MBS-TS09

Achieving Operational Security Excellence in Connected IoT Solutions

IoT Solution Implementation Questionnaires

Compliments of @MicheleDGuel
mguel@cisco.com

Executive Level IoT Security Engagement Questionnaire

The purpose of this questionnaire is to assist senior business leaders, typically at the C-level with the prioritization and funding IoT related projects. The questionnaire is intended to be completed prior to the "Business Commit" phase of a project. Ideally, for any project that has potential security and privacy risks, security engagement at the earlies stage of the project ensures greater success for the overall program.

1) **What is the expected business benefit of the IoT solution?** (Select all that apply)
   The purpose of this question is to invoke thought and validation as to the motivation or justification for the IoT solution. Senior business leaders should have a first grasp of the business outcome. It is possible that multiple business outcomes are desired.
   a) Revenue Growth
   b) Resource Optimization
   c) User Experience
   d) Business Process Optimization
   e) Data insights
   f) Other (Please Describe)

2) **Which IoT vertical(s) does the project or solution involve?** (Select all that apply)
   This question is geared at a future possible risk model that assigns a risk score based on vertical. The assumption is some verticals are more critical that others due to the information they process or physical world interactions they can impact.
   a) Healthcare
   b) Manufacturing
   c) Transportation (parking, bus, rail, fleet management)
   d) Building Automation (power, lighting, temperature)
   e) Security (surveillance, access, incident notification)
   f) Other (Please Specify)

3) **Does the IoT solution involve the collection, use or process of any data attributes that identifies an individual or from which identity or contact information of that individual can be derived?**
   Any collection, use or processing of personal data influences overall risk of the solution and the level of security and privacy requirements. If the answer is "yes" here, then it is recommended to complete a Privacy Threshold Assessment at this phase.
   a) Yes
   b) No
   c) Unknown

4) **Has this specific IoT technology been implemented or used in the environment before?**
   The intent of this question is to establish the reputation and/or familiarity with the technology. If the technology has been used within the organization or vendor references were validate, the risk is likely lower.
   a) No. This will be the first time this technology is used in our organization.
   b) Yes. This project is an extension to a current production solution that involves the same technology.

c) Yes. However, this project involves using the technology in a new way or in a different part of the organization.
d) Unknown

5) **What is the potential impact if all or parts of the IoT solution were to be successfully attacked, and data was disclosed, or the system malfunctioned?** (Select all that apply)
The intent of this questions it to help quantify the risk in the event of a system compromise. There are several levels of a compromise, not all of which involve a severe impact. Consider potential worse case scenarios that are plausible.
a) Disruption to resources that critical to run the business (e.g. building environment controls)
b) Disclosure of data that is regulated by a law (e.g. Personally Identifiable Information)
c) Severe impact to environment (Fire, flood, air pollution, etc.)
d) Destruction of physical property
e) Impact to human life, up to and including death
f) Other (Please Describe)

6) In the event of a system or data breach, what amount of financial loss in terms of percentage of earnings before interest and taxes (EBIT) would be considered "material"?
The intent of this question is to frame the acceptable amount of total financial loss due to a system or data breach. This would include all areas such as fines, notification, credit monitoring, loss of intellectual property, etc.). Some organizations have established this number as a normal part of operations.
a) Less than ½%
b) Less than 1%
c) Less than 3%
d) Less than 5%
e) Other (Please Describe)

7) Are there any known security risks that would result in an impact listed in Item 5 or a potential system or data breach?
The IoT market is rapidly evolving and first-generation products may lack appropriate security controls or may not have been subjected to extensive testing and validation. Or there may be known vulnerabilities in the product (e.g. does not support encrypted transport) or there have been publicized breaches involving this product. At this stage of the project, it is important to consider if the known risks are commensurate with the risk appetite of the organization or the intended users of the solution.
a) Yes (Please Describe)
b) No
c) Unknown

8) What is the expected timeline for the entire program, including any proof of concept or pilots?
Complex IoT implementations, such as multiple facets of a smart city or connected manufacturing may take 3-5 years for the full roll-out. There are several factors, such as organizational change, political climate, and budgeting challenges that can impact multi-year projects. A specific challenge in the IoT space is that a stalled or halts large scale program can result in a partially configured (and

secured) ecosystem of hundreds or thousands of sensors, which can be targeted by threat actors and used a launching point for cybersecurity attacks.

