Cyber Threat Intelligence Report

Navigating the Cybersecurity Maze in IoT

Cybersecurity Division
Compiled by Liam Ryan

Date: 20 March 2024

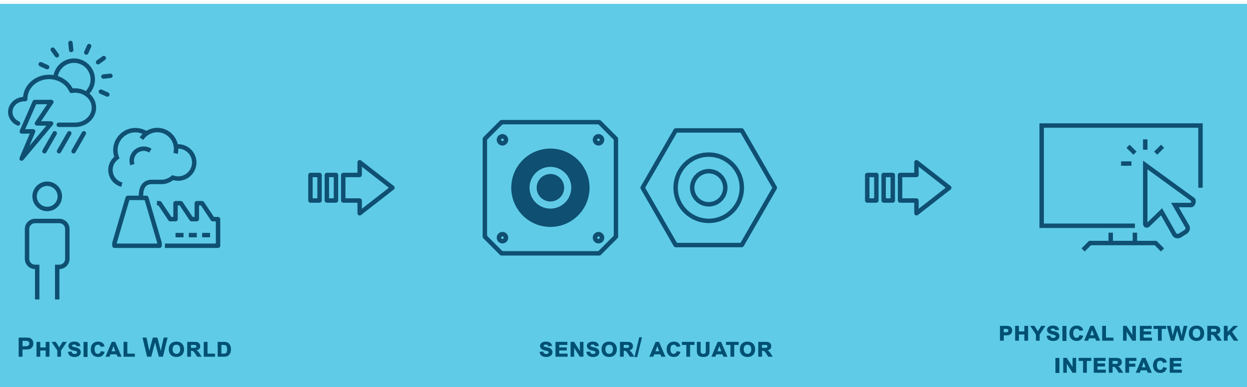
Executive Summary

The rapid proliferation of the Internet of Things [IoT] has transformed how organizations operate and improved consumer quality of life. For these reasons, IoT is spearheading the fourth industrial revolution; however, IoT is not without its cybersecurity challenges. The IoT has a dismal cybersecurity track record and is a prominent target or vector for threat actors. Understanding the risks of IoT is paramount for business leaders seeking to fortify their organizations against loss. This paper aims to help those in these organizations seeking to understand the IoT and the risk it presents.

IoT ecosystems encompass many networked sensors and actuators, resulting in an expansive attack surface. These products and systems can be found in everything from toys to nuclear centrifuges. This ubiquity means that the impacts of cyberattacks are diverse and more likely. The risks themselves are proving to be less understood than those associated with traditional information technology systems. This uncertainty is attributed to the diversity of modern networks, resulting in increased complexity. Other cited core issues are a lack of awareness, naïve cybersecurity practices, resource constraints, and absent industry standardization.

Business leaders must be proactive risk practitioners if they are to remain ahead of the curve. This paper provides readers with best practices for IoT cybersecurity as outlined by industry leaders. The application of these suggestions can minimize the risk of IoT while maximizing its benefit. So long as we remain vigilant and proactive risk practitioners, IoT—and the risk it poses—can be managed.

What is an IoT Device?



An IoT device is anything that contains at least one sensor or actuator for interacting with the physical world, and at least one physical network interface (*Fagan et al., 2020*).

Introduction

In today's interconnected world, where even our toasters can communicate with our smartphones, the concept of cybersecurity has transcended beyond just safeguarding traditional IT systems. Welcome to the era of the Internet of Things [IoT], where the limit is truly our imagination as anything can be connected to the internet. However, lurking amidst the convenience are threats to not only our devices, but also our lives. Imagine waking up to your thermostat being hacked, your doors being unlocked remotely, or a power loss caused by a cyber-attack. As we delve deeper into the realm of IoT, the necessity for robust cyber security becomes increasingly apparent. Organizations and individuals alike are wondering how they can manage these modern risks. To begin to answer these questions, we start at the beginning of this paradigm shift.

At the inception of the internet, digital systems communicating over networks did so about immaterial ideas and information. Something that Kevin Ashton of the Massachusetts Institute of Technology [MIT] at the time took issue with. He saw ideas and information as being less important than the physical things that populate our everyday lives. In 1999, this resulted in him coining the term Internet of Things [IoT]. According to Ashton, the Internet of Things succinctly conveyed his vision of a world where digital systems communicated not just about the immaterial, but also the material *things* around us (*Ashton, 2009*).

Today, the IoT is a buzzword whose definition lacks industry consensus (*Megas, Piccarrta, & O'Rourke, 2017*). It is often erroneously conflated with several other terms such as as Cyber-Physical Systems [CPS] (*Lesch et al., 2023*). According to Lesch et al., IoT commonly refers to a "global network of physical and virtual things." This definition aligns with Ashton's conceptualization and will serve as a foundation for discussing IoT in this report, along with the above minimum requirements of an IoT device--listed in the executive summary.

Positing the above, the IoT presents a rapidly advancing and radical shift that is pervading across all industries. The ubiquity of IoT in industry is compounded by its commercial availability, resulting in a world where digital interconnectivity extends beyond individuals to include the *things* and the environment that they both exist in. Historically, in technological paradigm shifts such as this, cybersecurity has been an afterthought, applied retrospectively. And so, despite its rapid onset and continuous advancement, it is evident from recent cybersecurity incidents that the IoT is still in its infancy and experiencing growing pains. This is especially alarming when one considers how ingrained these systems are into every aspect of our lives, as we transition to IoT reliant smart societies.

The cybersecurity challenges posed by the IoT are as inherent as its benefits, and whether one accepts this risk is normally dependent upon their tolerance for risk. However, IoT is at the forefront of the latest industrial revolution, affecting most individuals and organizations, regardless of their risk tolerance. This paper aims to return some of this control to the reader, by providing them with the information required to make informed decisions about IoT. The remainder of this paper is divided into sections which build upon the foundation established above.

The Scope of the Internet of Things

As discussed in the introduction, IoT refers to the global interconnectivity of things. This is a very general statement and can be difficult to work with as is. Thus, to further clarify the IoT, this section establishes its scope based on four factors: the IoT market, IoT interconnectivity, industrial IoT, and commercial IoT. For the sake of brevity, these compartmentalization's are not comprehensive, and any one of them could have entire papers dedicated to them—in-fact, they do.

The IoT Market

While specific figures vary across sources, the general sentiment is consistent: the IoT market is growing at neck breaking speeds.

According to Vailshery (2023a), the global market projection for IoT in 2023 was $293 billion (USD), with a market forecast of $621 billion by 2030. Recorded rates seem to be exceeding these predictions with a market evaluation of $544 billion (USD) in 2022, and a forecast of $3,352,97 billion by 2030 (Fortune Business Insights, 2023). The predicted Compound Annual Growth Rate (CAGR) of IoT is 26.1 per cent which supports continued—albeit riskier—investments and indicates significant continued growth. Other sources indicate similar growth but conclude with various specifics such as Manyika et al. (2015) who anticipates an $11 trillion global market evaluation as early as 2025.

