THE PRACTICAL ASPECT

Why Worry About IoT?

Do you have something to say about this article?

Visit the *Journal* pages of the ISACA® website *(www.isaca.org/journal)*, find the article and click on the Comments link to share your thoughts.

https://bit.ly/2DVZkcc

A recent post on a neighborhood blog read:

> *Our camera picked up a suspicious young male, approximately 17-24 years old, who approached the house, looked to the right of home, into the side door window, front door lock and into the camera before walking away quickly. Cannot be certain about his intentions, but wanted to make the neighborhood aware. My husband left message with the police department.*

So, the old door locks are not the same as today's smart locks with sensors, cameras an Internet connectivity. These locks not only prevent physical intrusion, but also do reconnaissance, record evidence along with a time stamp, and alert the owner and others charged with security responsibilities to act promptly.

The Internet of Things (IoT) refers to physical objects that have embedded network and computing elements and communicate with other objects over a network.[1] It is a network of items—each embedded with sensors—that are connected to the Internet.[2] These objects or devices possess at least two attributes: Each has a unique identifier and the ability to share data and interact remotely over a network without human intervention. These devices communicate over the network via wireless protocols such as Bluetooth; they are not dumb, but rather "smart." For example, the motion sensors embedded in the application (app) that supports the camera at the front door generated all images and alerted the device owner to the risk of an uninvited visitor.

The concept of IoT has become more real—more available—with the presence of the Internet combined with smart devices of recent origin. Over a relatively short period of time, smart devices have become smarter—that is, faster, with greater capacity to work with data, more processing capability and at a lower cost. And yet, what seemed like a wave of transformation enabled by IoT has lost some steam lately.

And yet, there is considerable optimism in what is anticipated in the world of IoT. According to a collaborative report on IoT in logistics, compared to 15 billion connected things in 2015, there will be 50 billion things connected to the Internet by 2020.[3] However, this represents only 3 percent of all connectable things, which continue to grow in number and sophistication over time. The proliferation of embedded sensor technology, wearables and apps has already caused incredible change in just a few short years. It can be concluded that "we are just beginning to connect everything unconnected."[4]

Vasant Raval, DBA, CISA, ACMA
Is a professor of accountancy at Creighton University (Omaha, Nebraska, USA). The coauthor of two books on information systems and security, his areas of teaching and research interest include information security and corporate governance. He can be reached at vraval@creighton.edu.

Ranjit D. Thaker, CISA, MCSM
Is the chief information officer for a leading time-critical, same-day air and ground transportation service provider. He has been in this role for more than 10 years. He has served in IT leadership positions in the specialty logistics industry for more than 25 years. He can be reached at ranjit.thaker@gmail.com.

Early evidence of the revival of IoT rests in the arrival of 5G. Citing MOBI, a *Wall Street Journal* article suggests that 5G could connect a trillion devices in the next decade.[5]

There are two distinct domains in which IoT has flourished. First, early adoption of the concept emerged in the industrial or manufacturing settings, where the supply chain was made more efficient or effective, perhaps even addressing issues of safety in the workplace. The following examples of such applications are drawn from the transportation logistics industry:

- **Tracking**—Most used for parcel or delivery service providers to track shipments and keep customers up to date on location of their shipment/estimated time of delivery
- **Environmental parameter tracking**—Used for sensitive cargo (e.g., specimens, organs, pharmaceuticals) to monitor temperature, humidity, speed, shock, etc.
- **Vehicle maintenance and driver behavior**—Used to optimize fuel efficiency, reduce breakdowns and monitor driver behavior (e.g., speeding, frequent breaking, lane violations)
- **Inventory management and operational optimization within warehouses**
- **Data analytics**—Analytics based on data collected from IoT devices and their use in improved decision support

Industrial IoT (IIoT) was a logical extension internally within the organization. The insights generated from the supply chain are harnessed into IoT apps developed and embedded into the supply chain support platform. Information security and privacy issues in IIoT are more easily controlled because the applications are within the boundaries of the organization, and devices and software are probably screened prior to acquisition. And their scope is tightly perimeterized, although anchored on the Internet.

