NMHC OPTECH_
CONFERENCE & EXPOSITION

Assessing Third Party Risk when Implementing IoT

Questions to Ask Third Party Suppliers:

- What data or metadata is collected, generated and stored or transmitted by the device?
- How is data stored on the device?
- How is data transmitted between the device and a central control system or cloud platform?
- Do the devices involved have security and privacy configuration settings?
    - If your organization has standards, regulations, or laws with which they must comply, those should be articulated for the provider and the provider should be able to articulate their ability to comply.
- Do devices have anti-tamper detection capabilities or tamper resistant features?
- What are the recommended connectivity and configuration options for the device to operate optimally while ensuring security and privacy?
- How often does the provider issue updates or patches for the firmware and software on the device? How are those delivered?
    - Do devices have to be connected to the Internet to receive updates?
    - Does the provider need remote access to devices for maintenance or monitoring?
    - Will the provider need physical access to the building or individual residential units to maintain devices or systems?
- Are installation and configuration services included with purchase?
    - Does installation include security configuration?
- How does the provider protect our company information? (contact information, names of personnel who server as points of contact, payment information, information on facilities)
- How does the provider protect the source code, firmware builds and hardware used in the devices?
- If a cloud-based platform is used to store data or configuration settings, or provide remote access to controls, has the cloud platform been penetration tested (also referred to as “pentest”) and a third-party vulnerability assessment performed?
    - How often are third party assessments performed?
    - Can they share the results of the most recent third-party assessment?
        - If not, how quickly were they able to resolve each of these: critical findings, “high” risk findings and “medium” risk findings
- What is the provider’s policy on notifications to customers in the event of:
    - Critical vulnerabilities
    - Threats specific to devices or systems
    - Data breach
    - Information leakage
    - Network intrusion or system compromise
    - Any systems failure or denial of service that could delay or impede monitoring or maintenance.
    - Availability of security updates for software/firmware
    - Safety recalls on hardware components
- If devices are leased, who is responsible for security and maintenance?
- How does the supplier ensure supply chain security and reliability for platforms, software, and hardware components in the system or devices?

- What happens when a device is decommissioned, broken or will not be repaired or re-used?
    - Are devices to be re-used purged of any stored data?
    - How is data destroyed or preserved and protected for privacy reasons?
- If devices are upgraded at a future point to incorporate a later version of the device, will this require a whole system upgrade, or will new devices be backwards compatible? How will the ability to secure the new devices and their integration with older system components be managed?
- Who is the Original Equipment Manufacturer (OEM)?
    - How many devices by that manufacturer have critical flaws?
    - How does the OEM prevent insiders from tampering with or adding spyware or malicious software or hardware components to the devices?
    - Does the OEM have a history of non-compliance with regulations in their country of origin?
    - Does the OEM have a relationship with foreign intelligence agencies?
- Is the supplier aware of any threat actor groups that have specifically targeted the company or particular devices or systems?
- Does the provider have an insider threat management program?
    - How are employees vetted for employment eligibility? Background checks?Credit checks?
    - How are employees trained and assessed on their knowledge and use of security best practices over time?
    - What controls are in place to ensure that only employees with a "need-to-know" have access to PII, payment information, or customer information?
    - What controls are in place to detect employee misuse of company equipment or information?
    - How is the termination process managed when an employee separates from the company?
        - Access to online systems, information assets, and remote access?
        - Physical access?
    - How often are physical and electronic access logs audited?
- What additional third parties does the supplier use to provide equipment and services and what information is shared with them in order to provide services or equipment to us?
    - Are the confidentiality agreements or non-disclosure agreements (NDAs) with the supplier's third parties available for review?
    - How does the supplier monitor and hold its third parties accountable for compliance with privacy and security requirements?

Additional Resources

Resource for Suppliers and Third Parties from ISACA – A Guide to Responding to Third Party Questionnaires: https://bit.ly/2RFMpgs

Framework for a Third-Party Risk Management Program from American Bar Association: https://www.aba.com/Tools/Offers/Documents/MCO.pdf

Example Third-Party Assessment Information Security Questionnaires:
https://www.vendorsecurityalliance.org/questionnaire2018.html
https://bit.ly/2FcKy1i
https://cloudsecurityalliance.org/artifacts/consensus-assessments-initiative-questionnaire-v3-0-1/