IoT is an ever growing market with the predicted CAGR of IoT being: **26.1%**

Accelerating IoT Interconnectivity

As with the market analyses, the specifics surrounding interconnectivity statistics vary across sources, but still the sentiment is consistent: interconnectivity is an accelerating trend compounded by the advent of IoT.

Cisco projected that the number of connected devices for 2023 was 29.3 billion, a 63 per cent increase from 2018. Of these, over 50 per cent are predicted to be Machine-to-Machine [M2M] networked (Cisco, 2022). Other estimates speculated there would be 15 billion IoT devices in 2023 and that by 2030, commercial devices *alone* would exceed this number (Vailshery, 2023b).

Did you know..

M2M refers to the direct communication of data and information between devices without interference by humans. It enables networks of devices to relay and respond to data autonomously.

A statistic that is equally important to IoT connected device counts over time, is device penetration values. The former value—device counts—represents the rate of interconnectivity when assessed with respect to another quantity, the latter—penetration values—offers ratio-based insights between two quantities. Device penetration is represented as the ratio of devices that are currently IoT versus those that are not but could be. Some early estimates pegged the number around 3 per cent, which would indicate room for significant growth (Kimani, Oduol, & Langat, 2019). Other sources speculate that IoT device penetration surpassed 50 per cent in 2020 (Lueth, 2021).

Industrial Internet of Things [IIoT]

Across the board, industries are reaping the rewards of IoT. The data driven advancements IoT enables are significant contributing factors in reaching sustainable development goals (Bachmann, 2022).

Industry 4.0 is a term used to refer to the fourth industrial revolution, a revolution driven by the envelopment of society by digital *things.* This envelopment is progressing exponentially and has left no industry untouched (*Ghobakhloo, 2020*; *Stouffer et al., 2023*).

Devices categorized as Operational Technology [OT], interact directly with their physical environment, or manage devices that do (*Stouffer et al., 2023*). This empowers providers with abilities such as the real time monitoring of complex physical systems, physical process automation, predictive analysis, hazard and anomaly detection (*Moradbeikie et al., 2020*), and much more.

In the energy sector, providers are pressured to meet growing global energy demands while simultaneously contributing to sustainable outcomes (*Hossein Motlagh et al., 2020*; *Kimani, Oduol, & Langat, 2019*; *United Nations [UN], 2023*). IoT ecosystems in energy enable the real-time monitoring of the energy supply chain, leading to technological advancements that can help meet these demands. One such example is Advanced Metering Infrastructure [AMI], which provides predictive forecasting and enhanced outage management (Kimani, Oduol, & Langat, 2019). And according to Hossein Motlagh et al. (*2020*) the efficiency improvements from OT additionally result in cost reductions for both consumers and providers.

Did you know..

In its industrious form, IoT is called OT and can take many different shapes—e.g., industrial control systems, business automation systems, physical access control systems, etc.

Just like in energy, the agricultural sector is met with sustainability issues driven by increasing populations and shifting consumption patterns. For example, irrigation-based agriculture uses approximately 70 per cent of all freshwater withdrawals, much of which is wasted (*World Bank, 2022*; *UNESCO, 2022*; *Koncagül, Tran, Connor, 2021*, *World Financial Review, 2021*). Moreover, water usage for irrigation-based agriculture has been increasing at an unsustainable rate, resulting in water shortage predictions (*Koncagül, Tran, Connor, 2021*). Data driven solutions made possible by OT have led to advancements like smart irrigation systems that improve yields and reduce waste (*Obaideen, et al., 2022*; *Ahmed & Khan, 2023*).

Consumer Internet of Things [CIoT]

The consumer space of IoT includes a myriad of smart devices such as TVs, fridges, lightbulbs, homes, cars, security systems, thermostats, cameras, door locks, toys, and wearables. The difference between commercial and industrial IoT systems are faint: when broken down, both include sensors and/or actuators, and a network connection. The difference usually resides in the target audience and scale of the system. This is exemplified by the difference between a heating, ventilation, and air conditioning [HVAC] system for a data centre and a smart thermostat in a smart home. Both smart systems regulate the environment they reside in, but on massively different scales.

Critical Infrastructure Sectors

- Transportation
- Finance
- Energy & Utilities
- Food
- Health
- Water
- Information & Communication Technology
- Government
- Manufacturing
- Safety

Source: (*CCCS, 2022*)

Exploring the Landscape of IoT and Cybersecurity

Recent incidents and industry leaders all indicate that robust cybersecurity is a significant hurdle for IoT solutions. Attacks on these systems are becoming more widespread and impactful, while simultaneously becoming less understood.

In cybersecurity, the battle against threat actors is a never-ending game of cat and mouse with the odds stacked in favour of the attackers. This bias is inherent in the game and likely to persist into the foreseeable future. In an attacker-defender scenario, the defender needs to identify and treat all vulnerabilities, and do so under the pressure of due dates. In contrast, the attacker has infinite time to find a single oversight which can compromise the system. With IoT growing exponentially, the attack surface is becoming unmanageable for the modern defender and often trivial to exploit for the attacker. Proverbially, we are overdriving our headlights.

However, recurring incidents, recent reports, and surveys are illuminating the troubles of cybersecurity in the age of IoT.

In 2016, the U.S. Department of Homeland Security [DHS] stated that "the reality is that security is not keeping up with the pace of innovation...[and IoT's] adoption will impact virtually all sectors of our society."

In 2017, the National Institute of Standards and Technologies [NIST] stated that IoT ecosystems pose risks that "extend beyond traditional data security" (*Megas, Piccarreta, & O'Rourke, 2017*).

In 2021, the Cybersecurity & Infrastructure Security Agency [CISA] stated that the scale of interconnectedness resulting from IoT "increases the consequences of known risks and creates new ones."

In 2022, the Canadian Centre for Cybersecurity [CCCS] identified IoT as a threat target which poses significant risks to CI.

A 2019 survey of 700 cybersecurity professionals across industries indicated that:

80% of organizations experienced cyberattacks on IoT devices

90% of which led to negative impacts (*Irdeto, 2019*).

