Facts and Fallacies of IoT-Driven Workplace Transformation

Due to the fast-paced, IT-enabled industrial revolution, new and innovative technologies have become more deeply ingrained in business operations and society in general. Notable advancements due to these technologies include smart banking, smart homes, smart wearables, smart home appliances, smart gates and smart vehicles. Many of these technologies are now being used around the world.

The COVID-19 pandemic accelerated this trend by forcing organizations to evolve their existing business models and become more driven by digital technology to continue operations with many employees working remotely. **Figure 1** illustrates the workforce transformation that has occurred during the last two years due to the pandemic.

VIMAL MANI | CISA, CISM, SIX SIGMA BLACK BELT

Is the head of the information security department at Bank of Sharjah. He is responsible for the bank's end-to-end cybersecurity program, coordinating cybersecurity efforts within banking operations across the Middle East. Mani is also responsible for coordinating bankwide cybersecurity strategy and standards; leading periodic security risk assessment efforts, incident investigations and resolution; and coordinating the bank's security awareness and training programs. He is an active member of the ISACA® Dubai (UAE) Chapter. He can be reached at vimal.consultant@gmail.com.

This transformation is enabled and strengthened by the support of multiple modern digital technologies such as the Internet of Things (IoT), artificial intelligence (AI), mobility technologies such as robotics and autonomous vehicles, cloud computing, and social media. IoT plays a significant role in connecting people, processes and technological devices. However, as with any other technology, IoT also has limitations and vulnerabilities that are targeted by adversaries for exploitation purposes.[1, 2, 3]

Some common misunderstandings about the implementation and usage of IoT devices include:

- The IoT ecosystem is built only with electronic sensors.
- All devices integrated into an IoT ecosystem will work well together without any issues.
- The IoT ecosystem cannot be fully secured and lacks privacy assurance controls.
- There are no exclusive security standards available for IoT ecosystems.
- IoT devices work only with wireless connectivity.

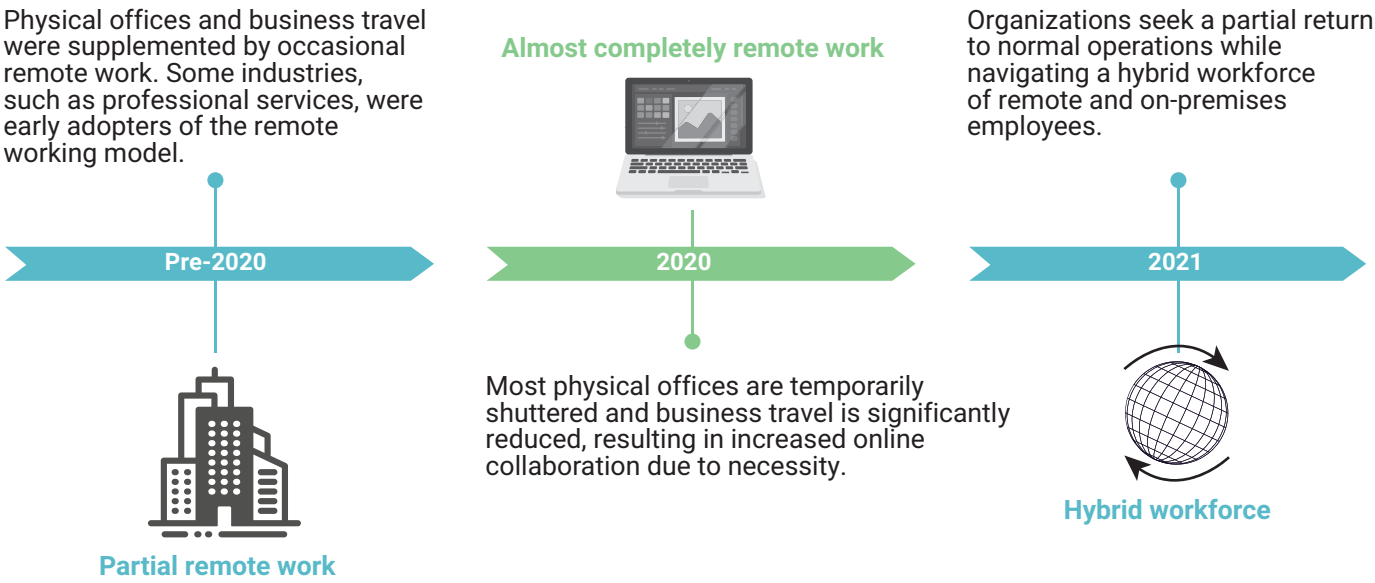
It is important to understand which of these are facts and which are just fallacies to create an effective technology management framework that drives the implementation of IoT ecosystems in a safe, secure and efficient manner.

