SIEMENS
Ingenuity for life

Investing in the Internet of Things (IoT)

How to Turn Data into Value

siemens.com/finance

Contents

Executive Summary Points

- Accenture defines IoT as a network of physical objects, systems, platforms and applications that contain embedded technology to communicate and share intelligence with each other, the external environment and with people[1].

- Enterprises across the globe are increasingly recognizing the importance of leveraging IoT in their core business operations. Many, however, have yet to invest in IoT or put a comprehensive digital strategy in place – citing concerns/challenges ranging from cybersecurity, to change management, to uncertainty about how to derive value from data.

- Early adopters of IoT and Industry 4.0 continue to report significant benefits and are widening their competitive advantage over late followers (i.e., laggard enterprises). Many large manufacturers are fast approaching the “tipping point”, in which more than 50% of the market will have already begun the process of digital transformation.

- In addition to cost reductions and efficiency gains, IoT is helping to spur new business models. In some cases, companies have been able to transition from simply selling physical products to “as-a-service” enterprises that sell outcomes. Two specific examples will be discussed in this paper.

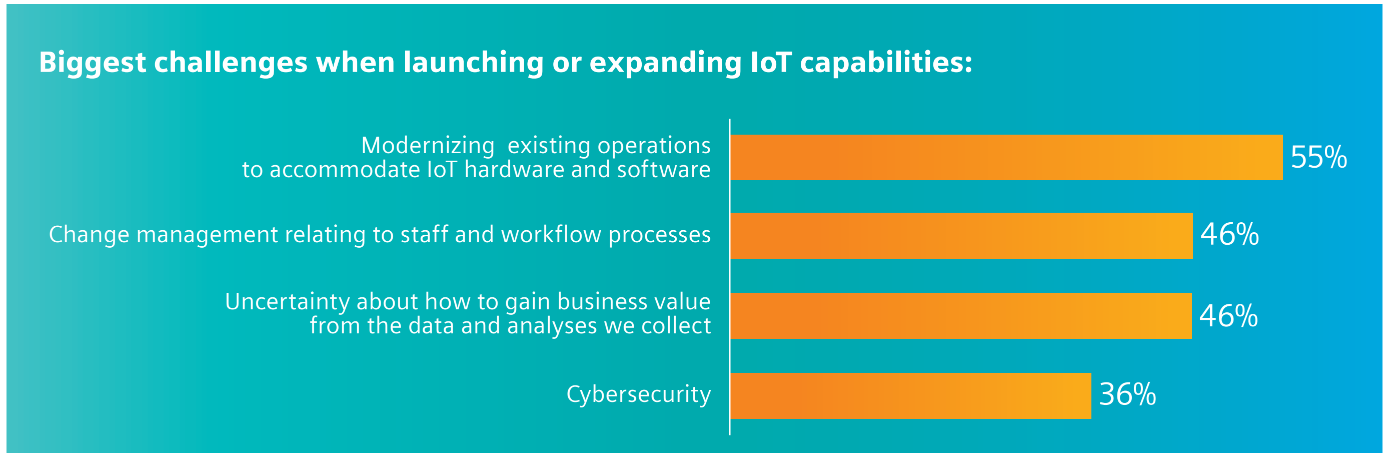
- Cybersecurity is now a key enabler of digital transformation. Companies implementing IoT should therefore be prepared to operate in an environment where cyberattacks are not only possible, but probable. Given this reality, stakeholders must be more expansive and comprehensive when evaluating business risk. This is particularly the case when conducting due diligence for potential acquisitions.

- Contrary to widespread belief, implementing an IoT strategy and capturing the benefits of Industry 4.0 does not require a significant upfront investment. Companies can facilitate a smooth transformation by starting small and allowing their business cases to drive the use of technology (instead of vice versa). Other keys to ensuring the long-term success of an IoT strategy include the use of an open and scalable cloud-based platform for analytics, and the adoption of a “security by default” approach to implementing digital infrastructure.

IoT Deployment – Where We Are Today

The Internet of Things (IoT) continues to emerge as a powerful driver of competitive advantage, enabling enterprises across every industry to realize operational efficiencies that just a short time ago seemed unimaginable. By 2020, as many as 30 billion devices will be connected to the internet, generating millions of terabytes per day[2]. According to Accenture, by 2030, the amount of data produced by IoT will add an estimated $14 trillion in value to the global economy[3].