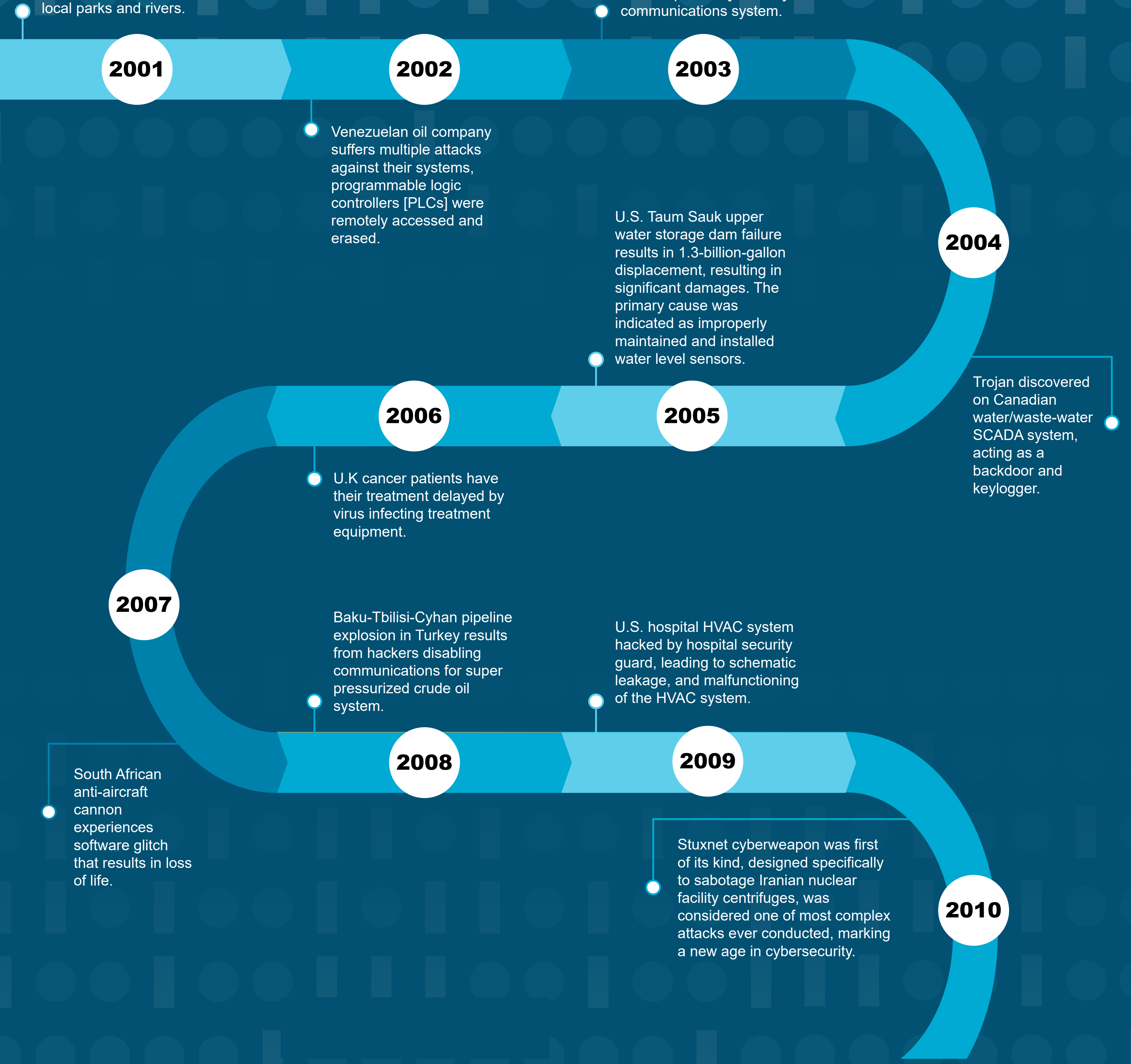
Additionally, the volume of IoT cyberattacks saw:

300% increase in 2019 (*Ghobakhloo, 2020*).

These concerns raised by industry leaders are not hypothetical, they are driven by historical evidence of IoT's dismal track record (*Cohen, 2021*; *Kovacs, 2023*; *Kuehn, 2018*; *Miller et al., 2021*; *RISI, 2015*). For an abridged history of some of these events, see the timeline on the following pages.

Up to this point, there has been a focus on the identification of one exceptionally large problem with IoT, specifically that robust cybersecurity is a significant challenge. However, this paper has offered little insight into the crux of the issue. Going forward, now that a problem has been identified, the remaining sections will be dedicated to uncovering the root cause and solutions. As was discussed in the introduction, IoT itself is difficult to define, and defining the root problem of cybersecurity in IoT mirrors this trend.

An Abridged History of IoT Incidents



2001 – Maroochy Shire insider attack on Industrial Control Systems [ICS] at sewage treatment plant results in 265,000 gallons (about 1003133.65 L) of untreated sewage being dumped into local parks and rivers.

2002 – Venezuelan oil company suffers multiple attacks against their systems, programmable logic controllers [PLCs] were remotely accessed and erased.

2003 – Telecommunication workers in Canada accidentally shut down critical circuit for supervisory control and data acquisition [SCADA] communications system.

2004 – Trojan discovered on Canadian water/waste-water SCADA system, acting as a backdoor and keylogger.

2005 – U.S. Taum Sauk upper water storage dam failure results in 1.3-billion-gallon displacement, resulting in significant damages. The primary cause was indicated as improperly maintained and installed water level sensors.

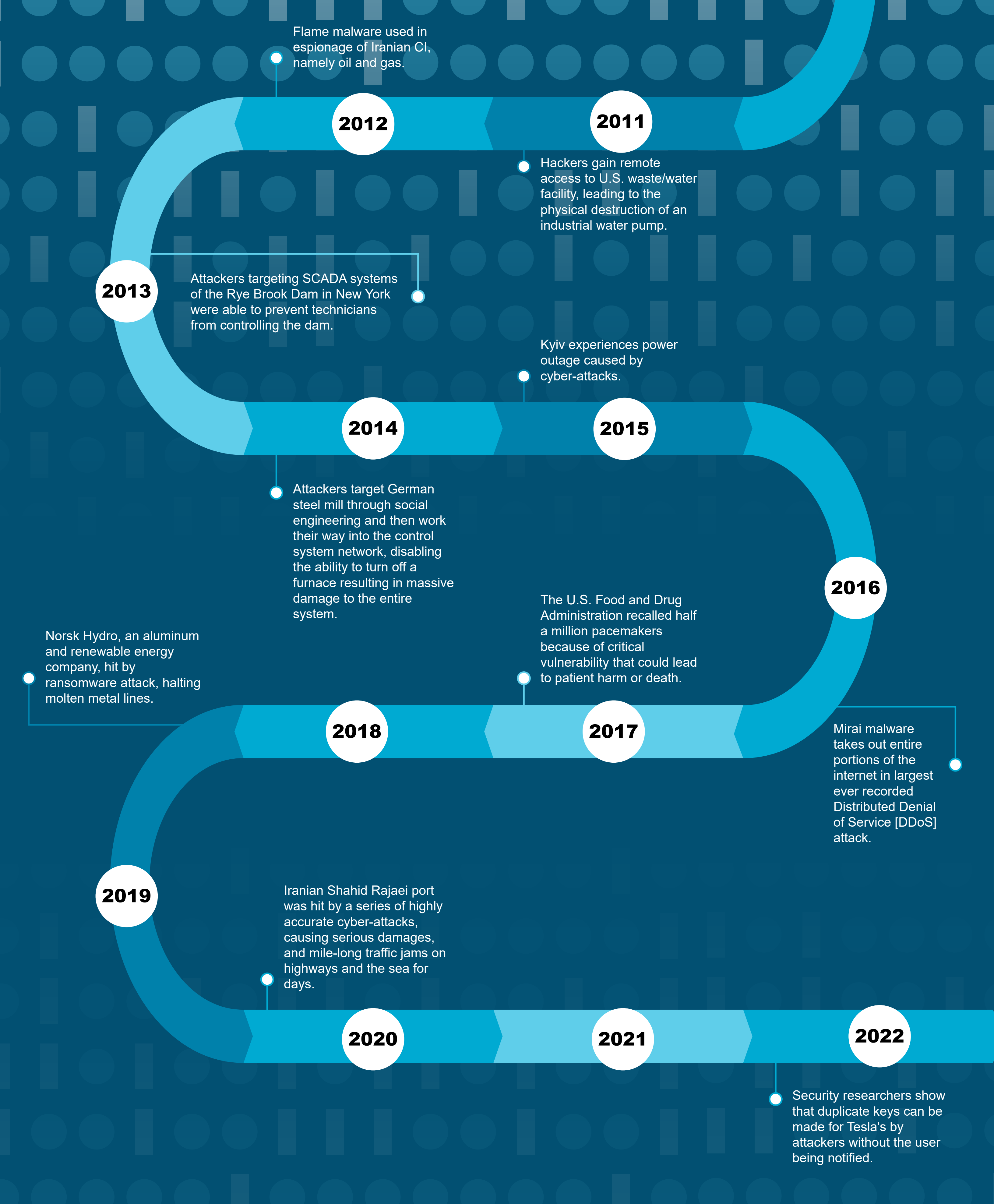
2006 – U.K cancer patients have their treatment delayed by virus infecting treatment equipment.

