Deloitte Review
ISSUE 17 | 2015

Complimentary article reprint

Safeguarding the Internet of Things

Being secure, vigilant, and resilient in the connected age

BY IRFAN SAIF, SEAN PEASLEY, AND ARUN PERINKOLAM
> ILLUSTRATION BY ALEX NABAUM

Deloitte.

About Deloitte
Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. Please see www.deloitte.com/about for a more detailed description of DTTL and its member firms.

Deloitte provides audit, tax, consulting, and financial advisory services to public and private clients spanning multiple industries. With a globally connected network of member firms in more than 150 countries and territories, Deloitte brings world-class capabilities and high-quality service to clients, delivering the insights they need to address their most complex business challenges. Deloitte's more than 200,000 professionals are committed to becoming the standard of excellence.

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited, its member firms, or their related entities (collectively, the "Deloitte Network") is, by means of this communication, rendering professional advice or services. No entity in the Deloitte network shall be responsible for any loss whatsoever sustained by any person who relies on this communication.

© 2015. For information, contact Deloitte Touche Tohmatsu Limited.


01100101101010101110 0110010
10101010110001100010 1010101
01101010110010101001 0110101
10101010000111101010 1010101
11010100110011010100 1101010
01000100010001001001 0100010
10001000100101011001 1000100

Safeguarding the Internet of Things

Being secure, vigilant, and resilient in the connected age

BY IRFAN SAIF, SEAN PEASLEY, AND ARUN PERINKOLAM
> ILLUSTRATION BY ALEX NABAUM

A defining element of the Internet of Things (IoT) is that objects are not merely smart—equipped with sensors and processing power—but also connected: able to share the information they generate. What separates the IoT from the traditional Internet is the removal of people. The Internet is powered by humans inputting data: search terms, e-retail browsing, looking up a friend's social media page. Based upon the answers, they make decisions about how to act: whether to visit the site, buy the sweater, or "like" a friend's photo.

With the IoT, the role of humans diminishes, to the point that in many cases they are removed from the equation: Machines input, communicate, analyze, and act upon the information. Using sensor detection, machines can create information about individuals' behavior, analyze it, and take action—ideally in the form of streamlined, tailored products and services or, in the case of businesses, greater efficiencies. This newfound capability is why the IoT enables enterprises and individuals alike to create value in new ways, at a faster velocity than we've ever seen (see the sidebar "The Information Value Loop").

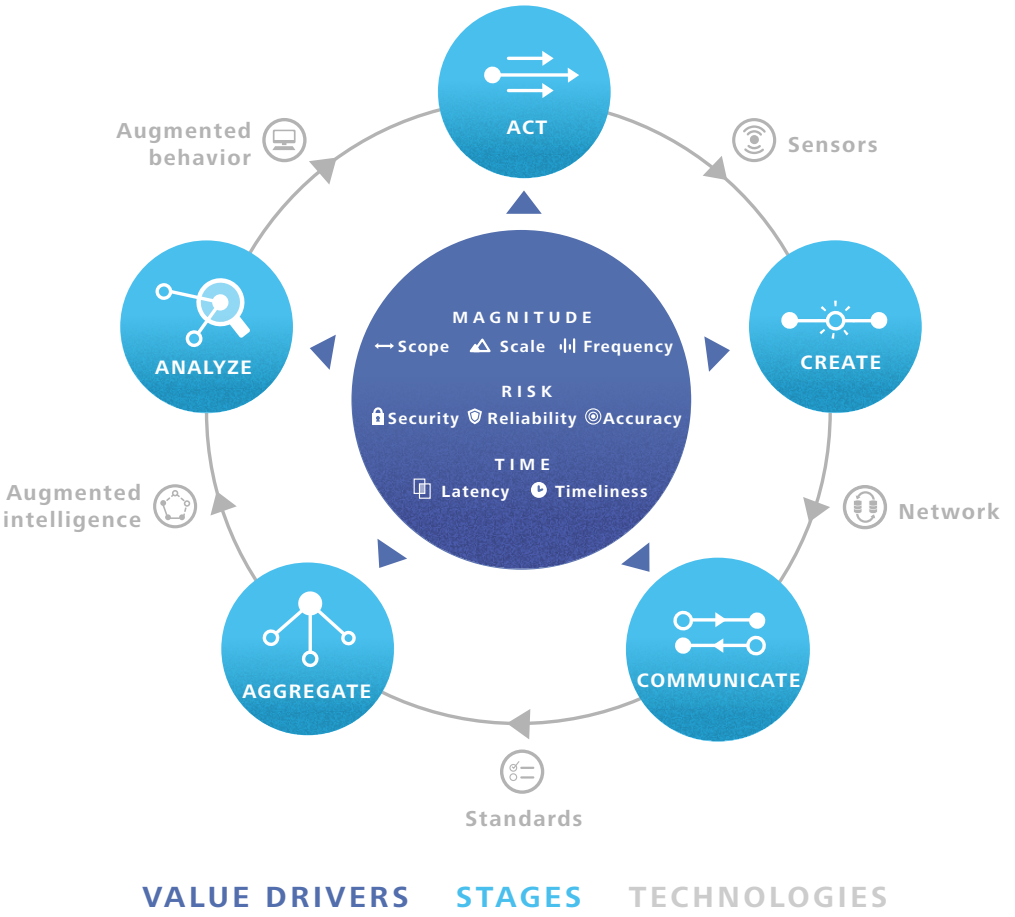
There is a dark side, however: As data are created and transmitted, this represents a new opportunity for that information to be compromised. More data, and more *sensitive* data, available across a broad network means the risks are higher and that data breaches could pose significant dangers to individuals and enterprises alike. Thanks to the IoT, data security risks will very likely go beyond embarrassing privacy leaks to, potentially, the hacking of important public systems. According to the World Economic Forum, "Hacking the location data on a car is merely an invasion of privacy, whereas hacking the control system of a car would be a threat to a life."[1] Consequently, in addition to new ways to create and capture value through