A recent survey by Siemens and the Harvard Business Review (HBR) found that while many businesses recognize the growing importance of leveraging IoT and digitalization in day-to-day operations, few have actually implemented a strategy to do so. In the survey, which polled approximately 750 executives, 74% of respondents said they believed IoT will be a competitive differentiator. Yet only 36% said they use it in their core operations[4]. Respondents identified a number of barriers that have prevented them from launching and/or expanding their IoT capabilities. Among these were the need to modernize existing operations to accommodate IoT hardware and software; change management related to staff and workflow processes; and concerns related to cybersecurity.


Biggest challenges when launching or expanding IoT capabilities:

All of the issues identified in the survey represent valid concerns for any company embarking on a digital transformation journey. However, the time to address them is now, as it is no longer a question of if or even when digital will disrupt their business, but rather how much of a disadvantage it will create for slow adopters (i.e., "laggard" enterprises). Certain industries, such as automotive manufacturing for example, are now entering a post-digital era, where IoT and Industry 4.0 are no longer competitive differentiators so much as they are a necessary part of companies' corporate strategy.

Today, the need for industrial companies to develop and deploy IoT strategies is imminent, as many sectors are rapidly approaching a tipping point where the majority of the market has already begun the process of digitally transforming their business models. Soon, the possibility of gaining an edge over competitors will have all but disappeared and any enterprises who do not have a comprehensive digital framework in place will be forced to upgrade just to remain relevant. Forward-thinking executives are therefore recognizing the importance of taking action to be able to operate in an environment where IoT is a core driver of business operations and profitability.

Quite simply, it is no longer a question of "whether" or even "when" enterprises should invest in an IoT strategy; it is rather "how" they should go about doing so.

> *"Cybersecurity concerns and difficulty getting support from the C-suite and board are two of the primary challenges we've had in launching our IoT strategy."*
>
> **– Principal at Private Equity Firm**

> *"In the coming years, we believe IoT will help drive increased profitability and competitive advantage by enabling companies to develop new business models and better maintain and manage products and services at customer sites."*
>
> **– VP at Private Equity Firm**

How IoT Fits into Industry 4.0

For industrial enterprises today, it has become difficult to have discussions with technology providers and project stakeholders without hearing "IoT" and "Industry 4.0" being mentioned.

While virtually every decision-maker today has some idea of what these terms mean, few have a clear understanding of how they apply to their business.

In many instances, individuals will often hear IoT and Industry 4.0 used interchangeably, but they are not completely synonymous. In simple terms, IoT refers to a system of sensors, instruments, equipment, and other devices networked together to form an interconnected digital environment. Within the ecosystem, devices recognize, communicate, and exchange data with one another, along with industrial computing applications (often cloud-based). This connectivity allows for the aggregation and analysis of operational data using advanced digital tools, such as artificial intelligence (AI) and machine learning (ML), and ultimately enables operators to facilitate improvements in productivity and efficiency by determining how the performance of one object impacts others and the facility as a whole.

Some of the key enablers of IoT include:

- **Cyber-physical systems** form the foundation for IoT and are what make it possible to connect equipment and machines to the internet. A cyber-physical system is a mechanism or function that is monitored and controlled by software in a computer-based application. Autonomous driving vehicles, for example, rely heavily on cyber-physical systems. The vehicle receives inputs regarding the surrounding physical environment via sensors and makes adjustments accordingly, without explicit direction from the driver. Among IoT-related technologies, the market for cyber-physical systems is expected to be one of the largest growth areas, reaching a total market value of $4.8 billion by 2023[5].
- **Cloud-based industrial platforms** enable companies to connect physical, web- and enterprise-based systems in one central location. They also provide the basis for powerful analysis and visualization of aggregated data, providing users with actionable insights on how processes and equipment performance can be improved and optimized. Siemens MindSphere is an open IoT operating system that supports multiple protocols concurrently. This uniquely simplifies and streamlines the connectivity challenges that most industries face – making it possible for every company to become a digital enterprise.
- **Big Data analytics** are embedded within the architecture of cloud-based digital platforms and provide the capability to analyze large and often disparate data sets to uncover patterns and identify correlations that can be used for decision-making.
- **Artificial intelligence** is an important enabler of digital transformation that involves giving machines the ability to perform cognitive functions in a manner that is similar to humans. Machine learning is a core part of AI, which allows the software to become more accurate with predicting outcomes without explicitly being programmed.