Advantages of Using IoT Devices

IoT devices are the preferred tools for pandemic-triggered workforce transformation because they have the potential to replace people-driven manual processes such as analytics, monitoring, and control and device administration.[4, 5] The use of IoT-connected robots, drones and sensors is also helping certain industries, such as healthcare, digitize their work. Robots can be used to deliver medicine and food and complete housekeeping tasks on hospital premises.[6] Similarly, in some cases, drones are being used to bring food and medical supplies to areas affected by COVID-19.[7, 8] IoT surveillance systems

FIGURE 1

Workforce Transformation During the COVID-19 Pandemic



are also growing in popularity for protecting property and assets owned by individuals and organizations because they do not need manual intervention. IoT devices can establish baseline user behaviors and detect suspicious user activity.

As organizations worldwide have started to reopen their physical offices, they are supporting staff—and new workplaces—with AI and IoT technologies. Using such devices to monitor health, facilitate remote interactions and aid in contactless access attempts made by staff helps ensure the well-being of employees.[9] Some organizations have established return-to-work policies and are mandating the monitoring of health indicators through wearable IoT devices supported by AI technology.[10] These devices can be used to enable staff to continue working from home (if needed) and facilitate social distancing in the workplace, such as by deploying facial recognition technology to set off alerts if the staff do not maintain social distancing protocols. IoT devices can also track which desks are occupied and how often meeting rooms are used by staff.

Limitations and Challenges of Using IoT Devices

However, although there can be many benefits to the growing use of IoT devices, like many other devices, IoT devices also have limitations and challenges that should be clearly understood when planning for any transformation using IoT technology, because there are increased risk factors and vulnerabilities for organizations that use them.

> "Every connected device becomes an endpoint that can be exploited by adversaries if not secured."

Security and Privacy

Data security and privacy are perceived as major challenges in the use of digital technologies in workplace transformation. IoT devices significantly increase the number of entry points into the network perimeter of an organization. Every connected device becomes an endpoint that can be exploited by adversaries if not secured. And these IoT devices also collect a large amount of user data when they are deployed in work environments. The data collected are often sensitive business-critical data such as in IoT devices used in healthcare and financial services, which means privacy must be ensured. As the abilities and usage of these devices continue to evolve and expand, the security of the user data collected

becomes a major challenge. IoT technology also has memory-related constraints, which makes it more difficult to implement memory-intensive security controls, such as encryption of the IoT ecosystem, which is essential in ensuring the confidentiality and integrity of the data shared among these devices and data transferred from these devices to the outside world. IoT devices also are not exempt from adverse events such as physical tampering, software and hardware vulnerabilities, and cyberattacks.

IoT technology also lacks the dedicated security guidelines that other industrial systems have,[11] which makes it a more appealing target for exploitation by adversaries. However, security and privacy standards, frameworks and laws such as US National Institute of Standards and Technology (NIST) standards, International Organization for Standardization (ISO) standard ISO 27002, North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP), Federal Information Security Management Act (FISMA), and the EU General Data Protection Regulation (GDPR) should be considered for implementation as appropriate and as required based on the feasibility of the organization.

LOOKING FOR MORE?

- Read *Assessing IoT. www.isaca.org/Assessing-IoT*
- Learn more about, discuss and collaborate on information and cybersecurity in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

Compatibility and Interoperability

In an IoT ecosystem, often multiple IoT devices, such as software applications, mechanical devices, electrical devices and electronic devices such as wireless sensors, work together as connected devices. Although certain IoT devices may be efficient on their own, they might not be compatible with other devices because different applications are required for operating different IoT devices. IoT ecosystems often lack the basic interoperability needed to connect various devices seamlessly. Effective use of guidelines from IoT consortiums and standards can help resolve IoT interoperability issues.[12]