2007 – South African anti-aircraft cannon experiences software glitch that results in loss of life.

2008 – Baku-Tbilisi-Cyhan pipeline explosion in Turkey results from hackers disabling communications for super pressurized crude oil system.

2009 – U.S. hospital HVAC system hacked by hospital security guard, leading to schematic leakage, and malfunctioning of the HVAC system.

2010 – Stuxnet cyberweapon was first of its kind, designed specifically to sabotage Iranian nuclear facility centrifuges, was considered one of most complex attacks ever conducted, marking a new age in cybersecurity.



2011

Hackers gain remote access to U.S. waste/water facility, leading to the physical destruction of an industrial water pump.

2012

Flame malware used in espionage of Iranian CI, namely oil and gas.

2013

Attackers targeting SCADA systems of the Rye Brook Dam in New York were able to prevent technicians from controlling the dam.

2014

Attackers target German steel mill through social engineering and then work their way into the control system network, disabling the ability to turn off a furnace resulting in massive damage to the entire system.

2015

Kyiv experiences power outage caused by cyber-attacks.

2016

Mirai malware takes out entire portions of the internet in largest ever recorded Distributed Denial of Service [DDoS] attack.

2017

The U.S. Food and Drug Administration recalled half a million pacemakers because of critical vulnerability that could lead to patient harm or death.

2018

Norsk Hydro, an aluminum and renewable energy company, hit by ransomware attack, halting molten metal lines.

2019

2020

Iranian Shahid Rajaei port was hit by a series of highly accurate cyber-attacks, causing serious damages, and mile-long traffic jams on highways and the sea for days.

2021

2022

Security researchers show that duplicate keys can be made for Tesla's by attackers without the user being notified.

The Dark Side of IoT: Cybersecurity Concerns

It is unclear what is at the centre of the IoT cybersecurity maze. But, reccurring incidents and echoing concerns are beginning to highlight the way. So, although the crux of the problem is still a mystery, the concerns of industry leaders are illuminating the path forward.

Cybersecurity in traditional IT environments is already complex, and augmenting these systems with OT and IoT further complicates the issue. To elaborate, IoT is penetrating *everything* that it can. Because of this, networks are more diverse, resulting in an upward trend in complexity (*Bachmann et al., 2022*; *Ghobakhloo, 2020*; *Kandasamy et al., 2020*, Lee, 2020; *Lu, 2023*; *Potter & Oloyede, 2023*; *Tariq et al., 2023*). However, a perfect correlation between complexity and vulnerability does not exist. Therefore, to understand why robust cybersecurity poses such a problem for IoT, it is necessary to delve deeper into recent incidents and current practices.

Naïve Cybersecurity Practices

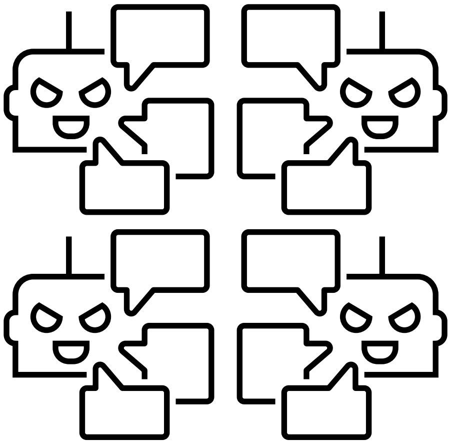
It is common for IoT devices to be built without cybersecurity in mind, resulting in systems which are trivial to exploit.

Naïve cybersecurity practices by manufacturers, organizations, and various end-users, are a recurring theme across IoT (*CCCS, 2022*; *Kandasamy et al., 2020*; *Tariq et al., 2023*). Many IoT vulnerabilities could be mitigated through cybersecurity best practices; however, devices often lack even the most basic security measures (*DHS, 2016*; *Ghobakhloo, 2020*). A prime illustration is the case of the Mirai malware, which made headlines in 2016 as the most devastating DDoS attack ever recorded.

Mirai Botnet

Since 2016, when the Mirai source code became public, several case studies have been conducted on the malware. This strain of malware resulted in the largest DDoS attack ever recorded, knocking out huge portions of the internet. An attack of this scale was so unheard of that Cisco security analysts developed a new term for it: Destruction of Service [DeOS] (*Brass et al., 2018*).

The way it worked was simple, Mirai would begin by enumerating the web for publicly accessible IoT devices, such as IP-Cameras. After finding a device, it would probe and analyze it for information which would indicate the type of system. Upon obtaining this information, it would exploit default or weak credentials associated with that system to control the device. At this point, the corrupted device could be used to discover even more devices and the process would repeat. After building itself up, this botnet was then used to target Dyn—a popular Domain Name System [DNS] provider—which led to the 2016 incident. The crux of the issue here, is that Mirai was successful because it relied on the assumption that these devices employed naïve cybersecurity practices, namely poor password management. Regrettably, this is not an exception; poor cybersecurity in IoT is often the status quo (*DHS, 2016*; *Saleem et al., 2018*; *Tariq et al., 2023*).



Lack of Standardization

Attempting to standardize IoT is like trying to hit a moving target. The field is growing quickly, and new devices emerge each day. A universal approach to standards is impractical, resulting in a fragmented industry.