A later development pushed IoT applications into the consumer arena, which can be called Consumer IoT (CIoT). Because it involves reaching out to customers who may have varying security environments and perhaps a variety of different devices among them, achieving reasonable goals on privacy and security fronts may be a challenge. The relative newness of integrating consumers into the IoT ecosystem adds a formidable dimension to the implementation of CIoT. It is challenging to understand the IoT footprint and control dimensions on each class of IoT devices. Also, IoT devices and technology integrate with several private and public network segments with a combination of privileged and open access; hence, a traditional third-party risk management (TPRM) approach to control devices and software needs an IoT technology-specific control domain to mitigate additional risk. The problem with these IoT devices is that they are made by consumer electronics companies. Unfortunately, consumer electronics products change often, adding to the risk scenarios. And even these organizations are themselves new to this level of computing and, therefore, vulnerable to making rookie errors in their firmware code.[6]

> “THE RELATIVE NEWNESS OF INTEGRATING CONSUMERS INTO THE IOT ECOSYSTEM ADDS A FORMIDABLE DIMENSION TO THE IMPLEMENTATION OF CIOT.”

Perhaps there are IoT applications that cut across IIoT and CIoT. However, from an information security viewpoint, it is easier to see the challenges if such applications are identified using this binary classification. The former is mature, better controlled, better known to the organization and limited to the internal network(s). The latter is new, introduces more devices from more vendors (likely from the consumer electronics industry), and connects the external customer to the internal world or internal employee to the outside world. Clearly, the IIoT ecosystem lands more comfort on the privacy and security front. CIoT is early in its development and, while popular and exciting to end users, needs more groundwork before an organization ventures into CIoT applications.

Essential Questions

Here are some essential questions that need to be addressed, among other things, to ensure that IoT is introduced to the organization with care and due diligence. Some of these questions apply equally to just about any IT introduction, but are certainly worth repeating because of the fundamental nature of the question of technology adoption:

- **Do you have a business case for the use of IoT?** Technology is an enabler of value creation; its use just for the sake of using it could be valueless. It is important to ask first, “Does the organization have the potential to create value through the adoption of IoT?” The answer to this question may change over time; therefore, it is important to revisit the question at appropriate intervals. Leaving the question buried in the past could hurt the organization’s competitiveness.
- **Do you have a policy on the deployment of IoT? Do you have other policies that support the IoT initiative?** Once it is determined that IoT adoption could potentially help create value, the development and use of a policy toward adoption of the technology should be considered. Without such a policy, a controlled and intentional introduction of IoT that meets the organization’s policy criteria is not possible. Just like the rules in configuring a firewall, the first rule is to not allow anything in, then progressively modifying the rule to embrace what is desired.
- **What appear to be the weakest links in defense-in-depth of the IoT ecosystem?** Network privileges and access vulnerabilities are the most significant. Where to draw the line in terms of allowing a network to access IoT applications is crucial to stemming any compromise of security. The security management should be quite discrete about what is essential to provide and what is a luxury, causing more risk than benefits to the organization. Another weak link in the CIoT environment is smart consumer electronics and the difficulty of tracking their ability to provide things acceptable under the organization’s policy. The extension of TPRM to the IoT ecosystem is easy to visualize but difficult to implement due to its diversity, vastness and constantly changing characteristics of the devices produced. It is doubtful if one can rely on the device makers to provide adequate security in the product features. Finally, the consumers who get connected to the IoT may not be aware of vulnerabilities that their use of the application would engender, and this could consciously or unconsciously enable a cyber compromise.
- **How do you limit the seemingly pervasive IoT networks?** First, a business case for each implementation must be made and, if this is done successfully, the minimum number of networks that should be allowed access to the IoT applications should be determined. Second, restricting scope and limiting risk is greatly affected by how well the perimeter of the network carrying the IoT traffic is controlled and how strong the access privileges to the network are. Sound security practices driven by a sound policy framework provide essential big steps toward secured IoT networks. Finally, user education is important, especially in the CIoT environments where users may be remote to the risk; their awareness and cautious behavior are soft, but important, components of IoT security.
- **How do you keep up with the continued development of the field (i.e., device, device makers, software, firmware)?** Should the organization trust smart devices its employees bring to work? As the Strava incident[7] has taught us, any device capable of running software could become problematic if that software is transmitting intelligence about the enterprise’s network. Employees could use their smartphones to run a seemingly innocent Internet speed test, for example, and end up sharing details about the internal network architecture that should be kept private.[8] While service level agreements (SLAs) could help gain some assurance that devices engaged in IIoT are secure, it would be difficult to implement a similar mechanism on the CIoT side, for the consumer electronics device makers are too diverse and do not necessarily focus on serving organizations in a one-to-one relationship as the third parties. Besides, continuity of electronic device makers or their products may be uncertain.