Ultimately, IoT is one of the many concepts and technologies that make up what is often referred to as the Fourth Industrial Revolution or Industry 4.0. At its core, Industry 4.0 is based on a set of design principles that link people, systems, places and equipment/ technology to create interoperability, information transparency, technical assistance and decentralized decision-making. It is practical means of seamlessly integrating physical machinery, robotics, information technology, and the internet to transform industrial facilities into "smart" enterprises.

MindSphere from Siemens

MindSphere is the open, cloud-based Internet of Things (IoT) operating system with data analytics and connectivity capabilities, tools for developers, applications and services. It helps evaluate and utilize manufacturing data and gain breakthrough insights.

With MindSphere, Siemens offers a cost-effective, scalable cloud platform in the form of a Platform as a Service (PaaS) for the development of applications. Designed as an open operating system for the IoT, this platform makes it possible to improve the efficiency of plants by recording and analyzing large volumes of production data. MindSphere provides a solid foundation for applications and data-based services from Siemens and third-party providers, for example in the areas of predictive maintenance, energy-data management and resource optimization.

How IoT is Creating Value and Driving New Business Models

In the early phases of Industry 4.0 (~ 2011 – 2014), there was a great deal of debate about the value that digital transformation could deliver, and whether its potential benefits were being overstated. However, this argument has largely been put to rest, as companies across all industries are reporting quantifiable gains in the form of reduced energy consumption, less downtime, improved margins, increased customer engagement, etc.

In the previously mentioned Siemens-HBR survey, executives identified a number of key benefits from IoT adoption, including enhanced customer service and satisfaction (48%); improved quality of products and services (44%), the ability to develop new products and services (41%), and reduced operational costs (40%)[6].

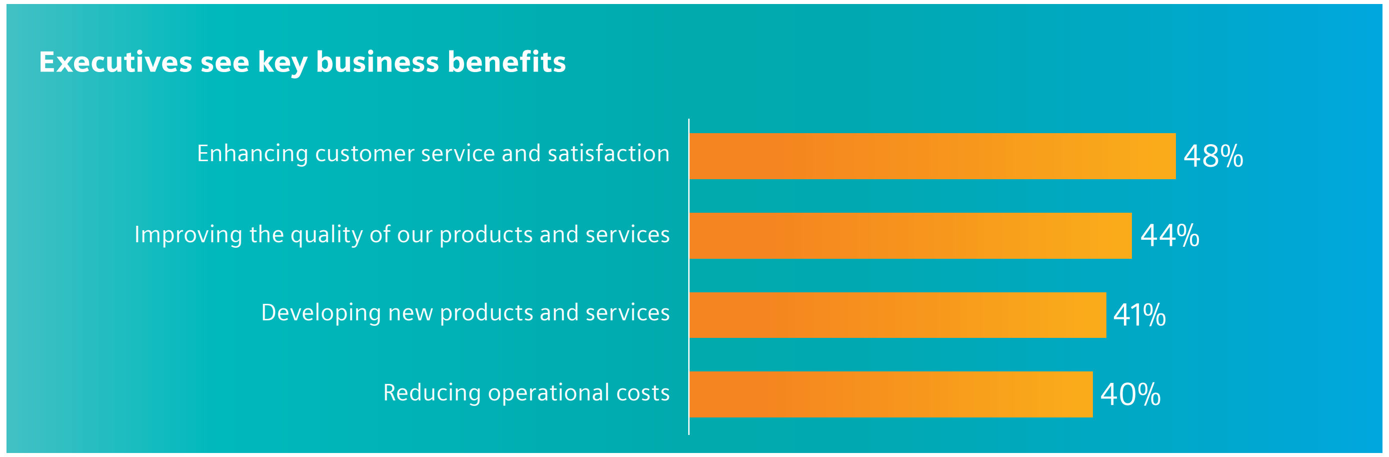
The use of IoT in daily operations is also helping companies implement new and robust financial models. Historically, industrial business models have focused on selling customers on the value that a physical product, piece of equipment or technology can provide over its life. While this is still the case today, the manner in which that value is being delivered is changing, thanks in large part to the growth of "industrial consumerism". As Accenture states:

