FROST & SULLIVAN

CYBER SECURITY IN THE ERA OF INDUSTRIAL IOT

Discerning implications of cyber security in a converged IT-OT environment

A Frost & Sullivan White Paper

TABLE OF CONTENTS

Executive Summary 3

Introduction and Context 3

Cyber Security in the Industrial Landscape...9

The Difficulty in Defining Industrial Cyber Security..12

Examining the Cyber Risk Gap: The End-user Perspective..13

Getting Started with Industrial Cyber Security...18

Industrial Cyber Security- The Viewpoint of Bayshore Networks 20

Conclusion 24

EXECUTIVE SUMMARY

Industrial cyber security has been a topic of much debate over the last decade. Despite the industry's widespread acknowledgement of its significance, cyber security in the industry continues to be an elusive subject for many. A huge gap exists in understanding the implications of cyber security; however, the subject has been greatly discussed. Interestingly, the industrial environment is currently passing through a key phase, where the idea of Internet of Things (IoT) is beginning to pervade all areas of industrial operation. This ongoing change is poised to expand the complex security needs in the factories of the future.

In an effort to shed light on how the evolution of cyber security is foreseen, this white paper tries to define, identify, and contextualise security needs in a connected enterprise. This paper's key intent is to indicate how the convergence of information technology (IT) and operational technology (OT) will close the gap between safety and security that currently exists in industrial processes. For this purpose, insights from new policy initiatives, industry use cases, and possible solutions presently available in the market have been leveraged. The objective of this endeavor is to emphasize clearly on why we need to move beyond discussions and approach cyber security as an essential and undeniable condition for a connected enterprise.

INTRODUCTION AND CONTEXT

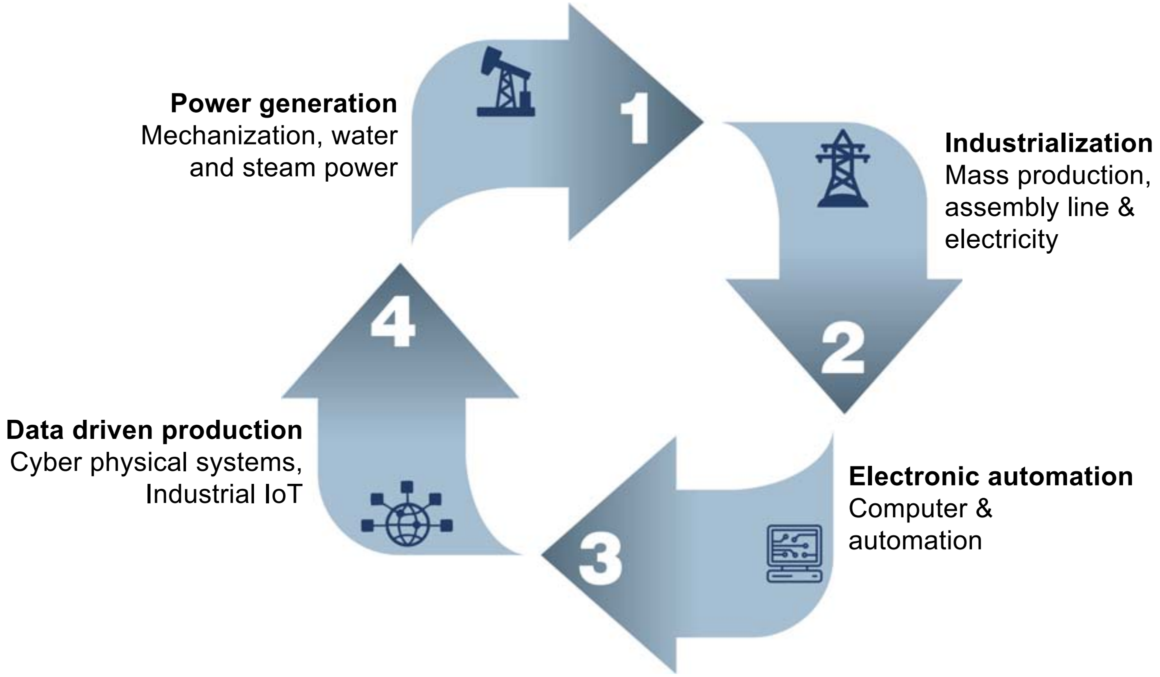
Industrial revolutions have been epochal events in global history. The invention of steam power in the 18th century marked the beginning of the first revolution in manufacturing. With steam power, factories that earlier relied on wind and water power could be built anywhere and not only adjacent to flowing rivers. Transportation, in particular, stood to gain the most during this period. For the first time raw materials and manufactured goods could be transported over land, by means other than those powered by humans or animals.

