of thinking. However, no silver bullet exists that can secure all use cases, and companies can no longer assume that traditional defenses will keep the bad guys out indefinitely. Stuxnet demonstrated that the use of zero day exploits, stolen certificates and a highly focused, multi-stage attack strategy can be devastatingly effective at penetrating defenses and avoiding detection for sustained periods.

So, how do enterprises detect a stealth attacker that is designed to be undetectable? Fortunately, the business world has entered an era where affordable computing power and algorithmic sophistication enables companies to employ analytics and pattern-finding software to detect malware at the very instant it is deployed. No matter how stealthy, malware alters the behavior of a system. By non-intrusively analyzing telemetry gathered from the IT and OT domains to detect and correlate tiny changes in system behavior, organizations can generate new security alerts and build awareness of anomalous behavior that could indicate the presence of malware, allowing them to take action before it achieves its goal. To attain this level of performance, companies need to embed security mechanisms in operational risk management and safety processes so that they include cybersecurity as one of their areas of concern. They should use existing telemetry data on the state of operations of a device in correlation with security events to obtain the right level of situational awareness.

**Governance**

What happens to disciplined risk, governance and compliance activities when previously hard-wired operational technology that controls critical functions and agile IT systems converge into a unified platform? The consequences of failures in such a converged system can be severe and far-reaching. We can expect the creation of new regulations and even new regulatory agencies, and this can lead to compliance requirements being levied and audited. This blurring of the cyber and physical worlds means that firms can only achieve effective end-to-end security by setting up a security governance model that accommodates both. To that end, enterprises must define roles, responsibilities and timelines for action, and establish clear communication mechanisms so that they can address IT and OT security issues in a coordinated and coherent manner. The differing requirements of the OT and IT domains have spawned different terminology and operating practices, so an effective, overarching governance model requires a combination of IT and OT experience to address and coordinate integrated security strategy and incident response mechanisms. The necessity for an overarching governance model to address IoT security also highlights the need for organizational changes. These can include the introduction of a chief risk officer empowered to coordinate IT and OT domains, or the development of a more federated model where the CISO has a seat at the table when it comes to making business decisions—ensuring that end-to-end security is a primary consideration.

**Data Assurance**

Companies should also consider data assurance as an essential part of security governance. Businesses must use data-level security approaches that enforce secure data policies through the entire product lifecycle—from creation to disposal—as potential solutions to data governance and integrity challenges. Fortunately, several data-centric security technologies aim to provide data-protection enforcement policies across multiple platforms. Voltage Security (acquired by HP), Informatica and Protegrity are examples of companies that have developed focused solutions with data-centric capabilities like data classification and discovery, data security policy management, the monitoring of user privileges and activity, auditing and reporting, and data protection. Low quality and low assurance data adds noise to the decision-making process, increasing the overall cost of extracting insights. As businesses establish infrastructure to collect and process data at speed and scale, they should implement data assurance and audit frameworks that scale to match the expansion. Businesses must also consider adding data quality tools designed for big data applications, since collecting, processing and maintaining IoT data is a big data exercise. Gartner’s Magic Quadrant for Data Quality Tools provides an insightful snapshot of the current vendor landscape and their tools’ capabilities to handle data as an asset.
Expectations of privacy

New privacy and confidentiality concerns will emerge in the collection of big data. The ability to read radio frequency identification (RFID) tags over distances or to use emerging technologies like Bluetooth low energy (BTLE) beacons (iBeacon) opens the opportunity to target locations or individuals. Also, hackers can control device drivers for monitors, cameras and microphones to “spy” on individuals, and to capture data such as passwords.

The emergence of wearable technology to measure personal well-being through biometric sensors is making people more aware of their exercise and dietary requirements. Most of the devices worn lack medical approval, which means the information collected is not covered by HIPPA and is potentially available for unregulated third parties to analyze and gain deeply personal insights into an individual’s physiology.

Software patching

With reports of new software vulnerabilities arriving every day, organizations need better ways to respond in the IoT. Unlike traditional IT equipment or consumer technologies, many IoT devices lack an interface for downloading and installing security updates. The situation is amplified in the consumer domain, where people can buy and install connected devices with scant awareness of the security or privacy issues that an attacker could exploit by an attack. Consequently, companies must start thinking now about how to engineer trust into their connected products. Clearly, consumer ignorance is no excuse—new security controls need to be implemented for connected device networks so that IoT use cases are beneficial and not potentially hazardous to the user.

As with industrial use cases, the centralized patching of IoT devices may be unacceptable because of the service interruption incurred. Imagine the consumer dissatisfaction if, for example, a connected vehicle or TV is unavailable for an extended period to allow essential, security upgrades to be installed! The increasing complexity of IoT use cases, communication protocols and new combinations of connected devices means that vendors also have to step up to the mark in ensuring that they follow rigorous, secure development practices. They also need to produce resilient code that can deal with unexpected or out-of-specification inputs in a safe manner. Doing so can reduce endpoint attacks and decrease the need for field software patches (with the understanding that companies can never entirely eliminate them).