> *"In the past, industrial companies' sales efforts relied on technology or product leadership to stay ahead of the competition. Today, they must successfully meet the rising service expectations of digitally empowered customers seeking the same levels of ease, transparency and service that they enjoy as consumers. Sales and marketing organizations need to focus less on product and more on the customer experience: continually differentiating the customer journey, leveraging digital technologies to improve established processes and ways of doing business, and becoming high performers in terms of process, organization and strategy[7]."*

Quite simply, digitalization has disrupted what was once a simple and linear buying process in the B2B space. Our experiences as consumers are increasingly influencing what we expect in the business world. In our personal life, we can order virtually any product in the world from our smartphone with all of its specifications customized to fit our unique needs. Why can't we have this same experience in the workplace? It is this mindset that is driving the need for industrial companies to fundamentally think about their business and products differently.

Although the process of adapting financial and business models to better serve the needs of customers will look different for every enterprise, the first step is always the same: enabling connectivity. At Siemens, we see a growing number of manufacturers digitally-enabling their equipment so they can gain visibility into how it is performing in the field. With the data, the manufacturer can then begin to paint a picture of how their products are being used by customers. They can also better understand what, if any issues the customer is experiencing and identify opportunities for improvements, both in the product's design and how it is being operated.

This is a key benefit for many organizations, as the sale of the physical product is only one component of their overall business model. For large pieces of equipment, there are often service and maintenance contracts that go along with the sale, which represent long-term revenue streams. Take an industrial air compressor, for example. By connecting the compressor and gathering operational data, the original equipment manufacturer (OEM) can monitor its condition and conduct maintenance and service based on need rather than on frequency. This type of predictive maintenance benefits the customer by reducing downtime. It also benefits the OEM by allowing them to efficiently allocate valuable time and resources, such as labor, while guaranteeing a certain level of performance to their customers.


Executives see key business benefits

Ultimately, by leveraging IoT and embracing connectivity, industrial companies can begin to adopt an "as-a-service"- or "outcome"- based business model. In the case of the air compressor, the customer is no longer simply buying the compressor; they are buying the outcome of compressed air – not dissimilar from how software companies have transitioned from licensed product sales to on-demand services.

One real-world example of a company that has had success with the as-a-service model is Michelin. In 2013, Michelin introduced its EffiFuel service, which is designed to help logistics companies improve fuel efficiency on the road. Part of the service involves the use of telematic devices to monitor drivers' behavior. The data gathered from these devices is analyzed on Accenture's cloud-based platform to better understand what driver actions affect fuel consumption. Michelin then uses that information to help its logistics customers enhance fuel efficiency[8]. Through its leveraging of IoT, Michelin has effectively transitioned from simply selling tires as a physical product, to a service company that can guarantee customers an outcome: quantifiable improvements in fuel efficiency.

The as-a-service business model is easier to scale and offers many financial advantages, including more predictable revenue, which often leads to an increased valuation of the business. It also allows organizations to capture areas of the market that they couldn't otherwise. Smaller manufacturers, for example, don't always have the resources to make large up-front capital investments in large pieces of equipment. Engaging with an OEM who provides industrial capabilities as-a-service changes that – opening up new possibilities to grow business.

Another company that is utilizing IoT to transform the products it provides is French-based Faurecia, which manufacturers automotive parts. Faurecia recently introduced its *"Cockpit of the Future"* concept – which is geared toward autonomous driving vehicles. Faurecia states:

> *"The increasing autonomy and connectedness of vehicles is radically altering the driving experience and as a consequence the vehicle interior. Different use cases are emerging for occupants allowing both drivers and passengers to be able to work or relax in certain situations. Faurecia has taken full measure of this, pioneering a comprehensive technology offer that makes the cockpit of the future a reality today"[9].*

One of the many advanced capabilities of the *"Cockpit of the Future"* is that it can record the preferences of the vehicle occupant to create a personalized user profile. When the occupant enters the vehicle, lighting, sound ambiances, and seat configuration automatically adjust to the desired setting and preferences – creating a truly customized experience for the driver and/or passenger. Similar to Michelin, Faurecia has also launched a *"Clean Drive"* application, which collects and analyzes the mobility behavior, providing actionable insights to drivers on what measures they can take to reduce emissions[10].

All of these opportunities (and more) are made possible by connecting products in the field and leveraging the data they generate. In the coming years, it is this data that will be the primary driver of revenue. Accenture predicts, in fact, that in the coming years, 70% of product value will be derived from the data it generates, and not from the product itself[11].