The second industrial revolution saw the advent of electric energy-driven mass production, enabling workers to make copies of products quickly using assembly line techniques. This change in approach helped workers conveniently send partially completed products through the line so they could work in batches, rather than having to wait for one person to work on a product from start to finish. With the third industrial revolution, electronics and computers were used to enable automation, resulting in a highly productive industrial environment and marking the beginning of the information age.

In the current juncture, the world is at the cusp of a fourth industrial revolution- one that will be empowered and catalyzed by the Internet of Things. This new and upcoming change in industries is also referred as Industrie 4.0- a term that was first introduced in Germany in 2013 and gained immense popularity henceforth. At its core, Industrie 4.0 places the idea of cyber-physical production as the means for improving operational efficiency, productivity, and customization.

While Industrie 4.0 is a broad framework for the future of manufacturing, the trend of IoT for Industries is more comprehensive and indicative of the nature of technological change set to impact global industries.

Exhibit 1: Industrial Revolutions – A Chronology


Power generation
Mechanization, water and steam power
1
Industrialization
Mass production, assembly line & electricity
2
Electronic automation
Computer & automation
3
Data driven production
Cyber physical systems, Industrial IoT
4

Source: Frost & Sullivan

Through Industrial IoT, systems, assets, and machines can be tapped for valuable product and process intelligence that can be used for real-time decision making. Industrial IoT is also succinctly referred as IIoT.

According to Frost & Sullivan research, only 25 to 30%[1] of manufacturing companies around the globe have adopted IIoT (in different forms and degrees) in 2016. This adoption is expected to increase to 80% by 2021. To enable this disruption, organizations from both public and private sectors are collaborating to initiate new policies surrounding IIoT.

Mega Trends Driven by Industrie 4.0

- Surging data volume, improved computational power, and connectivity
- Advancing data analytics and data processing capabilities
- Progressing human-machine interactive systems
- Ameliorating communication between the digital and physical environments

Organizations from the OT and IT sectors are realizing the need for co-optation and are working towards building common knowledge-sharing platforms. Some prominent initiatives in this space include the Industrial Internet Consortium (IIC), Plattform Industrie 4.0, and the Smart Manufacturing Leadership Coalition (SMLC).

The IIC is an open membership organization that brings together government, academia, and the industry. The IIC was initially formed by market participants such as AT&T, Cisco Systems, General Electric, IBM, and Intel. The IIC currently includes more than 200[2] top organizations and academic institutions worldwide, including those in countries such as India, China, and Germany. These organizations specifically focus on promoting IIoT by identifying potential applications and associated security issues in industries through three key focus areas: technology, test beds, and security.