Internet Connectivity and Power Supply

IoT devices require Internet connectivity and a continuous power supply to function as expected in an IoT ecosystem. IoT implementation can become a challenge in geographical locations where uninterrupted continuous power supply and Internet connectivity are not available, such as in rural areas where it is not feasible to have power generation resources. Battery-operated IoT devices can be used temporarily in these cases, but it does create increased cost for an organization if used as

> "IoT ecosystems often lack the basic interoperability needed to connect various devices seamlessly."

a permanent solution. IoT devices can work in wired and wireless modes; however, wireless connectivity is critical when an IoT ecosystem needs to connect with a host in a cloud environment. As noted, an IoT ecosystem is an amalgamation of a variety of devices that are connected to each other. These devices need to be integrated in a foolproof manner to provide their intended services. However, issues such as device compatibility and authentication, integration of hardware and software, data management and storage, power supply, and Internet connectivity are major challenges when integrating devices, applications, hardware and databases from various vendors. The technology risk related to these elements also will become a challenge that must be addressed to achieve an effective IoT ecosystem, such as:

- Ineffective user access governance
- Lack of timely deployment of patches and upgrades
- Lack of hardening of the devices
- Usage of weak encryption mechanisms
- Inadequate application security
- Insecure interfaces used by the devices
- Insecure data management

Protecting Against Cyberattacks

Similar to any other information system, IoT devices are vulnerable to cyberattacks. Because an IoT ecosystem consists of a variety of technologies such as sensors, gateways, hardware and software applications, the entire ecosystem may be vulnerable to cyberattacks if any of the individual elements fails to receive ongoing security updates. IoT attacks doubled during the first half of 2021 due to the significant amount of vulnerabilities present in the technologies used by these devices and lack of appropriate security.[13] Some of the major cyberattacks targeting IoT ecosystems include:

- Distributed denial-of-service (DDoS) attacks driven by botnets
- Spoofing attacks
- Code injection
- Man-in-the-middle (MitM) attacks
- Wireless attacks
- Malware attacks such as ransomware

Figure 2 illustrates the various types of attacks that target IoT ecosystems.

Data Privacy Concerns

IoT devices such as those used for health monitoring collect a significant amount of personal data. Any technology-driven device that collects sensitive personal information from the end user should be secured by sound privacy and data protection controls. In addition, the collection of health information may be subject to healthcare laws such as the US Health Information Portability and Accountability Act (HIPAA), violation of which can result in fines or sanctions against enterprises. IoT devices that collect data are also subject to potential attacks that target the privacy of data elements such as:

