KPMG

Smart-X

A holistic approach to cybersecurity for smart devices

January 2024
KPMG Professional Services

Content

Foreword

The increasing adoption of Internet-of-Things (IoT) technologies and smart devices introduces a new era of connectivity where physical objects are embedded with the ability to interact with their environment, execute autonomous activities, and connect with other objects or networks. This paradigm shift holds immense potential to enhance convenience and efficiency and unlock new functionalities across industries, including energy, automotive, government, and healthcare.

Over the coming years, there will be a surge in interconnected smart devices, transforming nearly all sectors, such as healthcare, transportation, manufacturing, and retail. From personalized health insights through wearables to autonomous vehicles, AI-driven manufacturing optimization, and immersive retail experiences enabled by AR and VR, there are numerous advancements anticipated. This growth is made possible by enhanced connectivity through 5G networks and edge computing.

However, the increasing interconnectivity of these technologies – what we will dub Smart-X technologies – brings forth significant security concerns. Data ownership, protection of smart devices, and privacy are central challenges that must be addressed. To ensure the security of Smart-X technologies, stakeholders need to develop comprehensive cybersecurity strategies, employ industry-standard encryption mechanisms, and prioritize application security.

Moreover, the expansion of these technologies also introduces new risks and vulnerabilities. Cybersecurity breaches can range from minor inconveniences to major threats to public safety, security, and privacy. Therefore, securing Smart-X technologies is not just crucial for protecting individual entities, but also for preserving the integrity, safety, and security of entire sectors and infrastructures.

To enable security, a holistic approach must be taken to the entire lifecycle of Smart-X devices, starting from secure design until the decommissioning of Smart-X devices, or it will fail. This includes considering the supply chain and recognizing that security is not just a support function but a business enabler for a digital transformation journey. Higher maturity in security practices is required to effectively mitigate the risks and ensure the security of these technologies. Given the risks and opportunities involved, we consider this topic to be of critical importance.

Ton Diemont
Partner,
Cybersecurity & Data Privacy

Hytham Elsohl
Director,
Cybersecurity & Data Privacy

The advent of Smart-X technologies

In recent years, the rapid advancement of technology has redefined the way we interact with the physical world around us, ushering in an era where objects and devices have the ability to communicate, analyze, and operate autonomously.

This seamless integration has been facilitated by innovative features, including intuitive user interfaces and machine-to-machine communication. As we stand on the cusp of a revolution guided by Smart-X technology, it is becoming increasingly evident that these interconnected systems are paving the way for unprecedented functionalities. These intelligent devices, driven by algorithms and artificial intelligence, are expected to play a central role in the next wave of digital transformation, touching nearly all sectors such as energy, healthcare, automotive, industrial manufacturing and government operations.

To facilitate a cohesive understanding in the context of this paper, we define Smart-X as any physical object that utilizes connectivity protocols to connect with other objects or networks. These devices possess the ability to interact with their environment or users and can execute autonomous activities.

This interactivity can be realized through various means. Sensors, for instance, enable the capture of data from the environment, such as temperature sensors in smart thermostats or motion sensors in security cameras. User interfaces, such as touch-screens on smart home hubs, facilitate user input and settings adjustment. Additionally, machine-to-machine communication enables devices to communicate with one another without human intervention.

A noteworthy characteristic of smart devices is their potential for autonomous activities. Governed by algorithms and artificial intelligence, these activities can range from simple tasks like automatic temperature adjustments based on occupancy in smart thermostats to complicated operations like predictive maintenance in industrial IoT devices. Such autonomous capabilities enhance convenience and efficiency and even unlock new functionalities that were previously unattainable with traditional, non-connected devices.

The future of Smart-X security holds immense potential, with an anticipated surge in demand driven by key sectors that rely on data-intensive operations and prioritize stringent security measures. Industries such as energy, automotive, government, and healthcare are expected to be at the forefront of this growth. As the need for secure and interconnected solutions continues to escalate, Smart-X is poised to play a pivotal role in shaping the future of these sectors, ensuring their operations remain efficient, reliable, and protected.