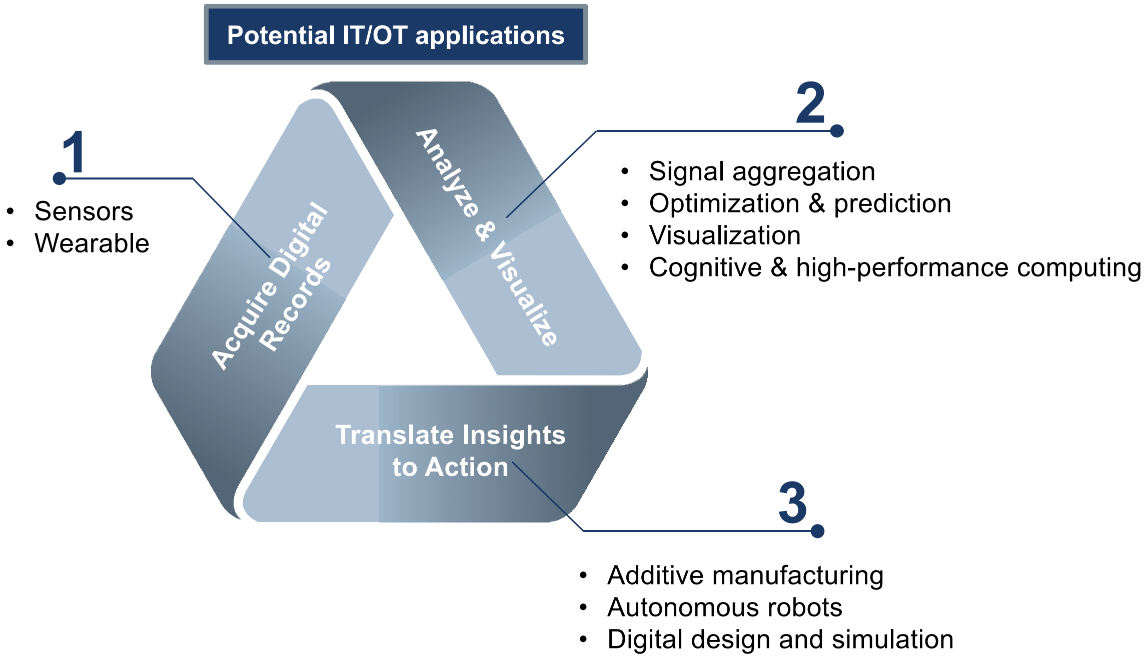
Industrie 4.0, the German initiative for advanced manufacturing, hinges on three sequential and conditional steps for implementation. This includes the following:

Step 1 - Acquire Digital Records includes the digitization of physical industrial products and process data through sensors. These sensors are attached to industrial assets and can sense and capture data, while closely mimicking human sensorial abilities. The technology that allows this fusion is called sensor fusion, which leverages a microcontroller to combine the individual data packets from multiple sensors, enabling a holistic view of the overall data collected.

Step 2 - Analyze & Visualize involves the application of analytical capabilities on the raw data collected from sensors, aided by the use of various data visualization and analytical tools. The serving infrastructure to this capability is provided by the industrial cloud that can help store the huge volume of collected data and serve as a platform on which this data can be further processed.

Step 3 - Translate Insights to Action involves the application of derived insights to automate decision making, resulting in tangible execution or action in the physical environment.

Exhibit 2: The Cyber-Physical Cycle of Industrie 4.0


Potential IT/OT applications
1
Sensors
Wearable
Acquire Digital Records
2
Analyze & Visualize
Signal aggregation
Optimization & prediction
Visualization
Cognitive & high-performance computing
3
Translate Insights to Action
Additive manufacturing
Autonomous robots
Digital design and simulation