There are few technology fronts where, upon adoption, one can choose to rest without periodic evaluation. It is necessary for organizations to constantly monitor changes in the domain space to determine if any action needs to be taken at their end. What might have been launched as a potential value could quickly dissipate or could result in greater risk than anticipated. To continue to leverage the organization’s strategic and operational excellence, it is necessary to continuously be on the lookout for the edge of the innovation in IoT.

Enjoying this article?

- Read *Assessing IoT Audit/Assurance Program*. *www.isaca.org/Assessing-IoT*
- Learn more about, discuss and collaborate on emerging technologies in ISACA’s Online Forums. *https://engage.isaca.org/onlineforums*

> “IN AS MUCH AS TECHNOLOGY IS AN ENABLER, NOT TAKING ADVANTAGE OF IT IN A TIMELY MANNER COULD, IN FACT, DISABLE THE ENTERPRISE.”

In as much as technology is an enabler, not taking advantage of it in a timely manner could, in fact, disable the enterprise. Today, it is not a choice to allow a technology to pass by without the organization conducting a thorough review regarding its potential role in value creation for the organization. A technology may get hot at times and cold during other times; however, keeping an eye on its edge is an important first step toward continuing to leverage the technology. Not all technologies may fit a larger, or any, role in an enterprise at any given time. However, scanning the environment to reflect on where it is today and what it can do for the enterprise is an opportunity that should not be sacrificed. That is why business and IT leadership should worry about IoT.

Endnotes

[1] ISACA®, *Internet of Things: Risk and Value Considerations*, USA, 2015, *www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/internet-of-things-risk-and-value-considerations.aspx*

[2] IEEE, “Special Report: The Internet of Things,” USA, 2014, *www.theinstitute.ieee.org/static/special-report-the-internet-of-things*

[3] DHL and Cisco, *Internet of Things in Logistics*, USA, 2015, *https://discover.dhl.com/content/dam/dhl/downloads/interim/full/dhl-trend-report-internet-of-things.pdf*

[4] *Ibid.*, p. 26

[5] Woo, S.; “Why Being First in 5G Matters,” *The Wall Street Journal*, 12 September 2018, *https://www.wsj.com/articles/why-being-first-in-5g-matters-1536804360*

[6] Jones, D.; “Does Your Organization Need an IoT Policy?” Pluralsight, 30 January 2018, *https://medium.com/pluralsight/does-your-organization-need-an-iot-policy-f09e3e3f967f*

[7] Romano, A.; “How a Fitness App Revealed Military Secrets—And the New Reality of Data Collection,” *Vox*, 1 February 2018, *https://www.vox.com/technology/2018/2/1/16945120/strava-data-tracking-privacy-military-bases*

[8] *Op cit* Jones