Cybersecurity, Data Privacy and the Role They Play in Due Diligence

Despite the immense value that Industry 4.0 and IoT can provide, connecting machines and equipment to cloud-based platforms does mean that companies must be prepared to operate in an environment in which cyberattacks are not only possible, but probable. While no industry or company is safe from the threat of a cyberattack, industrial enterprises represent a particularly attractive target because of how exposed their legacy IT systems often are.

Over the years, manufacturers, have dedicated a great deal of their focus to securing their operational technology (OT) assets – that is the machines and equipment that are critical to production. However, the protection and security of IT networks has lagged behind. Malicious actors are aware of the weaknesses in these systems and have targeted enterprises strategically. Cyber actors also know that the supply chain for manufacturers is large and complex with numerous vulnerabilities, making it an ideal environment to execute an attack, especially given that any infection could quickly spread to other businesses and suppliers. According to manufacturing organization EEF, 48% of manufacturers have at some point been subject to a cybersecurity incident, and half of those organizations suffered financial loss or a disruption to their business[12].

Given the increasing threat of cyberattacks and data breaches in today's environment, companies and investors must be much more expansive and comprehensive in their due diligence during potential acquisitions. It is no longer enough to simply assess the financial viability of the business being acquired. Buyers must ensure that whatever enterprise they are acquiring is sound from the perspective of data protection and cybersecurity. In most cases, this requires bringing in subject matter experts (SMEs) with knowledge of the cyber domain, such as technologists, to make sure the asset being acquired is really what it appears to be and not the proverbial "ticking time bomb".

> *"One of the primary concerns facing industries today is that the pace of technological advancement has not always been commensurate with attention to internal governance. IoT strategies can deliver huge financial advantages to any company, but without proper governance in place, those advantages will disappear quickly and possibly publicly. From an investment perspective, cybersecurity and data protection have traditionally been somewhat of an incidental issue. However, they are now fundamental and must be part and parcel of the devices, systems, and strategies companies are implementing."*
>
> **– Jeffrey Poston, Partner at Crowell & Moring, Co-chair of Privacy & Cybersecurity Group**

There are now many real-world examples of how costly a data breach can be for a company. Perhaps one of the most high-profile in recent years was Verizon's acquisition of Yahoo. Before the acquisition was final, it was revealed that Yahoo had experienced multiple data breaches. This resulted in the sale price of Yahoo being reduced by $350 million[13].

Overall, during an acquisition, there must be transparency regarding the cyber history of the company. Has the company had any reported instances of data breaches? Have there been unreported instances? These questions and others must be answered during the due diligence process to avoid potential problems post-acquisition.

Attention must also be paid to the specific type of data that is being acquired with a company. Healthcare data, for example, is subject to the Health Insurance Portability and Accountability Act (HIPAA). Other personal data may be subject to data privacy laws such as the EU's General Data Protection Regulations (GDPR). Buyers and investors must also consider issues related to corporate governance. For instance, how the new company or asset will align with current policies and procedures that are in place at the parent company. If proper governance is not in place, the benefits and advantages afforded by IoT can disappear quickly and sometimes publicly.

One other obvious issue besides internal governance is the proliferation of laws and regulations around the world, which have not been commensurate with the pace of technological advancement. In some cases, 100% compliance with regulations may not be possible. In these instances, companies have to focus on taking a practical approach. They must be able to demonstrate to governing bodies that reasonable measures have been taken to protect the systems they have put in place and the associated data they produce.

Overall, data protection and cybersecurity are no longer incidental to digital transformation; they are fundamental. Both have to be part and parcel of the company leveraging IoT. For example, Siemens teamed up with governmental and business partners in cybersecurity to implement the Charter of Trust, an initiative to protect data of individuals and companies, prevent damage to people, companies and infrastructure, and create a reliable foundation on which confidence in a networked digital world can take root and grow. Together, with market leaders in cybersecurity, Siemens is positioned to help ensure success and trust in our digital economy.

Historically, cybersecurity has been viewed as a cost. Increasingly, however, it is being viewed as an asset that can be a driver of competitive advantage and a market differentiator.