Why is it relevant

In the future, homes will be equipped with interconnected smart devices and systems that seamlessly communicate with each other. Voice assistants will become ubiquitous, controlling lighting, temperature, entertainment, and security. It is forecasted that the number of IoT devices worldwide will double from 2022 to 2030, reaching an estimated 29.4 billion devices.[1]

The integration of smart technologies will revolutionize sectors such as healthcare. Wearable devices and health monitors will continuously collect and analyze vital signs, providing personalized health insights and enabling early disease detection.

Furthermore, autonomous vehicles will become more common, with a market share of 5% worldwide by 2030.[2] Connected cars will communicate with traffic systems, optimizing routes and reducing accidents. Ride-sharing services will be enhanced, reducing the need for individual car ownership.

Smart manufacturing, with the help of AI, robotics, and automation, will maximize the efficiency of production processes. Machines will gather real-time data to predict maintenance requirements and continually refine operations. Through digital twins, virtual simulations and testing will be made possible, and customization will fulfill the unique preferences of individual customers.

In the domain of modern retail, the shopping journey will be elevated through connected in-store technologies. NFC-enabled price tags can offer detailed product information when tapped with a smartphone, while RFID-embedded garments enable rapid checkout and inventory tracking. Through the integration of IoT, smart shelves can alert staff when restocking is needed, and AR displays allow customers to visualize products in different colors or settings before making a purchase.

All these advancements will be underpinned by enhanced connectivity. 5G networks will provide ultra-fast and reliable connectivity, facilitating real-time data exchange and enabling new applications. Edge computing will become more prevalent, enabling faster processing and reducing latency for critical applications.

With increased interconnectivity, ensuring data privacy and security will become paramount.

Why we need to secure Smart-X objects?

Smart-X technologies, which operate outside the confines of traditional IT data centers, introduce unique security challenges that set them apart. These challenges arise due to diverse operating environments (hospitals, factories, homes, retail spaces, etc.), wide attack vectors, multiple stake-holders, operators with little cybersecurity expertise and other factors.

Data protection
Given the substantial volume of data generated by Smart-X technologies, it is imperative to establish appropriate data ownership, ensuring access is restricted solely to authorized individuals or entities. Weak passwords, unsecured networks, or other vulnerabilities can expose data to breaches that may impact the confidentiality, integrity and availability of the data.

Cyber attacks
Smart-X technologies are not only susceptible to breaches that compromise sensitive data, but also to attacks that could result in the outage of critical services or alter the behavior and decisions of these devices. Such interruptions can have grave consequences, from human safety concerns like compromised medical devices and autonomous vehicles to disruptions in essential services. Alongside threats such as malware, phishing, DoS attacks, and physical breaches, it's imperative to recognize and counteract the potential for these devices to be manipulated or shut down.

Privacy
The collection of personal information by Smart-X technologies necessitates stringent safeguards to preserve individual privacy. However, a lack of adequate security measures or failure to address potential privacy breaches may result in data breaches and the associated consequences.

Companies across various stakeholder groups, from original equipment manufacturers (OEMs) to service providers, and even the owners and operators of Smart-X, should collectively start implementing cybersecurity measures like security by design to reduce human error-proneness and address these challenges as a shared responsibility to ensure the security of Smart-X systems.

By addressing cybersecurity challenges, stakeholders can have a better understanding of the importance of securing Smart-X technologies and start protecting themselves from potential threats.

Security threats and risks

Several real-life incidents underline the significant cybersecurity risks associated with smart technologies.