Source: Frost & Sullivan

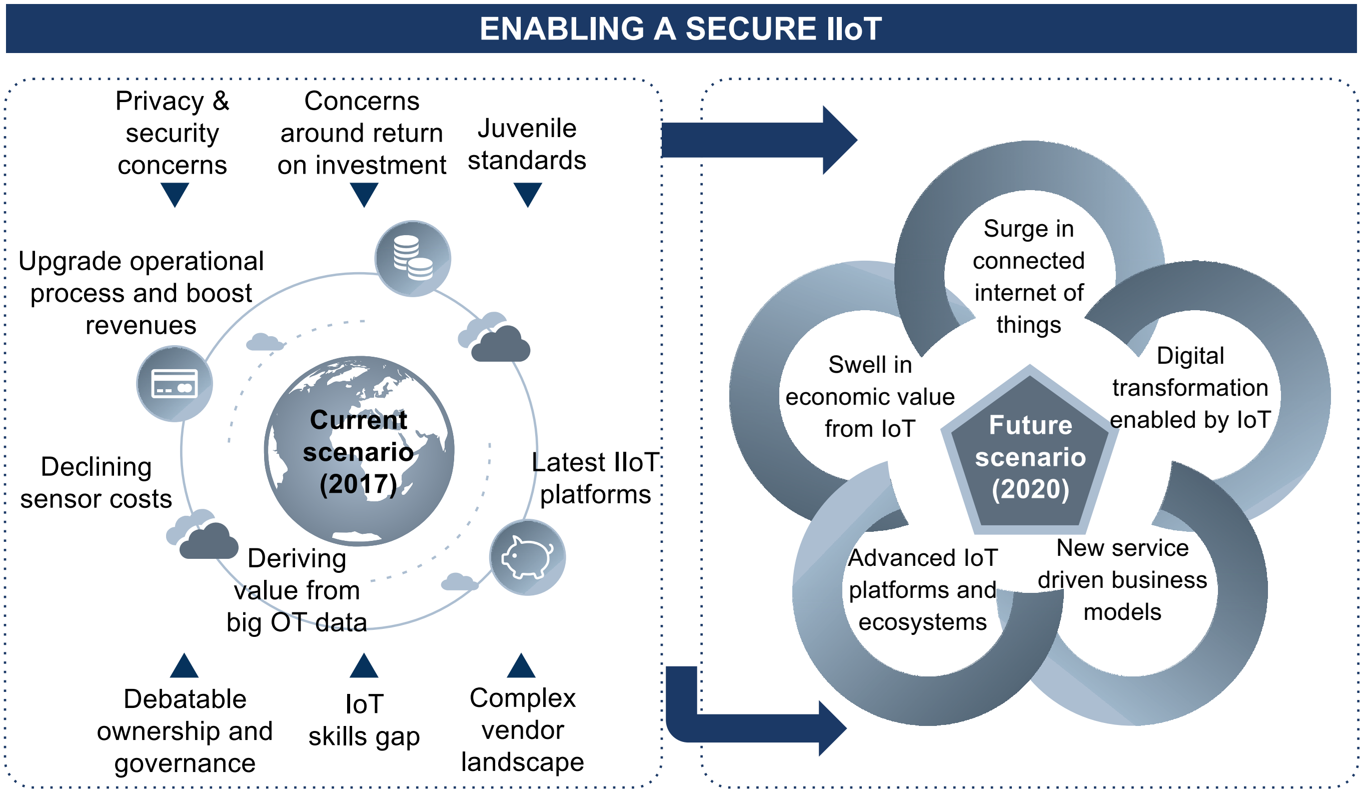
SMLC, on the other hand, is the US initiative for smart manufacturing that places a relatively stronger affinity towards commercial ICT (information and communication technology). It is a non-profit organization comprising manufacturers, technology partners, academic institutions, and government agencies. The main objective of this initiative is to build smart manufacturing enterprises that are fully integrated, knowledge enabled, and model rich.

The active role played by such policy bodies indicated here, have been significant in keeping the narrative on digitalized manufacturing alive. But this does not preclude many formidable challenges that need to be surmounted. For instance, traditional manufacturing has always involved manual processes, supervision, and testing; however, with the introduction of IIoT, new, advanced systems are required to be implemented across various levels of production. In the future, legacy systems have little or no utility in the factory floor unless they are converted into an entity that can generate value in an IIoT-enabled operational environment. According to the OPC Foundation (The Industrial Interoperability Standard), nearly 120 million[3] connected devices from automation suppliers are relaying data every second. Only a marginal portion of these connected devices are actually being analyzed- less than 10%, according to Frost & Sullivan research.