No matter how rigorous development practices are, it would be naïve to assume that companies can eliminate the need to patch software. However, they could redirect the stealth techniques used by cyber-attackers to access systems unobtrusively and install software as an alternative delivery model. For example, streaming “bits & bits” at a slow rate over time rather than trying to send out large, potentially disruptive patches at once could be a way forward.

Communication protocol diversity

The diverse protocols in the IoT make security much more challenging than web security related to HTTP. No single set of security protocols applies to all. Organizations must recognize that security is only effective when implemented as an end-to-end mechanism that integrates different protocols and device types in an IoT solution. Security architects must step up to the challenge of finding corresponding and effective security mechanisms for each IoT communication protocol, and for ensuring that they fit within the cost, performance and privacy constraints required by the governance model.

Digital identities

Many IoT devices today depend on hardcoded access keys, making them vulnerable to brute force or spoofing attacks. The types of credentials will differ from one system to the next, as will the methods used to store and use them on the system. IoT systems must solve these authentication issues. Therefore, organizations need a model that gives people and devices unique identities and that can understand whether an information exchange should take place or not. It should uniquely identify all IoT devices (e.g., as recorded in a device inventory database), and only managed devices should have the ability to access or connect to other devices and applications in the corporate network.
Access management
The challenge in this area is to understand two questions: “What has access to what?” and “To do what?” In traditional user access management, names (and passwords) enable authentication to services and assets. The challenge with IoT is that there are no universal standards for sensors and devices similar to the directory services or application user databases used for people. Companies need to determine which approach is most appropriate for each implementation (e.g., capability-based controls).

Security managers also need to identify which approach is most appropriate for each implementation. Access management based on digital identities should adopt claims-based techniques to allow for more dynamic access controls. The system should grant certain levels of access or withhold them based on the state of the device, the identity and the location.

Time services
The ability to determine “who or what did what and when” represents a fundamental security enabler, one that makes time an essential component of security mechanisms. The challenge with many IoT devices (such as NFC-enabled smart cards) is that they do not incorporate the concept of time. Therefore, logging systems will need to incorporate alternative ways to identify and correlate events.

Design for failure/cyber incident
Organizations should design solutions to cope with certain levels of failure resulting from cyber incidents. This drives the need for more resilient software, especially self-healing software that can cope with a certain level of cyber-attack rather than require a new patch every time. The design philosophy should incorporate alternative security methods when one security control fails so that there’s always room for “failover.” In other words, no single security breach should result in complete system compromise; companies must implement defenses in depth, putting mechanisms in place to limit the scope and extent of an attack. When operating in the physical domain, nothing should operate at maximum capacity and back-up mechanisms that deal with a failure should always exist. Companies should never assume that their security mechanisms are impenetrable. Consequently, while effective physical and cyber-security mechanisms are essential, organizations must also engineer intrusion detection and fault tolerance into the solution—particularly when the lack of availability or a malfunction may lead to economic or safety issues.
Assessing security readiness

To gauge their security readiness, company leaders need answers to the following questions.

**Who** is responsible for managing your security risk as your business accelerates toward connected products, equipment and services?

**How** do your governance practices integrate security with the business (decision-making) processes?

**How** are you protecting data collected in the field? Do your protection efforts extend from data collection to intermediate storage locations to the industrial data center?

**Where** is your data stored? Using the cloud may mean that data is not automatically stored in the region in which it was collected. Some countries have regulations relating to data usage that could limit cross-border transfers.

**What** happens to risk, governance and compliance activities when previously hard-wired OT that controls critical functions and agile IT systems converge into a unified platform? The consequences of failures in such a converged system can be severe and far-reaching.

**What** is the security model for mass-produced, mass-consumed connected products?

**How** do you failsafe thousands or millions of industrial system sensors or microelectromechanical systems (MEMS)? Organizations need to integrate and thoroughly test safety mechanisms for critical applications to ensure their robustness.

**How** do you stay ahead of attackers who are becoming more creative as they take advantage of the physical and digital “blur”?

**How** does your security organization embrace agile, resilient and reflex-like solutions that can be embedded in products and where threats and operational states are monitored in a way that operational decisions can be made before a cyber-attack causes damage?
Initial steps a digital enterprise should take in a connected world

To embrace the emerging IoT securely, an enterprise needs to perceive its surroundings and automatically respond to changes. Methods that the digital enterprise can use to achieve increased IoT security include:

Engineer "trust" into your connected products
One effective way to create a secure and interconnected system is to apply "secure by design" principles to the components themselves, from ideation all the way to manufacturing. When originally configuring a system, designers should also build in operational controls to verify that all component behaviors conform to expected operational norms. Design activities should include a complete analysis of a system's threat-versus-risk status. The threats more likely to lead to undesirable outcomes should drive engineering processes, but companies also need to develop contingency plans that make systems resilient in the face of attack.