THE INFORMATION VALUE LOOP

The suite of technologies that enables the IoT promises to turn most any object into a source of information about that object. This creates both a new way to differentiate products and services and a new source of value that can be managed in its own right.

Creating value in the form of products and services gave rise to the notion of a "value chain": the series and sequence of activities by which an organization transforms inputs into outputs. Similarly, realizing the IoT's full potential motivates a framework that captures the series and sequence of activities by which organizations create value from information: The Information Value Loop (figure 1).

Figure 1. The Information Value Loop



Graphic: Deloitte University Press | DUPress.com

Note first that the value loop is a *loop*: An action—the state or behavior of things in the real world—gives rise to information, which is then manipulated in order to inform future action. For information to complete the loop and create value, it passes through the *stages* of the loop, each stage enabled by specific *technologies*. An *act* is monitored by a *sensor* that *creates* information. That information passes through a *network* so that it can be *communicated*, and *standards*—be they technical, legal, security, regulatory, or social—allow that information to be *aggregated* across time and space. *Augmented intelligence* is a generic term meant to capture all manner of analytical support, which collectively is used to *analyze* the information. The loop is completed via *augmented behavior* technologies that either enable automated autonomous action or shape human decisions in a manner that leads to improved action.

information, the rise of the IoT creates a new need to *protect* this information-based value.

We have found it highly effective to think about cyber risk management using the following paradigm:

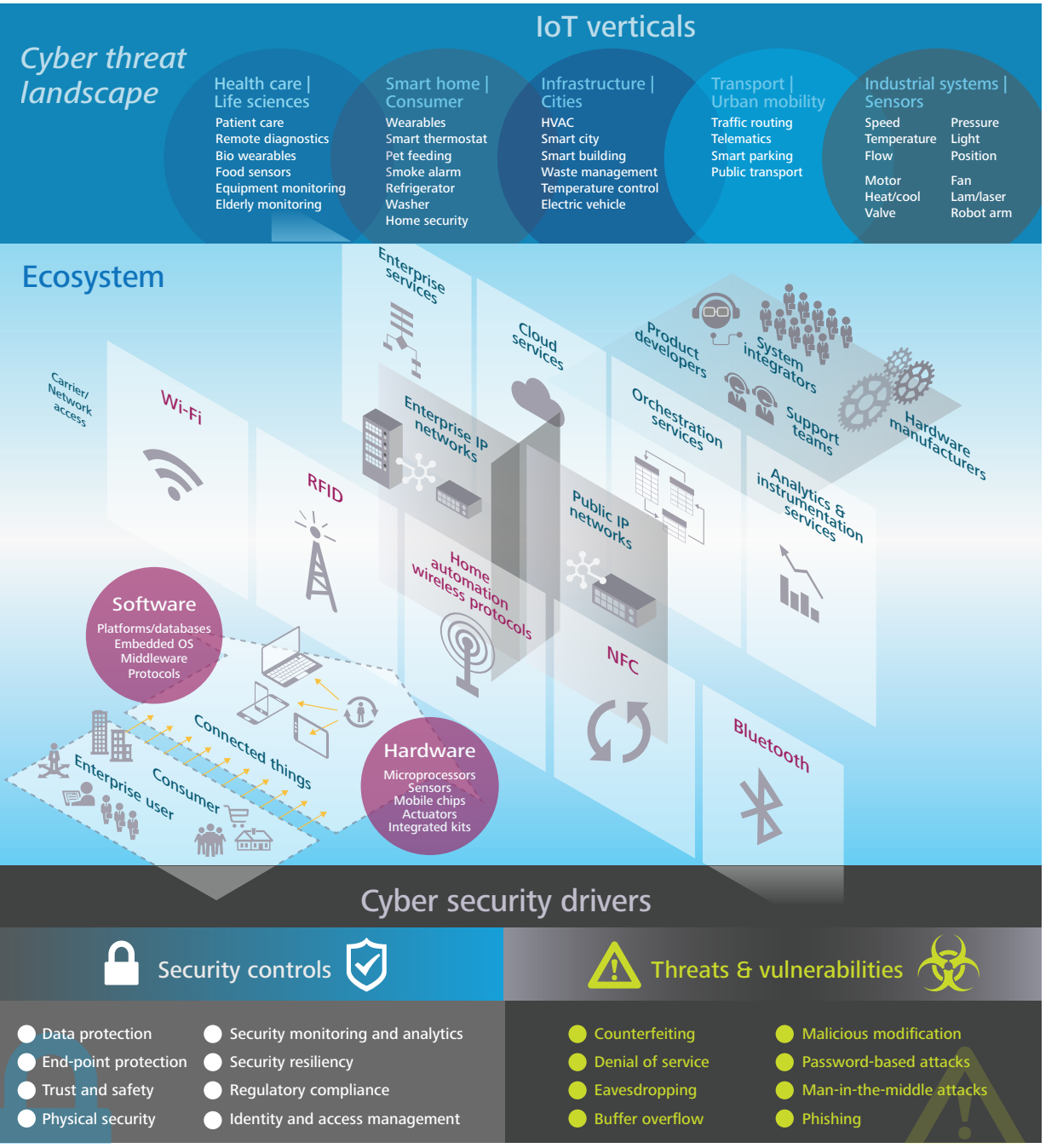
- **Secure:** In the spirit of "prevention" being worth more than a "cure," effective risk management begins by preventing system breaches or compromises. The forms that effective prevention takes include controls of many layers, types, and approaches, because the potential attacks are quite effective at exploiting weaknesses never imagined by their creators. We lock our doors because thieves might enter through them. Similarly, we physically "harden" sensors on power plants to protect them from accidental or deliberate assaults, and install software firewalls to keep out hackers.
- **Vigilant:** Making a system secure is not a once-and-for-all proposition. Both hardware and software degrade over time due simply to age. Worse, the nature and intensity of attacks can change in ways that render previously effective security measures obsolete. And, of course, no level of security is perfect: Best efforts still leave any system vulnerable. Consequently, security must be complemented by vigilance—monitoring to determine whether a system is still secure or has been compromised.
- **Resilient:** When a breach occurs, limiting the damage and reestablishing normal operations are much more easily and effectively done when there are processes in place to quickly neutralize threats, prevent further spread, and recover.