In 2015, two security researchers demonstrated they could remotely exploit a Jeep Cherokee's smart features, controlling its engine, brakes, and steering, leading Fiat Chrysler to recall 1.4 million vehicles.[3]

01

02

The 2016 cyber attack on Ukraine's power grid, which was coordinated and sophisticated, resulted in a widespread power outage, demonstrating the vulnerabilities of smart energy infrastructures.[4]

In 2017, the FDA confirmed that St. Jude Medical's implantable cardiac devices had cybersecurity vulnerabilities. If exploited, hackers could have depleted the battery or administered incorrect pacing or shocks, posing a significant risk to the patient's health.[5]

03

04

The 2018 SamSam ransomware attack on Atlanta's municipal systems paralyzed essential city services, demonstrating the potentially devastating effects of a cyber attack on smart city infrastructures.[6]

In 2019, a ring security camera installed in a family's home in Mississippi was hacked, and the intruder used the device's speaker system to harass an eight-year old child, highlighting the potential vulnerabilities of smart home systems.[7]

05

These incidents highlight the urgency for robust cybersecurity measures as societies across the world move towards greater reliance on smart technologies. As these technologies continue to grow and interconnect, the associated cybersecurity risks and potential impacts also escalate, making cybersecurity a paramount concern across all sectors.

It is important to adopt a holistic view of the entire Smart-X lifecycle, from product development and manufacturing to operation, maintenance, and even decommissioning, is significant. Stakeholders must also ensure that attention is devoted to the operational longevity and end-of-life stages of Smart-X devices. This is particularly essential as end-users may be directly impacted by cyber attacks on these devices.

With new regulations such as the EU Cyber Resilience Act (CRA) manufacturers now have increased obligations to ensure their products remain secure throughout their lifecycle and to report cyber incidents even post-market. At KPMG, we believe in a holistic approach that addresses the security of Smart-X across its lifecycle.

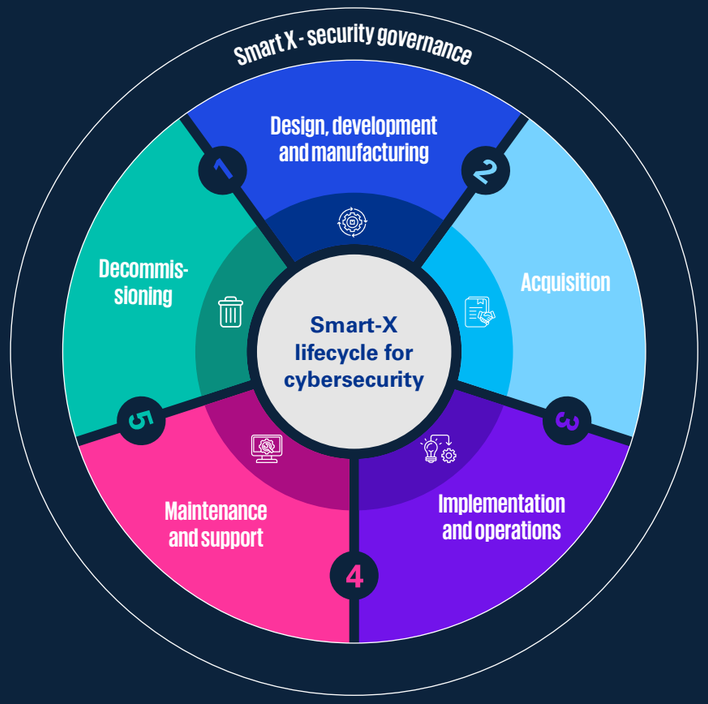
The KPMG approach

In order to mitigate the risks mentioned earlier, we have established a framework that identifies distinct critical domains at each stage of the Smart-X product life cycle, which we deem indispensable in evaluating cyber risks regarding Smart-X. The diagram below illustrates the KPMG Smart-X security lifecycle.

Smart-X security governance

Previously relegated to the post-sales process, it is now vital to embed cybersecurity directly into the business model, ensuring an agile and resilient network that leverages Smart-X technologies safely and maintains trust through evolving governance in the interconnected landscape. Holistic security requires the adoption of methods and toolsets specifically designed to address threats throughout the product cycle.

- Define roles, processes and responsibilities
- Ensure the compliance and awareness with data protection and security standards
- Review and adapt to keep up with changing regulatory requirements, technologies and best practices



1. Design, development and manufacturing

In the foundational stage of the Smart-X ecosystem, stakeholders must prioritize security, weaving considerations such as SBOM (Software Bill of Materials), threat modelling, and security by design and in development seamlessly into every facet of design, development, and manufacturing processes. Utilizing tools like TARA (Threat Analysis and Risk Assessment) further assists in proactively identifying and addressing potential vulnerabilities, facilitating a secure and harmonious interplay among various Smart-X technologies.