a) Less than 1 year
b) 1-2 years
c) 2-3 years
d) 4-5 years
e) 5 years or more

9) What percentage of the total program has committed funding from executive management?
This question related to Item 8 above. If budget is not secured for the entire roll-out of the IoT solution, there is a risk non-completion, potentially resulting in orphaned IoT endpoints that can become targets for threat actors.

a) 100%
b) More than 50%
c) More than 25%
d) Less than 25%
e) Other (Please Specify)

10) Is there a defined owner for the end-to-end solution and does this person embrace their role as an owner and feel truly accountable for any adverse outcome in the event of a system or data breach?
If the designated owner does not fully embrace their role as the owner, there is the potential their decisions and actions don't account for possible outcomes. In the case of multiple owners (think about a cross-functional solution), there can be challenges with agreement on action.

a) Yes, there is a single owner. (Provide name of owner)
b) Yes, there are multiple owners. (Provide names of each owner)
c) No, an owner has not been identified yet
d) Unknown

IT Leader IoT Security Engagement Questionnaire for IoT Projects

The purpose of this questionnaire is to assist IT leaders and/or Service Owners with the prioritization and funding IoT related projects. The questions in this section are intended to guide risk-based discussions with the IT and/or OT leader s and the questionnaire is intended to be completed prior to the "Concept Commit" phase of a project. Ideally, the appropriate security and privacy teams should be engagement by the Concept Commit phase or earlier. I

If the executive level engagement questionnaire has not been completed at this phase, we strongly recommend that the IT Leader or Service Owner complete that questionnaire as well.

1) **What type of data will be collected, used or processed on this IoT solution?** (Select all that apply)
   The type of data involved in this solution will guide the level of security requirements to offset the risk. It's also important to consider if there are new types of data that will be collected or used, and will the data be aggregated or anonymize.
   a) Health Data (Heart Rate, Glucose level, Activity level, etc.)
   b) Sensitive user data (Personally Identifiable Information, Salary, etc.)
   c) User Presence data (How many people are in a specific location)
   d) Environmental data (Air quality, Water use, Power Use, etc.)
   e) Endpoint operational data (battery life, uptime, firmware version, etc.)
   f) Other (Please Describe)

2) **Which statement(s) below reflects current state of IoT endpoints in your infrastructure?**
   The current infrastructures ability to effectively detect, manage and control IoT endpoints is a foundational principle to gauging the risk and complexity of introducing IoT technology for the first time or expanding existing implementations. Organizations which have fully embraced Bring Your Own Device (BYOD) will in theory be ahead of the game in terms of ability to support IoT endpoints.
   a) We fully support IoT endpoints in our infrastructure and we establish and enforce network polices based on the intended use of the devices.
   b) We have IoT endpoints in our infrastructure and we have a process (or technology) to register them with a known identity (e.g. this is Michele's Fitbit).
   c) We have IoT endpoints in our infrastructure and we have a process (or technology) to identify and profile them.
   d) We are certain we have IoT endpoints in our infrastructure, but we do not have a way to identity them.
   e) Unknown

3) **What is the expected scale of this solution in terms of the number of IoT endpoints?**
   Scale is one of the six characteristics that differentiate IoT from a security perspective as discussed in Section 2.1. Organizations may be able to support hundreds of IoT endpoints but may be very challenged to support thousands of endpoints.
   a) Dozens
   b) Hundreds
   c) Thousands
   d) Hundreds of Thousands
   e) Over a Million

4) **Have you validated that all vendor products meet IoT Critical 9 requirements?**
As a part of product evaluations, it is important to ask and validate if the products meeting the established minimum-security requirements for IoT products. The IoT Critical 9 has been established as a starting point for the minimum requirements.
   a) Yes
   b) No
   c) In-progress
   d) Unknown

5) **Are there government regulations that apply to this IoT solution?**
There are many instances where government regulations might apply. Some examples include: Use of personally identifiable information; Critical infrastructure, medical management and transportation solutions. The team may need to consult the legal group, privacy group or other groups to determine which regulations may apply.
   a) Yes (Please provide a list)
   b) No
   c) Unknown