This framework has proved valuable in creating effective risk management systems for IoT deployments. In this article, we will illustrate how to apply it in a newly connected age.

SOURCES OF RISK

An exhaustive itemization and review of the risks arising from all possible IoT deployments is not practical, nor perhaps even possible. The complex and rapidly changing ecosystems and technologies at play demand instead a structured approach to identifying risks and appropriate responses (figure 2).

Figure 2. The IoT cyber threat landscape



The cyber risk landscape is inexhaustibly complex and ever changing. This figure provides a broad framework for identifying and managing a much wider range of risks arising from IoT implementations.

Source: Deloitte & Touche LLP

By focusing on some of the defining features of many IoT deployments, we can begin to see how the reinforcing principles of security, vigilance, and resilience can help companies protect the value they create.

SECURE

Securing data is, of course, critical at every stage of the value loop. In some cases, the security challenges and remedies are very similar to those with which many companies are already quite familiar. For example, a company implementing a supply chain solution within its own factory or warehouse has created a new value loop, but the data being generated and transmitted are conceptually no different than the email or sensitive documents transmitted over the office Wi-Fi network. Similarly, most companies are already grappling with the collection, storage, and retrieval of vast quantities of data. Addressing these challenges effectively is critical, but, as they relate to the IoT, the differences are of degree rather than kind.

There are, however, elements of IoT deployments that give rise to risks that are, for many companies, entirely new. Specifically, what makes the IoT so powerful is the ability to *create* and *communicate* data—the first two stages of the value loop. These stages are enabled through sensor technology and, typically, wireless communications networks, and each is vulnerable to security breaches.

For example, sensors are susceptible to counterfeiting (fake products embedded with malware or malicious code); data exfiltration (extracting sensitive data from a device via hacking); identity spoofing (an unauthorized source gaining access to a device using the correct credentials); and malicious modification of components (replacement of components with parts modified to generate incorrect results or allow unauthorized access). Any or all of these compromises would leave the sensors vulnerable. Communication networks can be hacked, allowing data to be intercepted or their flow disrupted through denial-of-service attacks. The following three sources of risk are especially relevant to IoT deployments and can be addressed through the application of specific security countermeasures.

Enabling interoperability

A common feature of many IoT deployments is the creation of an ecosystem that can include many different organizations or other stakeholders. Both upstream and downstream supply chain partners generate data, which extend even to the end-use customer. A large part of the value of IoT deployments stems from an ability to aggregate these data, yet the sensor technologies that various players in an ecosystem use can often be very different. Data are generated in different formats, and sensors connect to different networks via different communication protocols.

The lack of a single, generally accepted standard governing the functioning of IoT-enabled devices is therefore frequently a barrier to the interoperability required to realize the IoT deployments that many envision. The need for such standardization is evident in some device manufacturers' willingness to join one of the standard-setting bodies devoted to establishing interoperability standards and providing open source software that enables manufacturers to certify their products.[2] Unfortunately, even where standards have been adopted, different companies in the same supply chain may well adhere to different standards.

Consequently, companies can find themselves falling back on ad hoc solutions to create the interoperability that a given IoT solution needs. Unfortunately, it can be difficult to invest the time and money required to harden and test these solutions at the same level as formally developed standards, and so they are potentially more vulnerable to attack. Companies therefore face a sometimes-painful trade-off between creating interoperability and adequate security.