- Security design and development
- Security testing during development
- Threat analysis and risk assessment
- Secure hardware and software components from trusted vendors
- Anti tampering capabilities
- Security requirement engineering

2. Acquisition

In the Smart-X landscape, the acquisition phase is pivotal for stakeholders aiming to integrate secure and resilient devices into their networks. It necessitates stringent review processes to guarantee that the products procured are aligned with the essential security benchmarks, safeguarding against potential vulnerabilities in an interconnected ecosystem.

- Benchmarking
- Secure product selection
- Vendor security management
- Smart-X device classification

3. Implementation and operation

In the Smart-X framework, striking a balance between security and safety hinges on continuous operational vigilance because of the hardware limitations. Robust safeguards must be incorporated to prevent security breaches and meet the demands of real-time autonomous activities. AI-driven tools can be pivotal by involving real-time monitoring tools that detect and neutralize threats and facilitate responsible data management in hyper-connected settings.

- Security hardening and enabling security features
- Secure physical deployment
- Identity and access management
- Security integration
- Compliance review
- User awareness training
- Securing availability of operation
- Data and communication protocols security
- Security logging and monitoring

4. Maintenance and support

In the Smart-X ecosystem, continuous maintenance and support are vital in preserving the security integrity of systems and applications. Stakeholders must foster a culture of regular threat analysis and risk assessments to identify and mitigate potential security risks, sustaining a resilient and trustworthy interconnected environment. This proactive stance facilitates a secure operational terrain where Smart-X technologies can flourish, backed by an ongoing commitment to safety and data protection.

- Security testing, patching and fixing of vulnerabilities
- Change management
- Security incident response
- Vulnerability management
- Continuous risk assessment

5. Decommissioning

In the Smart-X sphere, a critical step is to secure decommissioning in responsibly retiring systems and applications to reduce the risks associated with sensitive data exposure. It requires carefully planned protocols to ensure a protective environment where information remains shielded from potential security threats even as technologies are phased out.

- Data archiving
- Data disposal
- Device deactivation
- Authorization withdrawal
- Stakeholder notification

The future is here

The future of Smart-X is promising but also presents new challenges and risks that must be addressed. As the world becomes increasingly connected, the number of smart devices and applications is growing at an unprecedented rate. It presents both opportunities and risks for stakeholders, as they seek to leverage the benefits of smart technology while protecting against potential security threats.

KPMG's five-step lifecycle approach provides a solid foundation for stakeholders to build and maintain secure Smart-X systems and applications. By integrating security considerations into every stage of the Smart-X lifecycle, stakeholders can proactively identify potential security vulnerabilities and respond at the right time to mitigate them. This includes designing and developing systems and applications with security in mind and acquiring products and services that meet necessary security requirements.

It is paramount to consistently uphold and provide support to both systems and applications through the routine implementation of security updates and patches. Furthermore, in instances where systems and applications have surpassed their useful lifespan, secure and comprehensive decommissioning of such platforms should be ensured.

As technology evolves, stakeholders should stay updated with the latest security trends and best practices, which makes it important to take a proactive approach to security, which includes conducting regular risk assessments and compliance monitoring. As they arise, stakeholders must be prepared to adapt to new security threats and vulnerabilities and take appropriate measures to mitigate them before they can be exploited.

In addition to these technical considerations, stakeholders must also address the human interactions that could lead to security threats. This involves ensuring that employees are aware of their roles and responsibilities in maintaining security, as well as providing regular training and awareness programs to keep them informed about the latest security threats and best practices.

By taking a holistic approach to security and incorporating it into every aspect of the Smart-X lifecycle, stakeholders can help to ensure the security of their operations and protect them against potential security breaches. This is critical not only for protecting sensitive information and assets but also for maintaining the trust of customers and stakeholders. In an era of increasing interconnectivity, the importance of security will only increase.