If the industry is to expand its extent of data analysis, then this will involve building the appropriate capacity for storage infrastructure. This in many ways will be a pre-requisite for realizing an IIoT-defined operational environment that will be driven by data-based decision making. In such a scenario, a cloud-based data infrastructure is the only possible way for industries to move ahead.

The industrial cloud provides the required basis for industrial end-users to store plant data and serves as a platform where this data can be harvested further. In an industrial cloud, the raw data is turned into actionable insights through advanced data analytics. Furthermore, the data is processed constantly, and actionable insights can be generated on the fly in real-time.

Exhibit 3: Current and Future Benefits from the Converged IT/OT Environment


ENABLING A SECURE IIoT
Privacy & security concerns
Concerns around return on investment
Juvenile standards
Upgrade operational process and boost revenues
Current scenario (2017)
Declining sensor costs
Latest IIoT platforms
Deriving value from big OT data
Debatable ownership and governance
IoT skills gap
Complex vendor landscape
Surge in connected internet of things
Swell in economic value from IoT
Digital transformation enabled by IoT
Future scenario (2020)
Advanced IoT platforms and ecosystems
New service driven business models

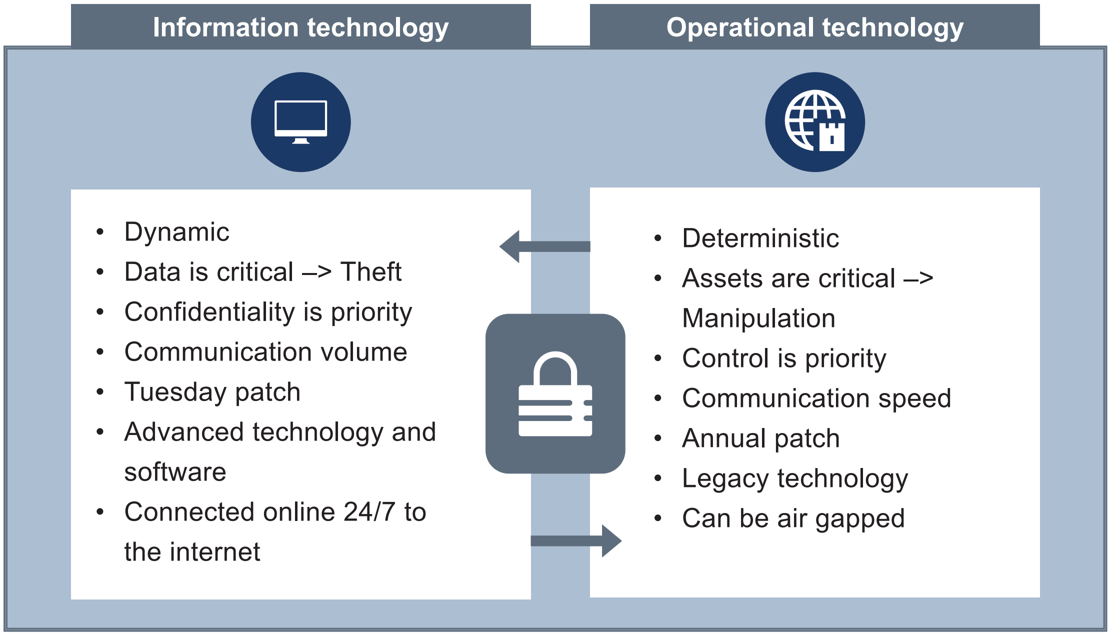
Source: Bayshore Networks

With such new transformations in manufacturing, we realize that IT (information technology) and OT (operational technology) environments are getting increasingly intertwined. The convergence of IT and OT, as we have seen, brings about tremendous opportunities for end-users to derive greater value out of everyday operation. At the same time, the fusion of IT and OT brings with it newer challenges, especially of cyber security.