In the short run, the commonsense advice is simply to "test and invest" in order to create sufficiently secure case-by-case solutions. The IoT is unlikely to be a short-lived strategic priority, however, and it will therefore often be in a company's long-term interest to set an active and deliberate standards strategy. This can take the form of promoting the adoption of a single standard within a supply chain; it might mean getting involved in the standard-setting process itself, with an eye to helping shape cyber security standards and promoting their widespread adoption. The temptation to delegate standard setting to others can be strong, but, with so much at stake, it is a temptation worth resisting.

Retrofitting

Large, established organizations looking to implement IoT solutions that have already deployed sensors on a significant scale, such as industrial control systems (ICS), often consider adapting existing sensors to the IoT. This can be much more economical than developing new purpose-built technologies and then replacing existing components.

Unfortunately, many of the systems already in place—think of water or gas meters—use sensors with minimal security protocols because they were not designed to be connected to a more generally accessible network. Relying on such devices can only amplify the already-endemic risk associated with any value loop. For example, a manufacturing plant might use sensors to track its equipment's performance and health, with all of those sensors feeding data to a secure central system. With IoT functionality, information moves in all directions, and the back-end system now aggregates and analyzes all the data. But with so many more points of communication, the older security programs' simple, shared-system accounts and passwords

are no longer adequate: If a malicious actor were able to break into such a system account, he or she could steal sensitive instrumentation data from anywhere in the system or launch a denial-of-service attack, devastating plant operations.

Eventually, however, retrofitting may cease to be a viable option from a security standpoint. Given the rapid pace of innovation, many devices will likely become physically incapable of being upgraded to prevent against the latest threats, rendering them outdated and vulnerable to threats.

Every new device added to an IoT ecosystem adds a new attack surface or opportunity for malicious attack, and each hand-off is a new opportunity for a security breach. This risk can be exacerbated by the lack of sufficient interoperability, which warrants an emphasis on increased security.

Awareness and accurate assessment of the risks arising from retrofitting are crucial to effectively managing them. Whenever possible, companies should err on the side of replacing legacy devices with wholly new purpose-built hardware rather than retrofitting. Failing that, developing purpose-built add-ons that are outfitted with appropriate security measures may be the next best route.

Extending functionality

In light of the rapidly evolving technologies that enable many IoT deployments, there is an understandable desire to experiment and keep investment levels low. There is a real danger of overcommitting to technologies and even business models that subsequent innovation renders obsolete. When waiting is not an option but commitment entails material risk, it can make sense to extend the functionality of existing protocols and tools beyond their original design parameters. This allows companies to experiment and then commit as proven designs emerge.

Unfortunately, many of the technologies and protocols that developers are repurposing for the IoT can lack the high degree of native security controls that these new applications might warrant.[3] Everything from short messaging service (SMS) to the Internet itself is used in ways that go beyond its original intent, often with negative implications for security. The Heartbleed OpenSSL vulnerability, for example, allowed third parties to steal information normally protected by the SSL/TLS encryption, affecting many IoT devices.[4] Estimates suggest that fully eradicating Heartbleed from IoT products may take years, if not decades.[5] Similarly, identity

management—the authentication and authorization of devices for machine-to-machine communication—is often accomplished by relying on user names, passwords, and basic machine certificates. These continue to be points of compromise, and it is possible that new solutions for machine-level authentication need to be created to more effectively secure the vast array of IoT devices that are being predicted.

As with retrofitting, the practice of extending functionality enlists off-the-shelf communication protocols in ways not originally intended for secure machine-to-machine connections. Thus, to shore up vulnerabilities, companies would do well to take a similar approach to that of retrofitting: by hardening current solutions; designing new, bespoke, IoT-specific solutions; or adding a bespoke security element to protocols repurposed for the IoT.

VIGILANT

Developing a security strategy for safeguarding an IoT ecosystem isn't enough; as the technology evolves, so too will the threats it faces. Therefore, remaining *vigilant* to new or unexpected challenges is crucial to maintaining security. Two aspects of the IoT that are new to many companies create challenges that warrant an especially attentive, watchful response.

Data

As the technologies upon which the IoT relies improve, so too will the *scale* and *scope* of data collected, as well as the *frequency* with which they are collected. Smaller, cheaper, smarter, lower-power sensors and near-ubiquitous high-bandwidth wireless networks make it possible to know much more about many more things far more often. We can know not just where data are but also their velocity, direction, operational status, and a host of other characteristics.

When it comes to people, the scope of data collection is still more remarkable. The smartphone is already a widely deployed sensor that can reveal all manner of personal behaviors. To that we can add wearables of all sorts, gleaning still further insights into people based on what their things—home, car, and so on—do.

More information creates more possibilities to create value: This is the promise of the IoT. On the other hand, it also creates new liabilities. The quantity and variety of information companies find themselves collecting can make it difficult for companies to know if their data have been breached—a situation exacerbated by the fact that much of companies' data may be held by third parties, making them even more difficult to safeguard. When dealing with such tremendous volumes of data, it is only too easy for relatively small, virtually unnoticeable thefts to pile up until they amount to a veritable fortune. Worse, the loss of a small amount of data

can translate into a threat to an entire system and irreparable tarnishing of an organizational brand. Under such circumstances, the need for heightened vigilance is especially acute.

Companies can address this threat by developing a deep understanding of the data they possess and combining that with analytics to measure against a set "normal." By establishing a baseline of what "normal" looks like, they can more readily and reliably identify possible abnormalities, triggering further investigation.