A lack of comprehensive standardization is one of the foremost issues facing the IoT according to several sources (*Ahmed & Khan, 2023*; *Aisenberg et al., n.d*.; *Brass et al., 2018*; *CISA, 2019*; *Potter & Oloyede, 2023*; *Saleem et al., 2018*; *Tariq et al., 2023*). However, it is important to note that this header is slightly misleading as several standards, frameworks, and guidelines do exist and will be discussed in the following section. Furthermore, as mentioned in the previous section, current best practices would suffice in bolstering IoT against most vulnerabilities. Across sources, the observed lack in standardization faced by IoT is explained as a threefold problem:

1. There is little incentive for adherence to standards by manufacturers, so, despite the existence of standards, they are non-binding and manufacturers therefore do not implement them (*Brass et al., 2018*; *Megas, Piccarreta, & O'Rourke, 2017*; *Potter & Oloyede, 2023*).
2. Manufacturers often do not create the entire device, meaning they must rely on third parties with poor or ambiguous cyber-hygiene (*CCCS, 2022*; *Megas, Piccarreta, & O'Rourke, 2017*; *Megas, 2021*; *Potter & Oloyede, 2023*).
3. Due to the heterogeneity of devices, developing a "one size fits all" approach is an intractable problem (*CISA, 2019*; *DHS, 2016*; *Megas, 2021*; Potter & Oloyede, 2023; *Tariq et al., 2023*). Although, this does not excuse the absence of basic cybersecurity.

When it comes to IoT, standards are not firmly tethered to security regulations. This has resulted in a divergence of practice amongst manufacturers, and disagreements about what the de facto cybersecurity approach is. This fragmentation has contributed significantly to the continuous proliferation of vulnerable devices into the market, an issue that will still pose risk long after the matter has been resolved.

Awareness

An unaware consumer audience is being supplied with IoT devices that are not secure by design; expanding the attack surface and increasing the risk.

Commercial audiences are not aware of the privacy and security risks posed by many smart devices, sometimes they are not even aware that the things they purchase are smart (*Tariq et al., 2023*; *Aisenberg et al., n.d.*). This has led to an absence of consumer demand for privacy and security (*Megas, Piccarreta, & O'Rourke, 2017*), contributing to the lack of incentivization for manufacturers outlined above.

Resource Constraints

IoT devices are highly susceptible to resource draining attacks that could result in a loss of system availability. This is driven by resource constraints which also contribute to the production of IoT devices with insecure encryption schemes.

The embedded systems used in smart devices are often significantly smaller than those used in prototypical devices (e.g., phones, personal computers, servers, etc.). Logically, it follows that these size restrictions result in reduced computational power, memory, and battery. These constraints make IoT devices more susceptible to resource draining attacks, meaning that it is easier for attackers to overwhelm these systems (*Ahmed & Khan, 2023*; *Lu, 2023*; *Potter & Oloyede, 2023*; *Tariq et al., 2023*). The impacts of such an attack are situationally dependent, but as outlined in the scope, our reliance on IoT in CI means a loss of availability poses significant safety risks. Importantly, the same goes for IoT used in the consumer space, as safety systems are included under its umbrella.

The issue of resource constraints has also resulted in the production of several already-in-market devices that lack secure cryptographic schemes (*Ahmed & Khan, 2023*; *Lueth, 2021*; *Mosenia & Jha, 2016*; *Potter & Oloyede, 2023*). Critically, this does not mean that because of limited resources, these devices cannot support these functions. Rather, because device resources are constrained, manufacturers make cost informed decisions that often negate cybersecurity (*Mosenia & Jha, 2016*).

Novel Risk Environment

The IoT presents risks that are not fully understood. This makes the job of frontline cybersecurity professionals more difficult and the tools they use less effective.

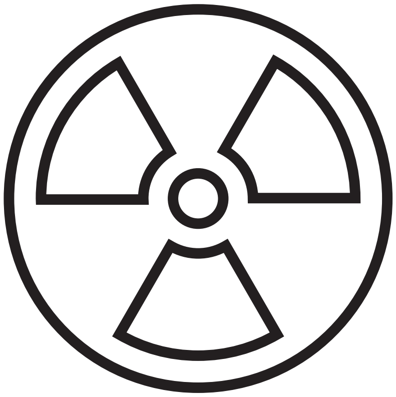
The cybersecurity risk landscape has always been dynamic, in this sense a novel risk environment is not so unfamiliar. However, IoT has proven to be especially tricky, as it comes with threats and vulnerabilities that do not easily mesh with existing risk frameworks (*Kandasamy et al., 2020*; *Lee, 2020*). The privacy risks posed to end users of the IoT are significant and are not well understood (*Ahmed & Khan, 2023*; *CISA, 2019*; *Kandasamy et al., 2020*; *Lu, 2023*; *Megas, Piccarreta, & O'Rourke, 2017*; *Mosenia & Jha, 2016*; *Saleem et al., 2018*; *Tariq et al., 2023*). Physical risks are also taking on a new form due to IoT, as cyberattacks are more likely to result in immediate physical impacts (*CISA, 2019*; *Kandasamy et al., 2020*; *Tariq et al., 2023*). Conversely, IoT devices are more likely to be subject to physical threats due to their ubiquity and physical presence. Organizations can have hundreds to thousands of sensors or actuators, something modern security solutions can struggle with (*Megas, Piccarreta, & O'Rourke, 2017*). Further complicating these concerns, is the rise in well-funded and sophisticated attacks such as the Stuxnet malware.

All these concerns are deeply entangled, often compounding one another. This makes them difficult to navigate, as derived solutions may be misdirected. Further, this list is not exhaustive and presents only one level of analysis.

Stuxnet

The Stuxnet worm targeted centrifuges used in the uranium enrichment process at the Natanz nuclear plant in Iran. At the time, this worm was considered one of the most sophisticated pieces of *malware* ever discovered, featuring four *zero-days*, and marking a new age in cyberwarfare. Its purpose was to sabotage the Iranian nuclear program, by manipulating precise industrial control systems into misbehaving.

Stuxnet worked by targeting SCADA systems. For Stuxnet, the vector to these target systems was through computers running the Windows operating system. Upon discovering vulnerable hosts, it would infect them and use valid, but stolen *driver certificates* to install its *rootkit*. Using these certificates gave the rootkit credence to find and modify files specific to the industrial control systems it was targeting. By infecting these files, Stuxnet could manipulate the integrity of the information that logical controllers were operating on, directly affecting physical processes. The centrifuges used were outdated and sensitive to abrupt changes in speed, which Stuxnet's developers were seemingly aware of as this is what they manipulated, resulting in irreparable damage (*Baezner & Robin, 2017*).



Illuminating the Path: Best Practices for IoT Cybersecurity

Remedying the cybersecurity deficit across the IoT industry is a slow, arduous, and uncertain process. While this work is being done, the risk remains, and the attack surface continues to expand. Organizations must be proactive if they are going to shield themselves from the risk posed by IoT/OT.