We will detail the application process of the Smart-X framework in forthcoming white papers, showcasing its adaptability across different sectors, including automotive, medical technology, smart energy, and smart cities.

References

Content sources:

[1] Vailshery, L. (2022). IoT connected devices worldwide 2019-2030. Statista. Available at: https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/.

[2] Placek, M. (2023). Worldwide - AV market penetration 2030. Available at: https://www.statista.com/statistics/875080/av-market-penetration-worldwide-forecast/.

[3] Greenberg, A. (2015). Hackers Remotely Kill a Jeep on the Highway—With Me in It. WIRED. Available at: https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/.

[4] BBC News. (2017). Ukraine power cut 'was cyber-attack'. Available at: https://www.bbc.com/news/technology-38573074.

[5] Cybersecurity Vulnerabilities Identified in St. Jude Medical´s Implantable Cardiac Devices and Melin@home Transmitter: FDA Saftey Communication. (2017) Available at: https://moph.gov.lb/userfiles/files/Medical%20Devices/Medical%20Devices%20Recalls%202017/16-1-2017/St_JudeMedicalimplantablecardiacdevices.pdf.

[6] SAMSAM Ransomware Suspected in Atlanta Cyberattack. Available at: https://www.trendmicro.com/vinfo/es/security/news/cybercrime-and-digital-threats/samsam-ransomware-suspected-in-atlanta-cyberattack.

[7] Chiu, A. (2019). She installed a Ring camera in her children's room for 'peace of mind.' A hacker accessed it and harassed her 8-year-old daughter.. Washington Post. Available at: https://www.washingtonpost.com/nation/2019/12/12/she-installed-ring-camera-her-childrens-room-peace-mind-hacker-accessed-it-harassed-her-year-old-daughter/.

Definition sources:

- ENISA Good practices for IoT and Smart Infrastructures Tool. [online] Available at: https://www.enisa.europa.eu/topics/iot-and-smart-infrastructures/iot/good-practices-for-iot-and-smart-infrastructures-tool.
- Madakam, S. (2015). Internet of Things: Smart Things. [online] Available at: https://www.researchgate.net/publication/280830675_Internet_of_Things_Smart_Things.
- Koroniotis, N., Moustafa, N., Schiliro, F., Gauravaram, P., and Janicke, H. (2020). A Holistic Review of Cybersecurity and Reliability Perspectives in Smart Airports. [online] Available at: A Holistic Review of Cybersecurity and Reliability Perspectives in Smart Airports | IEEE Journals & Magazine | IEEE Xplore.
- NIST. (2018) Available at: https://www.nist.gov/programs-projects/smart-and-connected-systems#:~:text=Description,actuators%20that%20can%20seamlessly%20interact.
- SERIES Y: GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS AND NEXT-GENERATION NETWORKS. (2012) Available at: https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-Y.2060-201206-I!!PDF-E&type=items.
- Disruptive Threats Against Business Operations and Their Impact - Focus on Cyber-Physical Systems. (2021) Available at: https://www.csa.gov.sg/Tips-Resource/publications/cybersense/2021/disruptive-threats-against-business-operations-and-their-impact---focus-on-cyber-physical-systems.

Contacts

Marko Vogel
Partner, Cybersecurity
KPMG in Germany
E: mvogel@kpmg.com

Ton Diemont
Partner, Cybersecurity & Data Privacy
KPMG in Saudi Arabia and Levant
E: antondiemont@kpmg.com

Jan Stoelting
Partner, Cybersecurity
KPMG in Germany
E: jstoelting@kpmg.com

Hytham Elsohl
Director, Cybersecurity & Data Privacy
KPMG in Saudi Arabia and Levant
E: helsohl@kpmg.com

Regional leaders

Dani Michaux
EMA Cyber Leader and Cyber Leader for KPMG in Ireland

Matt O'Keefe
ASPAC Cyber Leader and Partner for KPMG in Australia

Prasanna Govindankutty
One Americas Cyber Leader and Partner for KPMG in the US

Contributors

Batikaan Sarikurt
Abdullah Almuawi
Simon Class
Lukas von Ehr
Budoor Almarzouki

kpmg.com/sa