Ecosystems

The volume and complexity of the data in an IoT deployment are often a reflection and consequence of the variety and complexity of the stakeholders in the ecosystem that enables that deployment. IoT applications—particularly those employed at the enterprise level—can rely on the closely coordinated actions of multiple players, from vendors along the supply chain to clients, transport agencies, the showroom, and end-use customers.

As discussed before, every new device added to an IoT ecosystem adds a new attack surface or opportunity for malicious attack, and each hand-off is a new opportunity for a security breach. This risk can be exacerbated by the lack of sufficient interoperability, which warrants an emphasis on increased security. In addition, a complex ecosystem can diffuse responsibility for monitoring the flow of data around the value loop. This can be especially acute as ecosystems grow and change over time, and originally established responsibilities become less relevant.

As manufacturers extend IoT-enabled processes and systems beyond their own organizations to encompass these additional parties, information flows across multiple external devices and databases, each under the control of third-party organizations. These third parties, however, may not recognize that their secure, vigilant, and resilient strategies—or lack thereof—have implications for the systems of every other stakeholder: The chain is only as strong as its weakest link.

The complex nature of IoT ecosystems may lead enterprises to assume that all the players involved can share responsibility for security. However, it could be a mistake to assume that partners—much less customers—should or will take responsibility for maintaining data confidentiality and guarding against breaches. In other words, enterprises should consider behaving as if the responsibility for security were theirs, and theirs alone.

The smart home provides a particularly resonant example of the risks involved when multiple brands, devices, and stakeholders *aggregate* and *analyze* multiple data sets and are knit together to form an ecosystem. Take, for example, the garage door opener. This device provides access to not just the garage but also the primary home. In some configurations, opening the garage door deactivates the home

alarm—a welcome convenience to someone coming through the door laden with groceries. This, however, means that the entire alarm system is deactivated if only the garage door opener is compromised.

Vigilance in this case means looking across all the relevant information that can be gathered and analyzing that against a baseline normal before declaring an "all clear." For example, if neither the owners nor their cars are near the home—determined by using GPS data on registered smartphones and automobiles—then the garage door opening would not only leave the alarm system active but trigger an alarm, along with security cameras and a text message to the registered phones or security services. This is relatively easily done when one security company provisions the entire system. For companies operating as part of an ecosystem, however, it might well make sense to provide for this sort of integration, and even be able to act as the hub for it.[6]

Companies can remain vigilant for threats in several ways. First, they can develop and maintain clear accounting within the IoT ecosystem, so that each player knows where its responsibilities begin and end, and what each is charged with protecting. Reviewing the responsibilities of all the stakeholders that touch the data in each of your value loops in some way, as well as the measures in place to fulfill those responsibilities, and assessing the potential risks to protect against them are central to effective vigilance.

RESILIENT

No amount of security and vigilance can guarantee that there will never be a breach or compromise. Far closer to certain is that some sort of failure will occur at some point. And in the face of almost certain failure, a system's resilience defines how quickly a realized risk can be addressed and normal operations restored. Consider the following two ways in which the need for resilience is relevant to IoT deployments—one driven by data management, the other by the design systems in the physical world.

Many companies *aggregate* information of wide scope from multiple devices with the assumption that more data must be better—more valuable, more useful. It is tempting to cast a wide net and operate under a "collect it if you can" bias, believing the data will be useful at some point.[7] Advances in IoT technology aid this impulse: Sensors' low cost and increasing flexibility provide companies with the ability to easily collect more data than they currently need.

Such practices bring to the fore an often-overlooked domino effect that arises from gathering ever-more diverse data: unauthorized inferences. For example, a customer might be willing to hand over location data and grocery shopping patterns

SECURE. VIGILANT. RESILIENT.™

Deloitte & Touche LLP's Cyber Risk Services practice offers a range of services to help our clients establish Secure. Vigilant. Resilient.™ cyber risk programs. Rather than being a necessary burden, the program is a positive aspect of managing business performance. Cyber Risk Program Alignment and Governance services help leaders invest in and manage the cyber risk program. SECURE services help organizations establish risk-focused controls around sensitive assets. VIGILANT services use analytic and correlation technologies to help develop monitoring solutions around critical business processes. RESILIENT services help organizations be prepared for when incidents do occur. Managed Security services help organizations manage controls pertaining to enterprise applications, identity and access management environments, and outsourced security operations. Read more about our Cyber Risk Services practice on www.deloitte.com.

in return for discounts or real-time coupons, but that same person may turn out to be strongly averse to those data being used to infer her health status. Without limitations on how data can be combined, each new data field dramatically increases the transparency of a person's life to whoever holds that information.

Establishing data governance can help mitigate some of the risks arising from aggregation. Setting limits on what can be collected in the first place can help sidestep many risks altogether, as companies can avoid collecting data they won't use and collect only those data that will generate enough value to justify the risk. Guidance concerning data ownership (which stakeholder within the ecosystem owns each piece of information) and the length of the data's life cycle must be established to ensure that data cannot be retained beyond a suitable timeframe or used for nonprescribed purposes. Such measures make it far more likely that as a company collects more and more data, any compromises will be far better contained than otherwise.