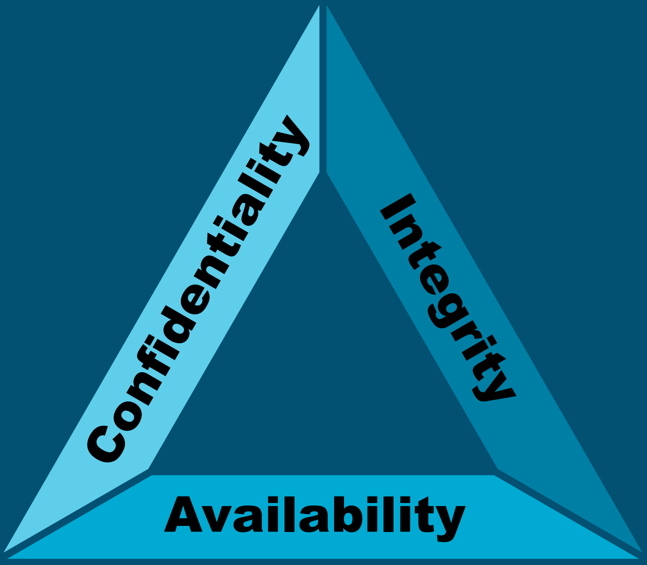
Several initiatives driven by regulatory agencies, governments, and industry leaders that would incentivize manufacturers adherence to standards are underway—e.g., procurement obligations and certification schemes (*Brass et al., 2018*; *Potter & Oloyede, 2023*). However, these processes are slow, arduous, and out of the hands of the average end-user. Thus, while this work is being developed the attack surface continues to grow and the risk remains. If organizations hope to be secure in the age of IoT, they must be proactive risk practitioners. This means adopting common best practices and amending to them IoT/OT specific considerations.

Cybersecurity Recommendations for IoT/OT

Modern risk management and cybersecurity is done through the focal point of the CIA triad; the protection of asset confidentiality, integrity, and availability. Losses in anyone of these areas could result in negative impacts that impede an organization's ability to reach its goals.

Risk Management

Organizations are advised to adopt a risk management framework; such practices are essential for those seeking to secure themselves against evolving threats. A comprehensive risk management strategy allows for the identification, prioritization, and economical treatment of risks. These frameworks bring much needed organization to an increasingly complex risk landscape and are adaptable to IoT/OT solutions (Aisenberg et al., n.d.; Stouffer et al., 2023).



Asset Management

Maintaining an accurate inventory of all assets and their configurations throughout their lifecycle—from procurement to disposal—is an essential practice. Risks begin with assets; if they are not accurately identified, then the subsequent management of risks becomes intractable. This is especially the case for IoT/OT assets as they are often copious compared to traditional IT systems (Fagan et al., 2020).

Vulnerability Management & Security Updates

No system stays secure forever, they must change and adapt to retain this classification. Even systems that are secured by design will eventually succumb to vulnerabilities. Therefore, vulnerabilities must be monitored, prioritized, and mitigated (DHS, 2016; Fagan et al., 2020). It is out of the control of end-users to fix these issues; they must instead rely on manufacturers to issue security patches and then install the patches as soon as practicable. Organizations that do not keep their systems patched are prominent targets for threat actors.

Governance & Awareness

The development of policy instruments, training, and educational material that applies specifically to IoT/OT is essential. IoT/OT oriented documents including standards, policies, and procedures will align these technologies, and their implementation with organizational values. All personnel who interact with these systems should receive mandatory cybersecurity training specific to OT system security and general IT cybersecurity training (Aisenberg et al., n.d.).

Solution Acquisition Lifecycle

Many of the problems described originate with manufacturers of IoT products and systems. To prevent the introduction of risky devices into an organization's ecosystem, it is critical to exercise due diligence during the acquisition of IoT products. The development of minimum-security baselines is essential to this process (Aisenberg et al., n.d.; Fagan et al., 2020). The solution acquisition life cycle contains an assessment of the need, acquisition planning and requirement development, solicitation, development and contract award, and production, deployment, and support. Risks must be continually monitored and assessed throughout this lifecycle (Aisenberg et al., n.d.).

Resource Constraints, Legacy Systems, & Integration

It is common for IoT/OT technologies and products to not contain prototypical IT security capabilities. This is particularly true for legacy OT systems. In the past OT networks were physically isolated from corporate networks, but now it is common to see them merged. It is important that organizations consider the impact of legacy systems on their environment; they may be difficult or impossible to securely integrate with (Aisenberg et al., n.d.; Stouffer et al., 2023). Organizational risk tolerance can be quickly exceeded by these systems.

Network Segmentation

Organizations should adopt a layered topology for their IoT/OT systems, where the most critical operations are performed in the most secure and reliable layer. The logical segmentation of devices and systems that do not need to communicate is recommended. Organizations should identify and implement physical segmentation as required. When integrating IoT/OT with traditional corporate networks, a logical separation should be created between the two (Stouffer et al., 2023).

Underpin Safety & Physical Security

Cybersecurity risk analysis is underpinned by the protection of asset confidentiality, integrity, and availability. Due to the frequent interaction and manipulation of the physical environment by IoT/OT, losses in any of these areas may manifest as physical impacts, which could lead to death or injury. Therefore, safety is an overarching priority for these systems, and should be emphasized during the assessment of risks (Stouffer et al., 2023).

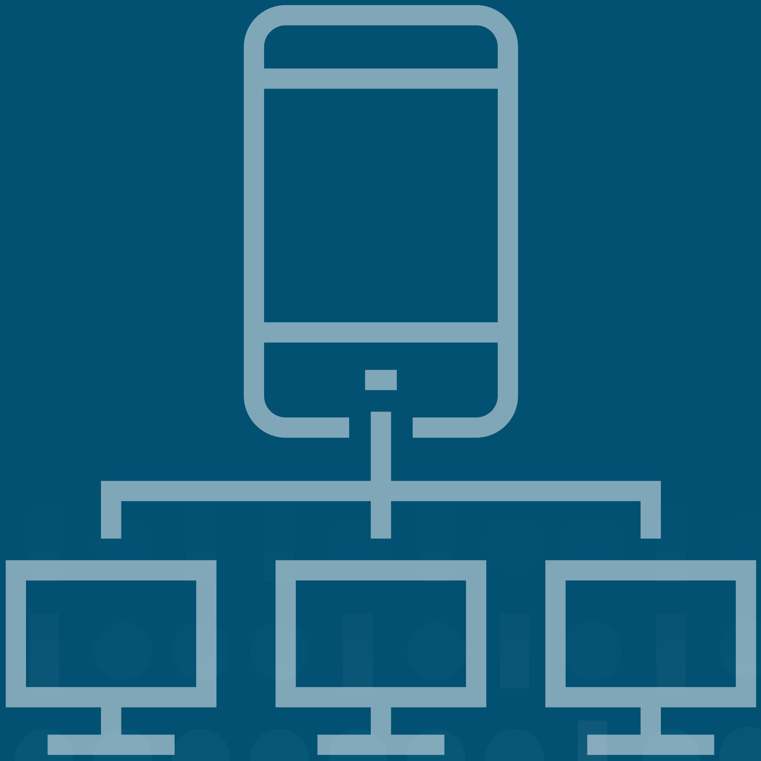
Measures must be taken to protect IoT/OT systems from unauthorized physical access; these systems are commonly more accessible than traditional IT systems. In certain situations, little can be done to prevent physical access, as it may be central to its operation; in these cases, a defense in depth strategy is emphasized. Physically exposed systems are also at increased risk of damage from adverse conditions. These systems should be designed to endure physical stress and fail gracefully (Stouffer et al., 2023).