6) **Which statement below most accurately describes the vendor viability and product maturity?**
The IoT market is rapidly evolving and expanding, involving many young start-up companies. Since IoT implementation may be complex projects lasting 3-5 years, it is important to consider the long-term viability of the vendor in terms of product maturity and ability to deliver and support. Also, take into consideration if there are other vendors who provide a similar product in the event that your primary vendor goes under.
   a) The vendor is a start-up company (< 3-year-old) and the product is first generation.
   b) The vendor is a start-up company (< 3-year-old) and the product is second generation.
   c) The vendor is a well-established company and the product is first generation.
   d) The vendor is a well-established company and the product is second generation or later.
   e) Unknown

7) **Which statement below describes how and where the solution will be implemented?**
The sensitivity of data, criticality of the solution in terms of day to day operations and the impact of outages should impact decisions regards how the solution will be implemented. Think about the entire solution in terms of how it will be installed and who will manage the day to day operations.
   a) Fully on-Prem in a single geographic location.
   b) Fully on-Prem in multiple geographic locations (e.g. United States and Europe)
   c) Hybrid model with some components on-Prem and some components hosted by third party SaaS providers.
   d) Fully hosted by one or more 3rd party SaaS providers.
   e) Undecided at this stage.

8) **Which statement below best describes the implementation team?**
The makeup and skill level of the implementation team can be a factor for a new technology area such as IoT. This is such a large space, it can be difficult to find implementation teams with the necessary skill level and experience to ensure success for the project.
   a) The implementation team is internal to the organization.
   b) The implementation team is internal to the organization and has experience with this technology.

c) The implementation team is an established partner.
d) The implementation team is an established partner and they have experience with this technology.
e) Implementation is being done by 1 or more established partners
f) Implementation is being done by 1 or more new partners.

9) Does the IoT Solution or Service involve any safety requirements or regulations?

IoT solutions that involve "wearables" may have specific requirements around ensuring device casing is not an irritant to skin, etc. IoT solutions that involve components installed in publicly accessible locations may have requirements for ruggedize design and tamper-proof enclosures.

a) Yes (*List known safety requirements*)
b) No
c) Unknown

10) Is the current IT infrastructure capable of support this IoT solution?

Are there any scaling issues (network bandwidth, power consumption, datacenter availability) or other infrastructure elements that may impact the success of this IoT solution? For example, does it require it require any level of infrastructure refresh?

a) Yes (Please list all known dependencies)
b) No
c) Unknown

IoT Security Implementation Worksheet

The purpose of the IoT Security Implementation Worksheet is to provide a foundation for technical implementers of the IoT solution to understand and evaluate the security issues within the various asset classes of the solution. It is meant to be a living document and grow over time. The current document covers some basic security questions around endpoint devices and gateways, supply chain, network, people, cloud/data center, and data collection. Additionally have a few questions on the extensibility of the overall solution.

1.1 Endpoint Device/Gateway Considerations

1. Describe the intended use for this IoT endpoint (e.g. controls led lighting)
2. Is this a brand-new device or an addition to an existing device?
3. Is your endpoint device free from backdoors? (e.g. non-documented interfaces)
4. Does your endpoint device have a JTAG interface? Is it disabled or been removed from production devices?
5. Does your endpoint device contain default credentials? Are they required to be changed after initial use?
6. How are credentials and configuration data provisioned on your device?
7. How are credentials stored on the endpoint device?
8. How does your endpoint device connect to the network?
    a. Through a gateway
    b. Through a multi-node peer network
    c. Direct connection to the internet
9. Is the endpoint device using a wired or wireless connection?
10. How does your endpoint device authenticate to the network?
11. Does your endpoint contain a Trust Platform Module/Hardware Security Module?
12. What security protections does your endpoint device support? (Mark all that apply)
    a. Secure Boot and signed images
    b. Data Execution Prevention (DEP)
    c. Address Space Layout Randomization
13. Are there any constraints which prevent you from enabling security features or protections?
    a. Regulatory
    b. Power
    c. Environmental
    d. Safety
    e. Reliability
    f. Economic
14. Describe the process to perform a firmware, software, or O/S update. This can be a reference to installation documents.
15. What protocols and ports does your endpoint device require to operate? Are the unused ports open by default?