Moving from bits to atoms, the value loop is complete when actions are taken based on the data gathered and the insight generated. This often occurs independently of any human intervention. The appeal of many IoT deployments depends on precisely this characteristic, which typically calls for tightly coupled systems. When these work, they work very well, but they are vulnerable to more widespread havoc. In one particularly illustrative case, a German computer science professor, who built one of the very first smart homes, discovered what can happen when one element—in this case a smart lightbulb—goes rogue. Like a string of Christmas lights that goes dark because of one errant bulb, one afternoon his entire smart home failed to respond; only after monitoring his internal home network traffic did he discover that a defective lightbulb had been swamping the automation hub with

error messages. The lightbulb had, by itself, created a denial-of-service attack that rendered the entire house nonfunctional.[8]

This anecdote is a small-scale illustration of a data-chain domino effect: Any element of the system can disrupt the entire system. Avoiding this sort of self-propagating disaster requires fail-safe systems—that is, if there is a system failure, the consequences are not catastrophic and do not trigger knock-on system failures. Thus threats can be contained to a smaller area, averting a more catastrophic failure. In some IoT deployments, this takes the form of loosely coupled systems. In our home automation example, this could have taken the form of implementing stronger security-event-monitoring controls at the hub to effectively shut down the affected smart component in a fail-safe manner, with more effective incident or error handling at the smart-lightbulb component level. These resilient controls would have prevented one element compromising the entire connected home network.

APPLICATIONS

Effective risk management in any IoT deployment will draw on all three factors: secure, vigilant, and resilient. To illustrate the application of these principles, however, we focus below on applications in which each, in turn, is especially salient.

Securing the smart car

The importance of securing individual sensors is perhaps most important in today's connected car, which has evolved into a data center on wheels with any number of Internet-connected features. A typical automobile today contains about 70 computational systems running up to 100 million lines of programming code—twice as many lines of code as in the Windows Vista operating system.[9] Along with GPS devices that aid navigation and report on real-time traffic and road conditions, diagnostic devices assess maintenance needs and alert authorities in the event of an accident or breakdown. As infrastructure evolves, smart cars will have the ability to communicate with roadside devices such as traffic lights as well. Therefore, they must be designed keeping security in mind at the outset.

It's no surprise that some automakers might rush to develop and install IoT-enabled features to attract early-adopter customers and aid safety and convenience. In today's cars, IoT-enabled technologies include power and infotainment systems, remote locking and unlocking, and remote engine start, with data flowing between different vendors. Vehicle-to-vehicle communication spans ecosystems as well—for instance, connecting an automobile to the driver's home. Through in-vehicle platforms, smart cars can communicate with smart home hubs to open garage doors, unlock front doors, and turn on house lights as the in-car GPS registers that the

driver is nearing his or her home. The *scope* of data communicated between connected vehicles encompasses a wide swath of personal yet highly sensitive information such as driving habits, real-time location, entertainment preferences, and daily schedule.

Much of this communication is accomplished via existing tools that have been repurposed for IoT technologies, including mobile apps, cellular networks, and SMS technologies typically used for casual texting and not intended for secure communications. These extended IoT functionalities leave networks vulnerable to security breaches. Indeed, a recent survey of automakers found that nearly 100 percent of cars currently on the market include wireless technologies that may be inadequately secure, and most automobile manufacturers may not be able to easily determine whether their vehicles have been hacked.[10] Hackers, on the other hand, have demonstrated the ability to infiltrate various vehicular systems simply by using SMS texting.[11] Physical attacks via onboard diagnostic devices have shown it could be possible to manipulate some systems even while cars are moving.[12]

Further complicating the matter, those managing the development and deployment of these technologies traditionally tend to have less experience doing so, and that, coupled with the newness of the technology, may mean many take fewer precautions to secure data at the device level. Thus manufacturers have yet to develop common security standards, and measures to prevent remote access to an IoT-enabled automobile are haphazard at best. Data transmission between multiple vendors—the automaker, dealership, third-party data centers, GPS and onboard diagnostics systems, smart home devices, and others—creates multiple vulnerable points that should be remotely monitored.[13] Hardening the current systems to install more appropriate security measures will be crucial to safeguarding the connected automobile.

Vigilance in industrial control systems

The importance of vigilance is perhaps most apparent when it comes to large networked systems such as power grids, transportation systems, and manufacturing plants. IoT integration into these systems promises efficiency benefits. However, remote ICS—once isolated within a factory or out in the field, and now interconnected online—has less of a legacy of mature cyber risk practices, and its developers and owners may have insufficient institutional knowledge to adopt an appropriately vigilant approach to security.

Security for ICS is often governed by cost-benefit analyses that place short-term production needs ahead of safeguarding systems over the long term. Concerns about production loss during maintenance downtime may trump safety concerns, even as production loss in the event of a security breach would likely be much

higher. Further complicating the matter, ICS consists of mostly proprietary vendor-certified configurations and may contain components from multiple vendors, making a unified approach more difficult.

Asset age presents further risks. Older systems may have been retrofitted to make them IoT-enabled, a more cost-effective approach than replacing them entirely. However, they run into the same challenges described earlier—a lack of advanced security protections or inadequate safeguards. Enterprises may also be employing traditional information security practices or traditional shop floor measures that simply don't apply to an IoT-enabled device.