Despite the value of IT-OT convergence, end-users in the industry are skeptical on the new security risks that are bound to arise with this development. For example, extending network connectivity to OT environments makes IT prone to newer forms of cyber-attacks. Many processes in the OT environment involve manual intervention; a prime reason as to why OT environments deeply stress on the need for physical security. With the onset of industrial data, industrial cyber security is poised to become another major requirement for industries. Many IT tools created to function within the enterprise layer may not necessarily function effectively in an OT environment.

Such unforeseen circumstances may result in OT systems crashing, leading to process disruptions, data corruption, and financial losses. Reliability is thus a very critical factor in an OT environment. It is also one of the main reasons for the slow pace of technology adoption that the industry has exhibited historically.

Exhibit 4: Growth of the Digital/Physical Threat in a Converged IT-OT Environment



Information technology

- Dynamic
- Data is critical –> Theft
- Confidentiality is priority
- Communication volume
- Tuesday patch
- Advanced technology and software
- Connected online 24/7 to the internet

Operational technology

- Deterministic
- Assets are critical –> Manipulation
- Control is priority
- Communication speed
- Annual patch
- Legacy technology
- Can be air gapped

Source: Frost & Sullivan

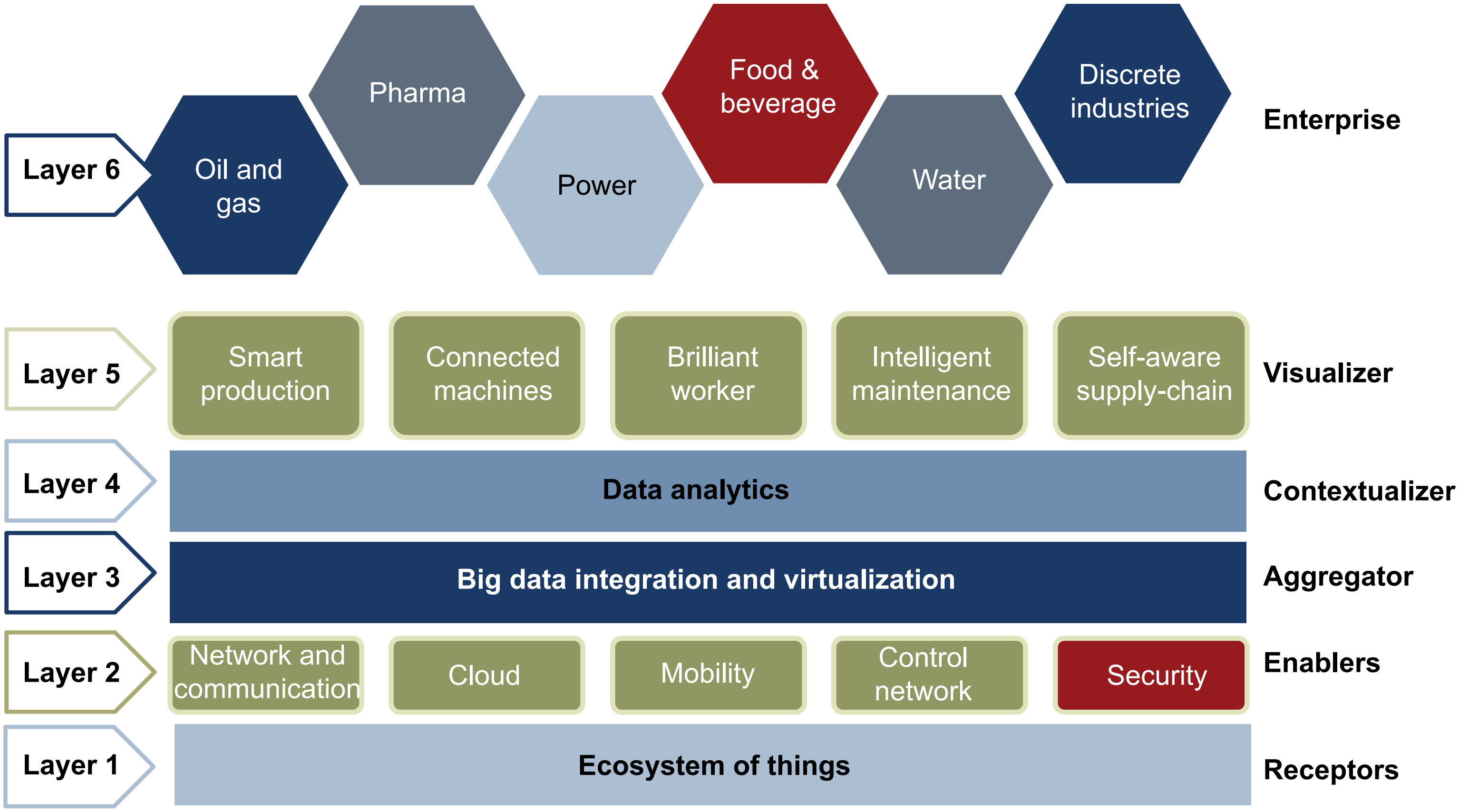
The conservative nature of the OT industry makes it possible for companies to adopt IIoT applications only after the underlying technology has a clear proof-of-concept and been sufficiently established in the market. In contrast, the IT industry has always been more open to change and experiments with newer technologies. This cultural difference between the two environments is likely to cause a certain level of friction in the adoption of IIoT by industrial customers. In particular, the inherent challenges arising out of IT-OT convergence is bound to get manifested especially in the case of industrial cyber security.