Starting the IoT Journey – "Think Big, Start Small, and Scale Fast"

Contrary to widespread belief, implementing an IoT strategy and capturing the benefits of Industry 4.0 does not require a significant upfront investment. Organizations often believe that complex change management measures must be put in place before embarking on the digital journey. However, transformation does not happen overnight. Every enterprise that leverages IoT as part of its core operations started with a single use case and scaled from there at their own pace.

Today, many industrial organizations no longer have the luxury of moving as slowly as they might like due to the risk of falling behind and becoming uncompetitive. They must instead adopt a *"think big, start small, scale fast"* approach, in which the primary focus is on studiously and aggressively making digital a key pillar of their business. There are many steps they can take to ensure successful adoption of an IoT strategy. Some of these include:

- **Drive from the business case, not the technology**
  Too often, companies begin their IoT journey by searching for ways to apply a new technology to a specific business case. They become enthralled with the capabilities the technology can provide and then "force feed" it into their operations. While in some instances this approach can result in capturing marginal efficiency gains, it very rarely ends up generating any type of transformative value. The organization may end up with several interesting proofs of concept which have limited real-world applicability. A more productive approach is to allow the business case to drive how technology and IoT are implemented – measuring the business against traditional metrics and key performance indicators (KPIs).

- **Choose an open and flexible IoT platform**
  Many advanced IoT platforms exist in the marketplace today. It is important that whichever option an organization decides to use as part of its digitalization strategy be open, flexible, and scalable so that the architecture can grow and advance as new technological opportunities arise.

  Numerous individual digital point solutions must be implemented to create a digitally-enabled enterprise or industrial facility. Being able to aggregate and analyze all of the data they produce on a single and consistent platform is critical to maximizing return on investment (ROI) from IoT. Open platform as a service (PaaS) capabilities enable a rich partner ecosystem that offers a wide range of innovative IoT solutions. By seamlessly integrating operational data throughout the value chain, companies will not only drive greater operational transparency and performance, but will also be able to compare simulation and test results with real-world observations to boost performance, sharpen their competitive edge and realize much more profitability.

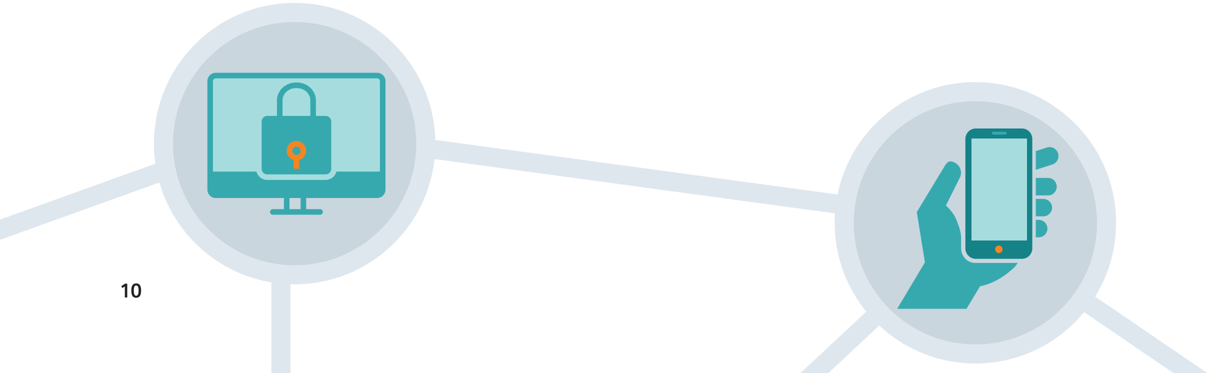
- **Get executive leadership on board**
  As is the case when adopting any new technology or business process, there will inevitably be bumps in the road and hurdles to overcome during the digital transformation journey. To ensure continuity, it is important that operations personnel implementing IoT capabilities make executive leadership apprised of progress and goals. Companies must strive to create a work environment where innovation and digitalization are part of the fabric of corporate culture – and this starts at the top of the house.

- **Emphasize "security by default / design"**
  The benefits afforded by digital transformation and IoT are no longer in question. However, operating in an environment where devices and equipment are connected does expose businesses to the risk of cyber attacks, which unfortunately are becoming the norm in today's environment. It is no longer a question if an enterprise will face an attack at some point, it is a matter of when. In some cases, intrusions have already occurred but have gone undetected. For this reason, cybersecurity and data privacy have to be a fundamental pillar of an IoT strategy – a concept often referred to as "cybersecurity by design or default".