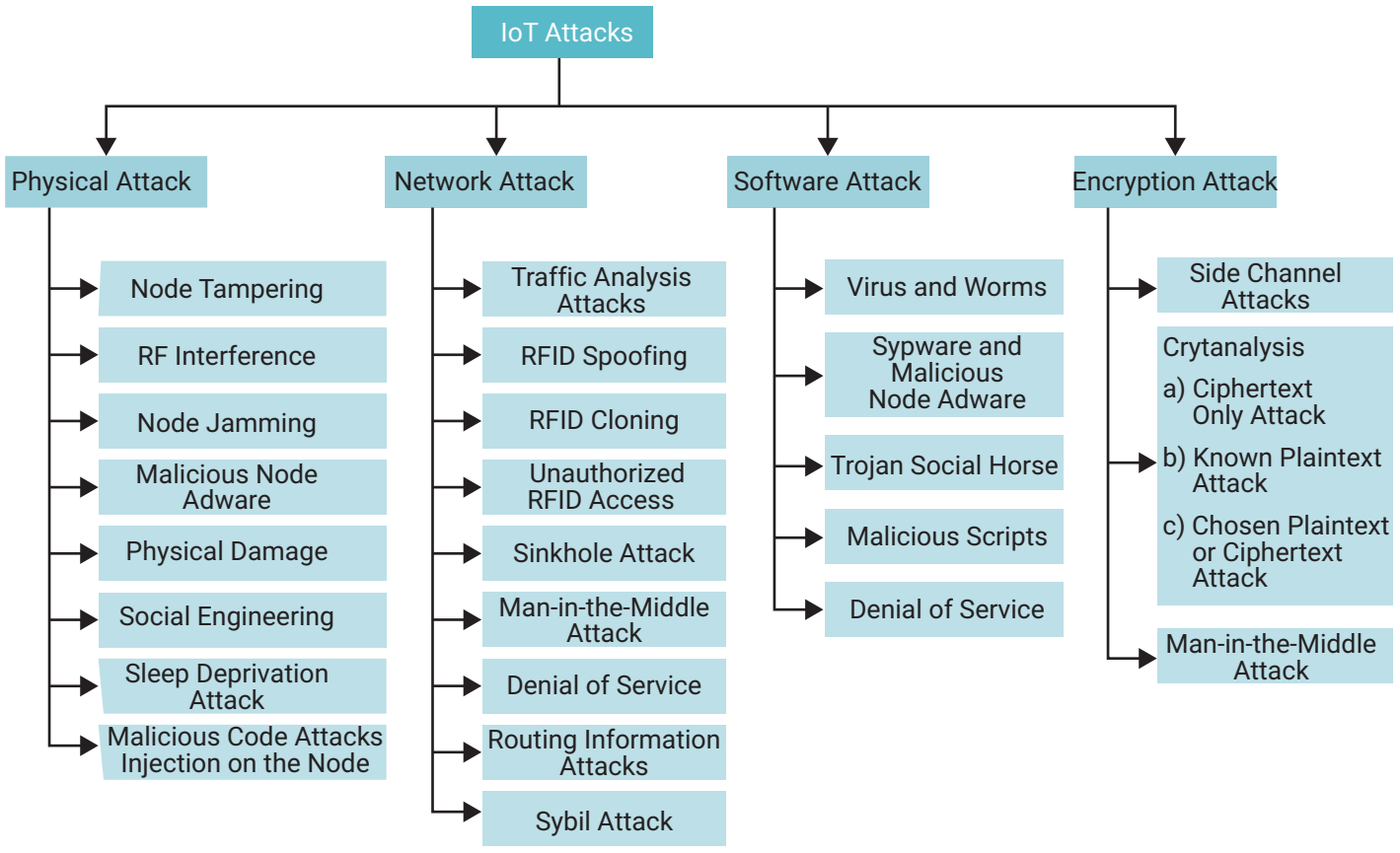
- Data leaks or breaches
- Data sovereignty attacks
- Data loss attacks
- Data authentication attacks
- Attack on availability of data
- Modification of sensitive data

Risk Mitigation Controls to Address Security and Privacy

The impacts, benefits and risk that could affect organizations and potentially individuals need to be thoroughly assessed before initiating the use of IoT devices. Based on detailed a risk assessment, appropriate risk prevention and mitigation controls should be implemented in the IoT ecosystem.

FIGURE 2

IoT Attack Spectrum



> "It is critical to have clarity on the facts and fallacies that exist in peoples' minds around the implementation of the IoT ecosystem in an organization."

There are several safety, privacy, reliability and interoperability controls that are recommended:

- Thorough testing of each individual mechanical, electrical and electronic device should be performed by vendors before integrating them into an IoT ecosystem. Multiple cycles of integration testing should be performed to ensure the reliability of IoT devices before they become an integrated package for use by end users.
- Implementation of robust integration and communication channels to exchange data across disparate and overlapping systems integrated into the IoT ecosystem. Integrating all devices in the IoT ecosystem into a secured virtual network would be advisable to address interoperability challenges.
- Secure protocols should be used to enable data transmission between devices.
- Robust authorization and authentication mechanisms should be implemented.
- Appropriate input/output validation controls should be implemented.
- Strong cryptographic algorithms and cryptographic keys should be used.
- Security configurations of various devices connected in an IoT ecosystem should be reviewed periodically.
- Rollout of security patches for all connected systems should happen in a timely manner.
- Privacy and data retention features of IoT products should be reviewed before procuring them.[14]
- Privacy-by-design principles should be implemented.
- Security standards and frameworks such as the Global System for Mobile Communications (GSMA), International Electrotechnical Commission (IEC) and NIST[15] should be implemented to improve the security posture of IoT devices.
- Review of logs generated by various systems connected in the IoT ecosystem should be reviewed periodically.

