help source

Q Various surveys point out that 20 to 50 billion devices will be connected using the Internet by 2020. What are threats associated with the use of the Internet of Things (IoT) and what approach should one have in implementing security for IoT?

A By now, information security considerations are well established. Initiatives to focus on cyber security due to new threats like distributed denial of service (DDoS), advanced persistent threats and targeted attacks are already being implemented by organizations. Implementation of IoT presents new security challenges, especially as this technology becomes more pervasive and integrated into our daily lives. Those concerns include:

- Can devices connected through the Internet be subjected to malware attacks?
- Can these devices be used for launching DDoS attacks?
- Will poorly secured devices serve as entry points for cyberattacks?
- Will the data transmission from these devices be tapped, resulting in data leakage and privacy-related issues?

Addressing these challenges to ensure that IoT products and services have controls to mitigate risk needs to be considered before implementing these services and products. The concerns are further escalated due to the complexity involved in deployment of IoT products and services. Other considerations such as mass deployment, device-to-device communication channels, placing these devices in unsecure environments and other vulnerabilities present in back-end environments that are generally deployed using cloud technology further add to this complexity. IoT devices are deployed at many locations like homes, offices, retail stores, buildings, hospitals, factories, worksites, vehicles and city areas.

The success of these IoT-based services and products depends upon the question, “Will users trust these products and services?” To establish this trust, the service providers must be able to secure IoT devices from vulnerabilities.

The security concerns related to IoT are:

- The cost of devices may increase due to security that needs to be implemented.
- Interoperability of devices is a concern since there are many entities to which the devices need to be connected. These can be another device by another manufacturer, gateway service provider, platform service provider and data users.
- Upgrading of devices or patching devices to addresses vulnerability identified after deployment. Users may not follow the necessary upgrade process due to inconvenience.
- Patching vulnerabilities after deployment may be challenging and more costly.
- Devices deployed cannot be maintained due to nonavailability of the manufacturer/maintenance contract, etc.
- Cross-border regulatory and legal compliance issues may make it harder to ensure the security of IoT devices.

To address these concerns, one needs to adopt a collaborative approach to security. The classical approach for gathering information and ensuring cyber security will help in providing reasonable assurance to the users. The following points may be considered:

- **Risk assessment**—While planning for the development of IoT-related devices and services, a detailed risk assessment using business is the first step. Many organizations adopt an asset-based risk assessment approach for information

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.

Sunil Bakshi, CISA, CRISC, CISM, CGEIT, ABCI, AMIIB, BS 25999 LI, CEH, CISSP, ISO 27001 LA, MCA, PMP
Has worked in IT, IT governance, IS audit, information security and IT risk management. He has 40 years of experience in various positions in different industries. Currently, he is a freelance consultant and visiting faculty member at the National Institute of Bank Management, India.

technology that may not help in this situation. One needs to consider "uncertainty in achieving business objectives" and evaluate risk based on the possible impact not only on business but also on users of these interconnected devices.

- **Secure application development**—IoT devices are placed on the Internet and, hence, are subject to Internet-related risk. Considering the mass-scale deployment, it will be extremely difficult and definitely not cost-effective to monitor these devices for known cyberattacks like the internal IT environment would be able to do. Hence, building security into the design of devices and applications that will be controlling these devices while developing the applications is the best preventive approach.
- **Communication channel security**—Almost all IoT devices are connected to the Internet on Wi-Fi connections at a user's home or office, or wherever the device is situated. If this connection is insecure, IoT may be compromised. For example, an unprotected refrigerator or a television infected with malware might send thousands of harmful spam emails to recipients worldwide using the owner's home Wi-Fi Internet connection.[1]

  IoT devices adopt multiple communication models:[2]

  – Device-to-device

  – Device-to-platform (cloud)

  – Device-to-gateway

  – Back-end data-sharing

  Deployment of these models depends upon the products and services provided. Security of communication depends upon the answer to the question: "How secure are these channels?" Using encryption at the application level is one way of securing the communication; however, the issue here is that of interoperability between gateway service providers, cloud or platform service providers, device manufacturers, and users of back-end data shared from a platform (cloud).
- **Platform security**—Organizations hosting platform services must adopt the cloud security guidelines.
- **Performance metrics for devices deployed**—Since these devices can communicate, capturing performance-related data is easier. However, it must be supported by monitoring of performance and identifying issues, if any.
- **Privacy-related compliance**—Since IoT devices collect and communicate the data to back-end or other devices, users must be aware of the nature and type of data being communicated. As per privacy principles, providing notice and choice of option must be provided before deploying the device.
- **Threat monitoring and incident management**—Threats to the back-end platform must be monitored; however, due to the spread of IoT devices, it is impossible to monitor each one of them individually and take corrective action.