16. Is your endpoint device traffic encrypted? How?
17. If your endpoint device is publicly accessible, how are you protecting and/or monitoring for physical tampering?
18. Is there an administrative interface or portal? Are users authenticated? Does it use secure connections for users and devices?
19. Does the device store any sensitive data locally (network credentials, usernames/passwords, etc.)? Is this data encrypted?
20. How is your device cleared of sensitive information before disposal/end of life?

1.2 Supply Chain

List and describe the major components that make up the endpoint device.

1. Who made the component? Did the vendor make the component or did they simply rebrand it (e.g. OEM)?
2. Which country(s) was the product manufactured? Does the country have a previous history of tampering with devices (e.g. installing backdoors)?
3. What 3rd party code is used in the component?
4. Is the component properly licensed?
5. How does the vendor keep up with patches/upgrades?
6. How often does the vendor provide upgrades and patches?
7. Are there any certifications or standards that the vendor can provide that can attest to the trustworthiness of your supply chain?
8. Does the 3rd party code conform to secure coding guidelines?
    a. Do they use Safe C libraries?
    b. Does their code do input validation?
    c. Do they perform static analysis?
    d. Do they perform fuzzing testing?
    e. Do they enable security compilation flags, such as those that enable Address Space Layout Randomization (ASLR), and Built-In Object Size Checking (BOSC)?
    f. Do web-based software protected against common web threats (OWASP Top 10)?
9. Has the vendor performed hardening of the component (e.g. disabled unnecessary features/services)?
10. How long will the vendor support the component? Does this include security updates?

1.3 Network

1. Is your IoT network traffic segmented? How?
2. Where are the intersection points between zones?
3. What type of data is traversing these zones?
4. Where are the trust boundaries?
5. How is your network protecting itself from unintended usage of your endpoints? (e.g. how are the endpoint devices prevented from being used to attack infrastructure or others)
6. Does your network have the capacity to handle the influx of traffic without impacting performance?

1.4 People

1. What sort of security training does your personnel have?
2. Have you completed background checks on your personnel?
3. Who in charge of your incident response?

1.5 Cloud/Data Center

1. What sort of hardening has been done on your infrastructure?
2. What sort of security monitoring is in place?
3. What type of security logging/auditing do you have in place?
4. What sort of access controls are in place?
5. What sort of identity access management solution is place?
6. Do you conform to guidance from the Cloud Security Alliance (CSA)?

1.6 Data Collection

1. What geographical regions will data be collected? (Select all that apply)
    a. US
    b. Mexico
    c. Highly restricted countries in Europe (Finland, Estonia/Latvia, Portugal)
    d. Other Europe
    e. Russia
    f. China
    g. Other Asia
    h. Africa
    i. Australia
    j. Argentina
    k. Other South America
    l. Other
2. Will data be collected in a different region that it will be stored?
    a. Yes
    b. No
    c. Unknown
3. How will the data be accessed by the end “users”?
    a. Directly on the endpoint
    b. Through a report or snapshot of the data
    c. Remotely through API’s
4. What user groups will have access to this data?
    a. System administrators
    b. End users
    c. Business users
5. Will the data be shared or sold, via an export, to third parties?
    a. Yes
    b. No
    c. Under consideration

    d. Unknown
6. Will the data be anonymized?
    a. Yes
    b. No
    c. Under consideration
    d. Unknown
7. Will the data be and aggregated?
    a. Yes
    b. No
    c. Under consideration
    d. Unknown
8. Will data collected be combined in new ways and offered to third parties?
    a. Yes
    b. No
    c. Under consideration
    d. Unknown
9. What implications could there be in case of the data becoming public?
10. Can we estimate damage in dollars if a third party was attacked by our thing and we can be liable?
11. Are there any special laws around access or retention that need to be taken into account (US, European, Chinese, …)

1.7 Overall Solution

1. Will device/service be fixed in scope or extensible with software updates/hardware accessories?
2. If extensible, how will updates be applied (manually by administrator, automatically through remote commands, etc.)?
3. Is your solution designed in such a way to be reusable by other IoT solutions?
4. Will this be integrating with an existing system or will it be an independent setup?
5. How will everything be managed (cloud-based administration, local software, etc.)?