Many of the current security solutions in the IT world are not custom-built to handle the complexities of an OT environment. Industrial cyber security has thus been identified as one of the top concerns in the manufacturing sector that has seen a marked increase in the number of cyber-attacks globally. Attacks are becoming increasing complex and possess the potential to create large-scale damage as perpetuators are becoming increasingly aggressive with new black hat hacking techniques. Cyber security, as a consequence, is poised to become the common underlying denominator for industrial advancement.

CYBER SECURITY IN THE INDUSTRIAL LANDSCAPE

With the emergence of the Internet, cyber security has been a widely debated and deeply invested topic in the IT industry for the last two decades. In contrast, the industrial environment has only recently taken to cyber security. The topic gained momentum especially after the infamous Stuxnet attack in an Iranian nuclear facility in 2010. While the Stuxnet event is considered a key inflection point, a broader technical understanding of the issue is needed to comprehend the overall risks in details. Exhibit 6 provides a list of most prominent cyber-attacks the industry has encountered since 2000.

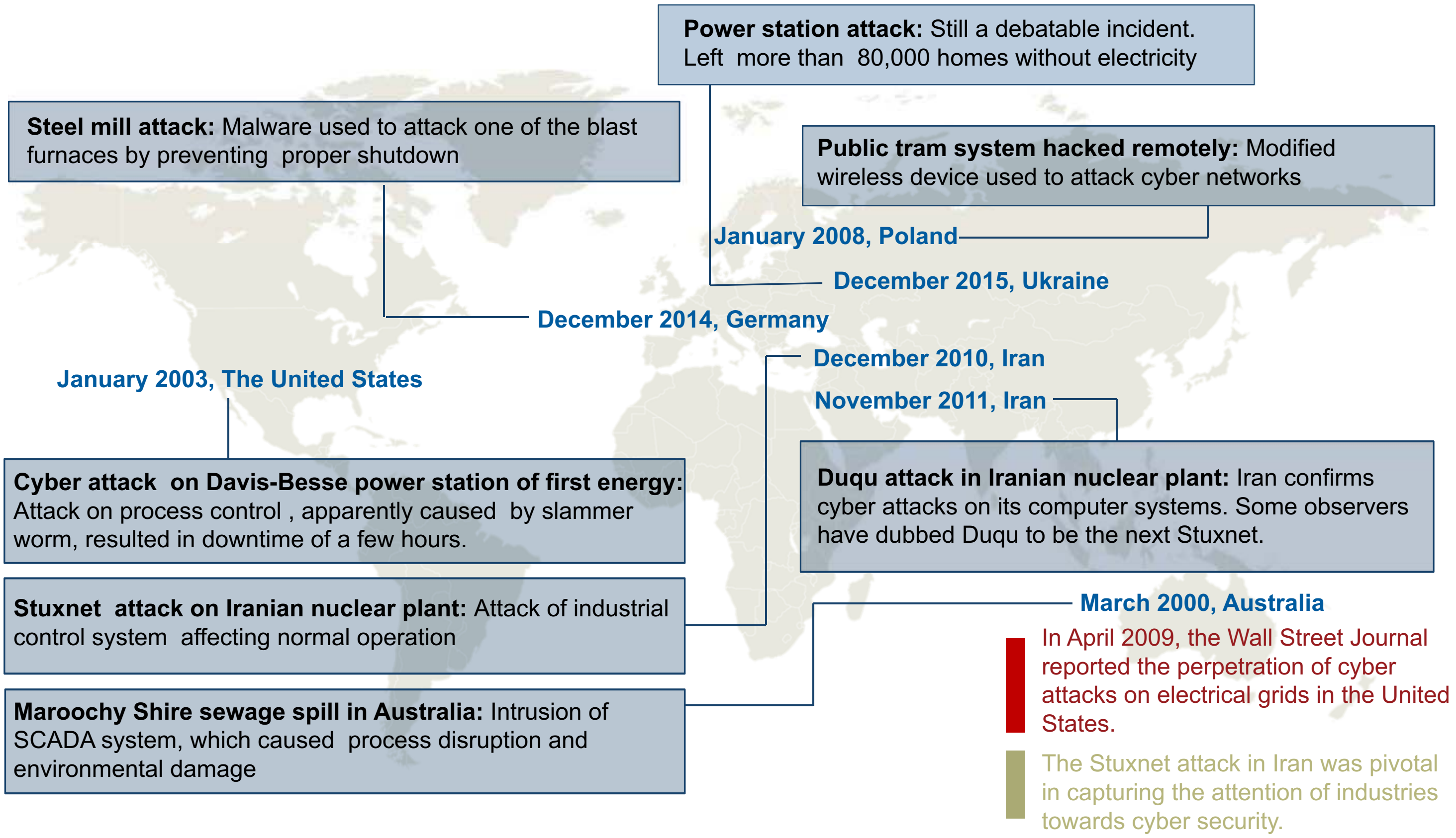
Exhibit 5: Cyber Security—A Key Enabler in the Industrial Enterprise of Tomorrow



Source: Frost & Sullivan