Conclusion

Many organizations use IoT systems for workforce transformation. Therefore, it is critical to have clarity on the facts and fallacies that exist in peoples' minds around the implementation of the IoT ecosystem in an organization. Enterprises deploying IoT systems for workforce transformation should keep this in mind and ensure that various teams and management are aware of the high standard of safety, security, reliability, interoperability and privacy controls that will be deployed around their IoT ecosystems. Workplace transformation using IoT technology is a smart way to grow the remote workforce and ensure business continuity under the business models changed due to the COVID-19 pandemic. However, organizations should consider the fact that security, privacy, reliability and interoperability risk factors are inherent and it is necessary to continually focus on implementing appropriate controls to proactively address risk.

Endnotes

1 Internet of Business, "Ransomware Disables Connected Hotel Door System in Austria," *https://internetofbusiness.com/ransomware-disables-hotel-door/*

2 Gregersen, C. R.; "Connected Medical Devices Brought Security Loopholes," *(IN)SECURE Magazine*, 26 April 2021, *https://www.helpnetsecurity.com/2021/04/26/connected-medical-devices-security/*

3 Palmer, D.; "Artificial Intelligence Could Be Used to Hack Connected Cars," *ZDNet*, 20 November 2020, *https://www.zdnet.com/article/artificial-intelligence-could-be-used-to-hack-connected-cars-drones-warn-security-experts/*

4 Chan, R.; "How the Pandemic Will Drive Digital Transformation for Deskless Workers in 2021 and Beyond," *Forbes*, 12 January 2021, *https://www.forbes.com/sites/forbestechcouncil/2021/01/12/how-the-pandemic-will-drive-digital-transformation-for-deskless-workers-in-2021-and-beyond/?sh=2900c0443ede*

5 Nambiar, K.; "Internet of Robotic Things: Robotics With IoT," Analytic Steps, 3 June 2021, *https://www.analyticssteps.com/blogs/internet-robotic-things-robotics-iot*

6 Marr, B.; "Robots and Drones Are Now Used to Fight COVID-19," *Forbes*, 18 March 2020, *https://www.forbes.com/sites/bernardmarr/2020/03/18/how-robots-and-drones-are-helping-to-fight-coronavirus/?sh=3fd408fd2a12*

7 Abu Dhabi Department of Health, "Abu Dhabi to Use Drone Technology for Medical Supply Transfer and Delivery," 22 September 2021, *https://www.doh.gov.ae/en/news/Abu-Dhabi-to-Use-Drone-Technology-for-Medical-Supply-Transfer-and-Delivery*

8 Reuters, "In Indonesia, 'Drone Medics' Help Make No-Contact Deliveries to COVID-19 Patients," *South China Morning Post*, 1 September 2021, *https://www. scmp.com/news/asia/southwest-asia/article/3147198/indonesia-drone-medics-help-make-no-contact-deliveries*

9 Monirujjaman Khan, M.; S. Mehnaz; A. Shaha; M. Nayem; S. Bourouis; "IoT-Based Smart Health Monitoring System for COVID-19 Patients," *Computational Mathematical Methods in Medicine*, 2021, *https://www.hindawi.com/journals/cmmm/2021/8591036/*

10 Covington and Burling, LLP, "Return to Workplace Considerations for Business Using AI and IoT Technologies," 10 June 2020, *https://www.cov.com/-/media/files/corporate/publications/2020/06/return-to-workplace-considerations-for-businesses-using-ai-and-iot-technologies.pdf*

11 International Society of Automation, "New ISA/IEC 62443 Standard Specifies Security Capabilities for Control System Components," *InTech*, September/October, 2018, *https://www.isa.org/intech-home/2018/september-october/departments/new-standard-specifies-security-capabilities-for-c*

12 Khokale, S.; "Role of IoT Consortiums and Standards in Resolving IoT Interoperability Issues," eInfochips, 11 December 2019, *https://www.einfochips.com/blog/role-of-iot-consortiums-and-standards-in-solving-interoperability-challenges-of-iot-ecosystems/*

13 Cyrus, C.; "IoT Cyberattacks Escalate in 2021, According to Kaspersky," *IoT World Today*, 17 September 2021, *https://www.iotworldtoday.com/2021/09/17/iot-cyberattacks-escalate-in-2021-according-to-kaspersky/*

14 Agarwal, A.; "Protecting Your Privacy in the IoT Era," *Attify Blog*, 1 November 2018, *https://blog.attify.com/protecting-your-privacy-in-the-iot-era/*

15 Senki, "IoT Security Standards and Frameworks," *https://www.senki.org/operators-security-toolkit/ºsp-security/iot-security-standards/*