Emphasize Availability

In IoT/OT, availability is often emphasized as system processes are continuous, and a system outage could result in cascading impacts. Before deployment, testing should be proportional to the system's criticality; high criticality systems must undergo exhaustive tests. In some circumstances, OT systems cannot be stopped once turned on as their function is more important than their data. In these situations, deploying redundant systems is recommended and the level of redundancy will again depend on the criticality of the system (Stouffer et al., 2023). Incidents are bound to occur in any organization, so planning and having processes in place are necessary to ensure continuous operations.

Conclusions

IoT is prolific in its industry wide adoption, but it is experiencing significant challenges with robust cybersecurity. This is a concern echoed by many in the industry and reflected by repetitive cybersecurity incidents. Due to the sheer diversity and complexity of these networked systems, the industry is divided in its current cybersecurity approach. These issues will take years to solve and are out of the control of the average user, but business leaders and end-users are not hopeless or alone in their endeavour to secure themselves. Reputable organizations have produced guides for managing IoT/OT risk and most current best practices are applicable in securing these systems. A defense in depth strategy and proactive approach to cybersecurity will help any organization remain ahead of the curve, minimizing the risks of this new paradigm shift, while maximizing its benefits.



References & Further Reading

Ahmed, S., & Khan, M. (2023). Securing the Internet of Things (IoT): A Comprehensive Study on the Intersection of Cybersecurity, Privacy, and Connectivity in the IoT Ecosystem. *AI, IoT and the Fourth Industrial Revolution Review*, 13(9), 1–17. https://scicadence.com/index.php/AI-IoT-REVIEW/article/view/13

Aisenberg, M., Allor, P., Bergman, M., Nadine Burris, David Durcsak, Funk, K., Goertzel, K., Grant, P., Gyurek, R., Hall, T., Hill, K., Humble, J., Jackson, H., Martin, R., Monette, E., Rossell, M., Sage, O., Sheehy, R., Shein, R., Smith, A., Tamarkin, E., Tousley, S., Walker, P., & Wenger, E. (n.d.). Internet of things acquisition guidance. *CISA*. https://www.cisa.gov/sites/default/files/publications/20_0204_cisa_sed_internet_of_things_acquisition_guidance_final_508.pdf

Andrade, R. O., Yoo, S. G., Tello-Oquendo, L., & Ortiz-Garces, I. (2020). A comprehensive study of the IOT Cybersecurity in smart cities. *IEEE Access*, *8*, 228922–228941. https://doi.org/10.1109/access.2020.3046442

Ashton, K. (2009) That "Internet of Things" thing. *RFiD Journal*, 22, 97-114. https://www.rfidjournal.com/

Bachmann, N., Tripathi, S., Brunner, M., & Jodlbauer, H. (2022). The contribution of data-driven technologies in achieving the Sustainable Development Goals. *Sustainability*, *14*(5), 2497. https://doi.org/10.3390/su14052497

Baezner, M., & Robin, P. (n.d.). Stuxnet. *CSS Cyberdefense Hotspot Analyses*, 4. https://doi.org/10.3929/ethz-b-000200661

Brass, I., Tanczer, L., Carr, M., Elsden, M., & Blackstock, J. (2018). Standardising a moving target: The development and evolution of IOT security standards. *Living in the Internet of Things: Cybersecurity of the IoT - 2018*. https://doi.org/10.1049/cp.2018.0024

Canadian Center for Cybersecurity. (2022, April). Security considerations for critical infrastructure. *Government of Canada*. https://www.cyber.gc.ca/en/guidance/security-considerations-critical-infrastructure-itsap-10100www.cyber.gc.ca.

Cisco. (2022, January 23). Cisco Annual Internet Report - Cisco Annual Internet Report (2018–2023) White Paper. *Cisco*. https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html

Cloudflare. (n.d.). What is the Mirai botnet?. *Cloudflare*. https://www.cloudflare.com/learning/ddos/glossary/mirai-botnet/

Cohen, G. (2021, November). Throwback attack: An insider releases 265,000 gallons of sewage on the Maroochy Shire. *Industrial Cybersecurity Pulse*. https://www.industrialcybersecuritypulse.com/facilities/throwback-attack-an-insider-releases-265000-gallons-of-sewage-on-the-maroochy-shire/

Cybersecurity and Infrastructure Security Agency. (2015, September 17). FCA Uconnect Vulnerability. *Cybersecurity and Infrastructure Security Agency*. https://www.cisa.gov/news-events/ics-alerts/ics-alert-15-203-01

Cybersecurity and Infrastructure Security Agency. (2015, September 17). Securing the internet of things (IOT). *Cybersecurity and Infrastructure Security Agency*. https://www.cisa.gov/news-events/news/securing-internet-things-iot

Cybersecurity and Infrastructure Security Agency (CISA). (2019, March). The Internet of things: Impact on public safety communications. *CISA: Cyber-Infrastructure*. https://www.cisa.gov/sites/default/files/2023-02/CISA%20IoT%20White%20Paper_3.6.19%20-%20FINAL.pdfwww.cisa.gov.

Department of Homeland Security. (2016, November 15). Strategic principles for securing the internet of things (IOT). *Department of Homeland Security*. https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL_v2-dg11.pdf

Fagan, M., Megas, K. N., Scarfone, K., & Smith, M. (2020). Foundational Cybersecurity Activities for IOT Device Manufacturers. *NIST*. https://doi.org/10.6028/nist.ir.8259

Fortune Business Insights. (2023). Internet of things [IOT] market size, share & growth by 2030. *Fortune Business Insights*. https://www.fortunebusinessinsights.com/

Ghobakhloo, M. (2020). Industry 4.0, digitization, and opportunities for Sustainability. *Journal of Cleaner Production*, *252*, *119869*. https://doi.org/10.1016/j.jclepro.2019.119869

Hossein Motlagh, N., Mohammadrezaei, M., Hunt, J., & Zakeri, B. (2020). Internet of things (IOT) and the energy sector. *Energies*, *13*(2), 494. https://doi.org/10.3390/en13020494

Irdeto. (2019, May 29). New 2019 global survey: IOT-focused cyberattacks are the new normal. *Irdeto Resources Hub*. https://resources.irdeto.com/global-connected-industries-cybersecurity-survey/new-2019-global-survey-iot-focused-cyberattacks-are-the-new-normal