For ICS, one critical factor is the need to maintain 24/7 business operations. This illustrates the importance of having a vigilant security strategy, one that proactively looks for security gaps and anticipates malicious acts to prevent their causing unplanned downtime.

A traditional steel mill in Germany, for example, fell prey to a cyber attack in (probably) 2014 that disrupted internally networked control systems to the point that a blast furnace did not shut down properly, resulting in massive physical damage to the facility.[14] While this incident was limited to one mill, as systems grow ever more networked across facilities and span multiple players, the *scale* of data *communicated* and thus the risks for disruption on a wider scale grow larger, as well as the need for better monitoring. Indeed, establishing a baseline of "normal" data will help companies recognize when such anomalies arise, to stem the flow before they create a larger catastrophe.

Resilience in retail

Thus far, even the most personally inconvenient data breaches—for example, theft of credit card information—have left consumers remarkably unfazed.[15] But the IoT, by incorporating unique personal information gleaned from sensors, may alter that equation, and companies may find themselves in uncharted territory. Scenario planning, then, is key to preparing for reputation risk management and possible crises based on data breaches or worse. For instance, if a cyber criminal's work compromises a communication network partner's information flow, it is useful to have a sense of how to contain the problem, continue operations, and work with partners to restore the network.

Previews of the potential problems have already surfaced: In recent years, several major retailers, victims of high-profile thefts of customer information from infected point-of-sale devices, have been forced into crisis management mode, promising new, stringent security measures from the payment industry. Thus retailers must be resilient, prepared with a security response that enables them to bounce back from a massive data breach.

In addition to safeguarding their own internal data troves, retailers must contend with external supplier risks, including counterfeiting. Retailers will want to avoid being a party to selling faux products that leave customers vulnerable, however inadvertently. In particular, retailers will need to implement product verification to mitigate the risk of counterfeiting wearables, a market in which the buying channels are bigger and therefore prone to cheap imitations with potentially embedded malware.

For their part, consumer product manufacturers should consider their ability to be resilient in the face of a data breach. The range of connectable home devices—TVs, webcams, home thermostats, remote power outlets, sprinkler controllers, door locks, home alarms, smart home hubs, and garage door openers—creates multiple opportunities for hackers to gain entry into home ecosystems, entire customer bases, or even manufacturers' back-end systems each time data traverse the ecosystem.[16]

Specific risks from unprotected consumer devices may come in the form of eavesdropping, manipulated data in a man-in-the-middle attack, or data halted entirely due to a denial-of-service attack. An IoT-enabled door lock may allow entry into a homeowner's house by disabling the alarm and unlocking the front door; and a lock that's been tampered with, either by including parts corrupted somewhere along the supply chain or via malware, or is counterfeited could offer just about anyone access to a private home—a nightmare for customers and a potentially fatal scandal for an implicated manufacturer or retailer.

With the IoT and its attendant privacy and security concerns still at an early stage, any company's worst-case breach scenario is just that: a scenario, with no precedent. It's critical, then, for any firm looking to capture value from IoT technology to consider next steps if a data breach compromises a product or network—not only how to manage reputation risk but also how to continue operations. Establishing governance around which data can be collected, by whom, and how they can be used can help mitigate some of the effects of a breach. Additionally, establishing clear accounting so that each stakeholder understands its responsibilities and what it needs to protect can help further safeguard the system. Loosely coupling devices within the network will also help ensure that an attack on one node won't spread.

NEXT STEPS

For enterprises and individuals alike, smart, connected objects offer tremendous opportunities for value creation and capture. Those same objects, however, also create tremendous risk, demanding new strategies for value protection: A single vulnerable device can leave an entire ecosystem open to attack, creating

the potential for disruptions ranging from individual privacy breaches to massive breakdowns of public systems.

In the face of such challenges, companies can remain secure, vigilant, and resilient by taking several steps to safeguard their ecosystems and the data they create:

Work to define standards for interoperability. Adhering to one standard only or actively getting involved with consortiums to develop a set of standards can help ensure that devices within a network can all communicate and work together safely and effectively.

Use purpose-built devices or add-ons, rather than pre-IoT solutions. Rather than retrofitting or extending functionality of old systems in ways for which they weren't designed, companies should strongly consider wholly new, secure technologies designed specifically for the IoT. If this is impossible, any add-ons used to retrofit the device should, at the least, be purpose-built specifically for that use, outfitted with appropriate cyber security measures.

Develop clear responsibilities for the players in your ecosystem. Rather than sharing responsibility across a diffuse ecosystem, players must know where their responsibilities begin and end, and what they are responsible to protect. Taking an assessment of all stakeholders and assessing the potential risks at each point—and making sure the stakeholders are aware of those risks—can help make a solution more secure.

Establish a baseline of data. Viewing IoT systems more broadly and monitoring environmental attributes such as usage, location, and access would better enable enterprises to gather a broad enough scope of data to establish a baseline, helping companies to discern what is normal and what constitutes a suspicious aberration. This, in turn, enables enterprises to take appropriate and effective action when data do stray from the norm.

Institute data governance. Enterprises should consider playing a stronger governance role by defining which data to secure, what it means to be sufficiently secure, and, by extension, which products meet that goal. Guidance around how data can be securely collected, used, and stored can help prevent unwanted breaches and prevent a risk event from snowballing into something larger, and can also outline the lines of responsibility in the event of a breach.