Adopt a new operational mind set
Companies usually cannot create perfect security. Consequently, they need to conduct continuous monitoring of the IoT's operational and security health. This is a big data challenge that requires a big data solution. What's more, an IoT system might include pieces of other such systems. Therefore, organizations need to design to survive failure and focus on resiliency. This process can start with establishing anomaly detection capabilities enabled by machine learning and effective responses.

Develop contextualized threat models
The IoT will enable new business models, and it will be imperative to identify links between business goals and security operations to improve the effectiveness of security programs. Organizations should build tailored threat models that take into account key business goals, the underlying technical infrastructure, and potential threats that can disrupt the business. Such a contextualized threat model can help in prioritizing potential IoT security threats, and uncover blind spots that traditional controls-focused approaches are not equipped to handle.

Apply mobile and cyber-physical system (CPS) security lessons
The IoT systems and applications relate to, but are not the same as, those in the mobile and CPS (i.e., embedded systems) arenas. Nonetheless, companies should consider the lessons learned and the growing pains endured by these precursors to the IoT.

Adopt privacy by design (PbD) principles
Firms can establish access and authorization rights to data sets as they collect them. Enterprises should co-locate these rights with relevant data sets when moved or stored.

Track and make use of emerging standards
Enterprises should understand emerging standards from collaborative organizations and even consider joining standard bodies and groups to exploit the rapidly evolving world of technology innovation.

Continue to educate system users
 Companies need to educate users about increasingly sophisticated phishing and social engineering attacks. Historically, a strong focus on physical security has been a priority for industrial control systems. The IoT will make this strategy less effective because there will be too many invisible devices to make it generally applicable. However, security experts should update their physical security controls to include tamper-proofing techniques where a physical interaction might trigger a device shutdown. Security professionals also need to recognize that relying solely on physical security measures will not be sufficient.
Conclusion

Organizations can often improve their defense of cyber-physical systems using carefully engineered network segmentation schemes. Since the IoT largely consists of a vast wireless sensor network, these kinds of protective strategies do not apply. Instead, companies can rely on the experience of sensor makers and users to detect bad actors and cordon off suspect ones. Additionally, enterprises can introduce logic to detect when "out of norm" information flows to any device. Companies should look out for situations in which device firmware receives unexpected updates without the proper handshake from an authorized device management point, or when the handshake comes from an unexpected source address.

The enterprise and user must take ultimate responsibility for end-to-end security across domains. The more a company can take a trusted systems approach, the greater assurance it has that it is properly accounting for security. Because perfect security is not possible, an enterprise must remain vigilant, and be prepared to react quickly when it suspects a system compromise. In the IoT, monitoring and understanding vulnerabilities and applying the capability model provide the blueprint to react.

In the broad context, Accenture recommends that stakeholders take the following actions in order to seize near-term opportunities and capitalize on the long-term structural shift of the Industrial Internet:

- Technology providers should share best security practices through a global security commons.

- Public policy makers must clarify and simplify their data protection and liability policies.

- All stakeholders need to collaborate on long-term, strategic R&D to solve fundamental technology challenges.
Contributors

Allan Haughton
Accenture Digital: Digital Mobility/IOT Security Lead

Michael Teichmann
Accenture Security: IoT/IoT Security Capability Lead

Pablo A. Vaquero

About Accenture

Accenture is a global management consulting, technology services and outsourcing company, with more than 336,000 people serving clients in more than 120 countries. Combining unparalleled experience, comprehensive capabilities across all industries and business functions, and extensive research on the world’s most successful companies, Accenture collaborates with clients to help them become high-performance businesses and governments. The company generated net revenues of US$30.0 billion for the fiscal year ended Aug. 31, 2014. Its home page is www.accenture.com.

References


2. World Economic Forum, in collaboration with Accenture, “Industrial Internet of Things: Unleashing the Potential of Connected Products and Services”


4. Gartner, The Internet of Things Is Moving to the Mainstream (10 January 2013 – G00247190)

5. Gartner, Uncover Value From the Internet of Things With the Four Fundamental Usage Scenarios (15 May 2013 – G00249065)

6. Critical Infrastructure (CI) is a term used to describe systems controlling the essential resources required to live our lives – electricity, water, gas, oil, transportation, health and communication systems. Disruption to CI systems will lead to wide scale disruption, and could potentially destabilize an economy, or influence a nation’s ability to defend itself.

7. Gartner defines Operational technology (OT) as “hardware and software that detects or causes a change of state, through the direct monitoring and/or control of physical devices, processes and events in the enterprise.”


14. Axway, Top Ten Security Considerations for the Internet of Things

15. Accenture, “Winning with the Industrial Internet of Things”