Kandasamy, K., Srinivas, S., Achuthan, K., & Rangan, V. P. (2020). IOT cyber risk: A holistic analysis of cyber risk assessment frameworks, risk vectors, and risk ranking process. *EURASIP Journal on Information Security*, *2020*(1). https://doi.org/10.1186/s13635-020-00111-0

Kimani, K., Oduol, V., & Langat, K. (2019). Cyber security challenges for IOT-based smart grid networks. *International Journal of Critical Infrastructure Protection*, *25*, 36–49. https://doi.org/10.1016/j.ijcip.2019.01.001

Koncagül, E., Tran, M., & Connor, R. (2021). The United Nations world water development report 2021: Valuing water; facts and figures. *UNESDOC Digital Library*. Unesdoc.unesco.org. https://unesdoc.unesco.org/ark:/48223/pf0000375751

Kovacs, E. (2023, January 22). Researcher shows how Tesla Key Card feature can be abused to steal cars. *SecurityWeek*. https://www.securityweek.com/researcher-shows-how-tesla-key-card-feature-can-be-abused-steal-cars/

Kuehn, B. M. (2018). Pacemaker recall highlights security concerns for implantable devices. *Circulation*, *138*(15), 1597–1598. https://doi.org/10.1161/circulationaha.118.037331

Lee, I. (2020). Internet of things (IOT) cybersecurity: Literature review and IOT cyber risk management. *Future Internet*, *12*(9), 157. https://doi.org/10.3390/fi12090157

Lesch, V., Züfle, M., Bauer, A., Iffländer, L., Krupitzer, C., & Kounev, S. (2023). A literature review of IOT and CPS—what they are, and what they are not. *Journal of Systems and Software*, *200*, 111631. https://doi.org/10.1016/j.jss.2023.111631

Lu, Y. (2023). Security and privacy of internet of things: A review of challenges and solutions. *Journal of Cyber Security and Mobility*, *12*(6), 813–844. https://doi.org/10.13052/jcsm2245-1439.1261

Lueth, K. L. (2021, November 8). State of the IOT 2020: 12 billion IOT connections, surpassing non-IOT for the first time. *IoT Analytics*. https://iot-analytics.com/state-of-the-iot-2020-12-billion-iot-connections-surpassing-non-iot-for-the-first-time/

Manyika, J., Chui, M., Bisson, P., Woetzel, J., Dobbs, R., Bughin, J., & Aharon, D. (2015). The internet of things: Mapping the value beyond the hype. *McKinsey*. http://tinyurl.com/yjxv7cfs

Megas, K. (2021, March 4). NIST cybersecurity for IOT. *NIST*. https://csrc.nist.gov/CSRC/media/Presentations/nist-cybersecurity-for-iot-update/images-media/NIST%20%20Cybersecurity%20for%20IOT%20Update%20Megas.pdf

Megas, K., Piccarreta, B., & O’Rourke, D. G. (2017). Internet of Things (IOT) Cybersecurity Colloquium: A NIST Workshop Proceedings. *NIST*. https://doi.org/10.6028/nist.ir.8201

Miller, T., Staves, A., Maesschalck, S., Sturdee, M., & Green, B. (2021). Looking back to look forward: Lessons learnt from cyber-attacks on industrial control systems. *International Journal of Critical Infrastructure Protection*, *35*, 100464. https://doi.org/10.1016/j.ijcip.2021.100464

Moradbeikie, A., Jamshidi, K., Bohlooli, A., Garcia, J., & Masip-Bruin, X. (2020). An IIOT based ICS to improve safety through fast and accurate hazard detection and differentiation. *IEEE Access*, *8*, 206942–206957. https://doi.org/10.1109/access.2020.3037093

Mosenia, A., & Jha, N. K. (2016). A comprehensive study of security of internet-of-things. *IEEE Transactions on Emerging Topics in Computing*, *5*(4), 586–602. https://doi.org/10.1109/tetc.2016.2606384

Obaideen, K., Yousef, B. A. A., AlMallahi, M. N., Tan, Y. C., Mahmoud, M., Jaber, H., & Ramadan, M. (2022). An overview of smart irrigation systems using IOT. *Energy Nexus*, *7*, 100124. https://doi.org/10.1016/j.nexus.2022.100124

Pal, R., Huang, Z., Yin, X., Lototsky, S., De, S., Tarkoma, S., Liu, M., Crowcroft, J., & Sastry, N. (2021a). Aggregate cyber-risk management in the IOT AGEage: Cautionary statistics for (re)insurers and likes. *IEEE Internet of Things Journal*, *8*(9), 7360–7371. https://doi.org/10.1109/jiot.2020.3039254

Potter, K., & Oloyede, J. (2023, May 1). Securing the internet of things (IoT) ecosystems: Challenges, threats and solutions in cybersecurity. *Research Gate*. https://www.researchgate.net/publication/329183740_Securing_the_Internet_of_Things_Challenges_Threats_and_Solutions

RISI. (2015, January 28). RISI Online Incident Database. *RISI*. Retrieved February 2, 2024, fromhttps://www.risidata.com/Database

Saleem, J., Hammoudeh, M., Raza, U., Adebisi, B., & Ande, R. (2018). IOT standardisation: challengesChallenges, perspectives and solution. *Proceedings of the 2nd International Conference on Future Networks and Distributed Systems*. https://doi.org/10.1145/3231053.3231103

Stouffer, K., Pease, M., Tang, C., Zimmerman, T., Pillitteri, V., Lightman, S., Hahn, A., Saravia, S., Sherule, A., & Thompson, M. (2023). Guide to Operational Technology (OT) Securitysecurity. *NIST*. https://doi.org/10.6028/nist.sp.800-82r3

Tariq, U., Ahmed, I., Bashir, A. K., & Shaukat, K. (2023). A critical cybersecurity analysis and future research directions for the internet of things: A comprehensive review. *Sensors*, *23*(8), 4117. https://doi.org/10.3390/s23084117

UNESCO. (2022). Agriculture. *UNESCO*.org. https://www.unesco.org/reports/wwdr/2022/en/agriculture

United Nations. (2023). The Sustainable Development Goals Report. *United Nations*. https://unstats.un.org/sdgs/report/2023/

Vailshery, L.S. (2023a, July 27). IoT total revenue worldwide 2030. Statista. https://www.statista.com/statistics/1194709/iot-revenue-worldwide/

Vailshery, L.S. (2023b, July 27). IoT connected devices by vertical 2030. Statista. https://www.statista.com/statistics/1194682/iot-connected-devices-vertically/

World Bank. (2022, October 5). Water in agriculture. *The World Bank*. (2022, October 5). https://www.worldbank.org/en/topic/water-in-agriculture

World Financial Review. (2021, September 7). Water wastage in agriculture. *The World Financial Review*. https://worldfinancialreview.com/water-wastage-in-agriculture/