Create loosely coupled systems. Ensure devices within an ecosystem are loosely coupled and resilient so that the failure of one device does not lead to widespread failure.

The prospects for creating and maintaining a seamless, secure network—with or without external partners—may seem daunting, considering that vulnerabilities exist on all sides, be they physical or virtual, inadvertent or malicious. Security cannot be an afterthought—it must be integral throughout the design process. IoT

solutions will need to blend a deep understanding of organizational operations with knowledge of multilayered cyber risk management techniques, creating offerings that are secure, vigilant, and resilient. **DR**

Irfan Saif *is a principal with the Cyber Risk Services practice at Deloitte & Touche LLP. He is also the US Advisory Technology leader and one of the leaders of Deloitte's CIO Program.*

Sean Peasley *is a principal with the Cyber Risk Services practice at Deloitte & Touche LLP and the US Consumer Business & Industrial Products leader for cyber risk services.*

Arun Perinkolam *is a senior manager with the Cyber Risk Services practice at Deloitte & Touche LLP. His focus is cyber risk strategy and program development.*

The authors wish to thank ***Brenna Sniderman****, a senior manager and subject matter specialist for Deloitte Services LP, for her invaluable assistance in the preparation of this article.*

Endnotes

1. World Economic Forum, *Global risks report 2015*, http://www.weforum.org/reports/global-risks-report-2015, accessed March 31, 2015.
2. Examples of such bodies include the AllSeen Alliance (https://allseenalliance.org/) and the Open Interconnect Consortium (http://openinterconnect.org/).
3. Robert Vamosi, "Security in DNS left out on purpose, says creator," *Forbes*, March 28, 2011, www.forbes.com/sites/firewall/2011/03/28/security-in-dns-left-out-on-purpose-says-creator/, accessed April 16, 2015.
4. Bill Oliver, "Heartbleed and the risk to IoT," *Tom's IT Pro*, April 16, 2014, www.tomsitpro.com/articles/heartbleed-internet-of-things-security,1-1876.html, accessed April 16, 2015.
5. Meghan Neal, "The Heartbleed bug will lurk in the Internet of Things for decades," *Motherboard*, April 11, 2014, http://motherboard.vice.com/read/the-heartbleed-bug-will-lurk-in-the-internet-of-things-for-decades, accessed April 16, 2015.
6. This additional functionality would likely incur additional expense, which could be reflected in different prices for different models. In the scenario described here, for example, a maker of garage door openers might have a simple, non-IoT-enabled device, one that is connected into the larger home security system, and one that is a hub integrating various data streams in the manner described. The same options would apply to the maker of the alarm system, the heating and lighting systems, and anything else connected to a smart home that responds to its owners' arrival.
7. Bruce Schneier, *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World* (New York: W. W. Norton & Co., 2015).
8. Kashmir Hill, "This guy's light bulb performed a DoS attack on his entire smart house," *Fusion*, March 3, 2015, http://fusion.net/story/55026/this-guys-light-bulb-ddosed-his-entire-smart-house/, accessed April 16, 2015.
9. Robert N. Charette, "This car runs on code," *IEEE Spectrum*, February 1, 2009, http://spectrum.ieee.org/transportation/systems/this-car-runs-on-code, accessed April 16, 2015; John P. Mello Jr., "Report: Connected vehicles vulnerable to hack attacks," *TechNewsWorld*, February 9, 2015, www.technewsworld.com/story/81692.html, accessed April 16, 2015.
10. Ed Markey, *Tracking & hacking: Security & privacy gaps put American drivers at risk*, February 2015, www.markey.senate.gov/imo/media/doc/2015-02-06_MarkeyReport-Tracking_Hacking_CarSecurity%202.pdf, accessed April 16, 2015.
11. Robert McMillan, "'War texting' lets hackers unlock car doors via SMS," *Network World*, July 27, 2011, www.networkworld.com/article/2179633/data-center/-war-texting--lets-hackers-unlock-car-doors-via-sms.html, accessed April 16, 2015.
12. D. J. Pangburn, "How easily can a moving car be hacked?" *Motherboard*, June 28, 2013, http://motherboard.vice.com/blog/how-easily-can-a-moving-car-be-hacked, accessed April 16, 2015.
13. Markey, *Tracking & hacking*.
14. Kim Zetter, "A cyberattack has caused confirmed physical damage for the second time ever," *Wired*, January 8, 2015, www.wired.com/2015/01/german-steel-mill-hack-destruction/, accessed April 16, 2015.
15. Jeffrey Roman, "Despite breach, Home Depot's profits grow," *BankInfoSecurity*, November 18, 2014, www.bankinfosecurity.com/home-depot-profits-hurt-by-breach-a-7575, accessed April 16, 2015.
16. Hewlett-Packard, *Internet of Things research study*, 2014, www8.hp.com/h20195/v2/GetDocument.aspx?docname=4AA5-4759ENW, accessed April 16, 2015; Arik Hesseldahl, "A hacker's-eye view of the Internet of Things," *Re/code*, April 7, 2015, http://recode.net/2015/04/07/a-hackers-eye-view-of-the-internet-of-things/, accessed April 16, 2015.