  Cybersecurity by design refers to a proactive approach to securing the digital environment – not only through front-end protections that prevent breaches, but also through monitoring of networks to detect any intrusions. Companies must also have incident response plans in place in the event that a breach does occur. Ultimately, IoT and cybersecurity are two sides of the same coin. Failure to acknowledge this reality can have wide ranging and costly consequences, regardless of an organization's size or industry.

Conclusion

IoT and Industry 4.0 are generating transformative value for industrial enterprises, ushering in a new era where digital is a key driver of competitive advantage. Research suggests that an increasing number of companies recognize this trend; however, the majority have yet to put a comprehensive IoT strategy in place. Reasons for this include concerns related to cybersecurity, change management difficulties, the need to modernize existing operations, and uncertainty about how to gain business value from the data that is collected. While all are valid concerns, they can no longer be seen as barriers to IoT adoption, as the world is fast approaching a tipping point in which any organizations that have failed to act will be at a significant disadvantage. Quite simply, the time for passivity, as it pertains to IoT and digital transformation, has come and gone. The Fourth Industrial Revolution is well underway and companies must adapt their financial and business models in order to remain relevant.



References:

1. Winning with the Industrial Internet of Things (2015). Accenture. https://www.accenture.com/t00010101T000000Z__w__/it-it/_acnmedia/PDF-5/Accenture-Industrial-Internet-of-Things-Positioning-Paper-Report-2015.pdf
2. The Company (2019). Siemens AG. https://www.siemens.com/press/pool/de/homepage/Siemens-company-presentation.pdf
3. Winning with the Industrial Internet of Things (2015). Accenture. https://www.accenture.com/t00010101T000000Z__w__/it-it/_acnmedia/PDF-5/Accenture-Industrial-Internet-of-Things-Positioning-Paper-Report-2015.pdf
4. Internet of Things Pulse Survey (2019). Siemens AG and Harvard Business Review Analytic Services. https://www.siemens.com/press/pool/de/homepage/Siemens-company-presentation.pdf
5. Industry 4.0 Technologies to Reach 23.1% Annual Growth Rate. (July 2018). BCC Research. https://www.globenewswire.com/news-release/2018/07/09/1534764/0/en/Industry-4-0-Technologies-to-Reach-23-1-Annual-Growth-Rate.html
6. Internet of Things Pulse Survey (2019). Siemens AG and Harvard Business Review Analytic Services. https://www.siemens.com/press/pool/de/homepage/Siemens-company-presentation.pdf
7. Industrial Consumerism Getting Serious About Disruptive Growth. Accenture. https://www.accenture.com/us-en/insight-industrial-consumerism?c=prod_indsrurltwt_10000035&n=smc_1216
8. Michelin: Tires-as-a-service (November 2016). Harvard Business School. https://rctom.hbs.org/submission/michelin-tires-as-a-service/#
9. Cockpit of the Future. Faurecia. https://www.faurecia.com/en/innovation/smart-life-board
10. Max, J. Faurecia's Auto Cockpits of the Future Dazzle at CES (January 2018). Forbes. https://www.forbes.com/sites/joshmax/2018/01/19/faurecias-auto-cockpits-of-the-future-dazzle-at-ces/#6697e8264e1f
11. Investing in the Internet of Things – How to Turn Data into Value (May 2019). Brian Irwin. Accenture. Intergrowth Panel.
12. Camillo, M. Cyber is Moving Up the Agenda for Manufacturers. (February 2019). AIG. https://www.aig.co.uk/insights/cyber-agenda-manufacturers-camillo
13. Lunden, I. After Data Breach, Verizon Knocks $350M Off Yahoo Sale, Now Valued at $4.48B (2017). TechCrunch. https://techcrunch.com/2017/02/21/verizon-knocks-350m-off-yahoo-sale-after-data-breaches-now-valued-at-4-48b/

Published by
Siemens Financial Services, Inc. 2019

Siemens Financial Services, Inc.
170 Wood Avenue South
Iselin, NJ 08830

For more information:
E-mail: usamarketing.sfs@siemens.com
Updated (unless stated otherwise): December 2019

usa.siemens.com/finance

Follow us!

linkedin.com/company/siemens-financial-services

twitter.com/siemens_sfs

fb.com/siemensfinancialservices