Q I'm still struggling with auditing the cloud environment. I know about resources like the Cloud Security Alliance Security Trust and Assurance Registry (CSA STAR) and Cloud Controls Matrix (CCM) and Consensus Assessments Initiative Questionnaire (CAIQ)—I also leverage other artifacts like the Payment Card Industry Data Security Standard (PCI DSS) information (e.g. Ro's, etc.), Service Organization Controls (SOC) audits, etc.

However, only a subset of the service providers in my environment have these artifacts. What are some best practices for how to get this done—particularly in smaller service providers that might not know what any of these things are?

A Any audit is planned based on the scope of the audit. Now what is the scope of your audit? I assume that you are auditing an organization that is using a third-party cloud service provider for information technology. It can be for only infrastructure (IaaS); or platforms (PaaS), including operating systems, databases, middleware except application; or it may use applications hosted on the cloud (SaaS). The audit objectives will change depending upon the type of service.

Continue auditing by understanding the auditee organization's objectives. When it comes to auditing cloud services provided by a third-party service provider, use auditing techniques like any other third-party service provider with the focus on the organization's objectives. Verify the contract for type of assurance from the service provider. Please note that use of third-party cloud services is the same as outsourcing at a third-party location. (You may refer to vendor management using COBIT® 5 for guidance. The book has one chapter on managing cloud service providers.[3])There could be two options in the contract:

1. Service provider allows you, as auditor, to audit the cloud environment.
2. Service provider provides an independent external auditor's report.

In the case of the first option, where you need to audit the cloud service provider, the resources you mentioned are useful. The primary advantage of these resources is that they provide a benchmark for selecting appropriate controls. Please note that only applicable controls from the CSA's CCM might be required to be audited based on the service levels. The CAIQ—assessment-friendly version of the CCM using yes/no questions—may also help for quick assessment.

CSA's STAR registry[4] is a list of cloud service providers that comply with CSA's security requirements. IT is the same as ISO 27001 certification, which may provide a limited assurance that the third party has implemented required controls; however, their ongoing effectiveness needs to be verified.

In the case of the second option, the cloud service provider has many clients and therefore may not agree to be audited by each client. In this scenario, ensure that the independent auditor's report is made available. Earlier, the SAS 70 audit report was most common, which has now been replaced by SSAE16/ISAE 3402.[5] It has three types of reports:

- SOC 1 is on relevant controls over financial reporting.
- SOC 2 is on the security, availability, integrity, confidentiality and privacy of information systems.
- SOC 3 is like a certification and does not provide details of the testing performed.

Some expert auditors opined that SSAE 16 is stricter than ISAE 3402, because it requires the auditor to assess the risk associated with Intentional Acts by Service Organization Personnel.

Endnotes

[1] Starr, M.; "Fridge Caught Sending Spam Emails in Botnet Attack," CNET, 19 January 2014, *www.cnet.com/news/fridge-caught-sending-spam-emails-in-botnet-attack/*

[2] Rose, K.; S. Eldridge; L. Chapin; *The Internet of Things: An Overview*, October 2015, *www.internetsociety.org/sites/default/files/ISOC-IoT-Overview-20151022.pdf*

[3] ISACA®, COBIT® 5, USA, 2012, *www.isaca.org/COBIT/pages/default.aspx*

[4] Cloud Security Alliance, CSA Security, Trust and Assurance Registry (STAR), *https://cloudsecurityalliance.org/star/*

[5] International Standard on Assurance Engagements, ISAE No. 3402*, http://isae3402.com/ISAE3402_overview.html*