Exhibit 6: Chronology of Industrial Cyber Attacks

The number of cyber attacks on industries and commercial IT networks has seen a marked increase in terms of both frequency and intensity over the last five years.



Power station attack: Still a debatable incident. Left more than 80,000 homes without electricity

Steel mill attack: Malware used to attack one of the blast furnaces by preventing proper shutdown

Public tram system hacked remotely: Modified wireless device used to attack cyber networks

January 2008, Poland

December 2015, Ukraine

December 2014, Germany

December 2010, Iran

January 2003, The United States

November 2011, Iran

Cyber attack on Davis-Besse power station of first energy: Attack on process control , apparently caused by slammer worm, resulted in downtime of a few hours.

Duqu attack in Iranian nuclear plant: Iran confirms cyber attacks on its computer systems. Some observers have dubbed Duqu to be the next Stuxnet.

Stuxnet attack on Iranian nuclear plant: Attack of industrial control system affecting normal operation

March 2000, Australia

Maroochy Shire sewage spill in Australia: Intrusion of SCADA system, which caused process disruption and environmental damage

🟥 In April 2009, the Wall Street Journal reported the perpetration of cyber attacks on electrical grids in the United States.

🟩 The Stuxnet attack in Iran was pivotal in capturing the attention of industries towards cyber security.

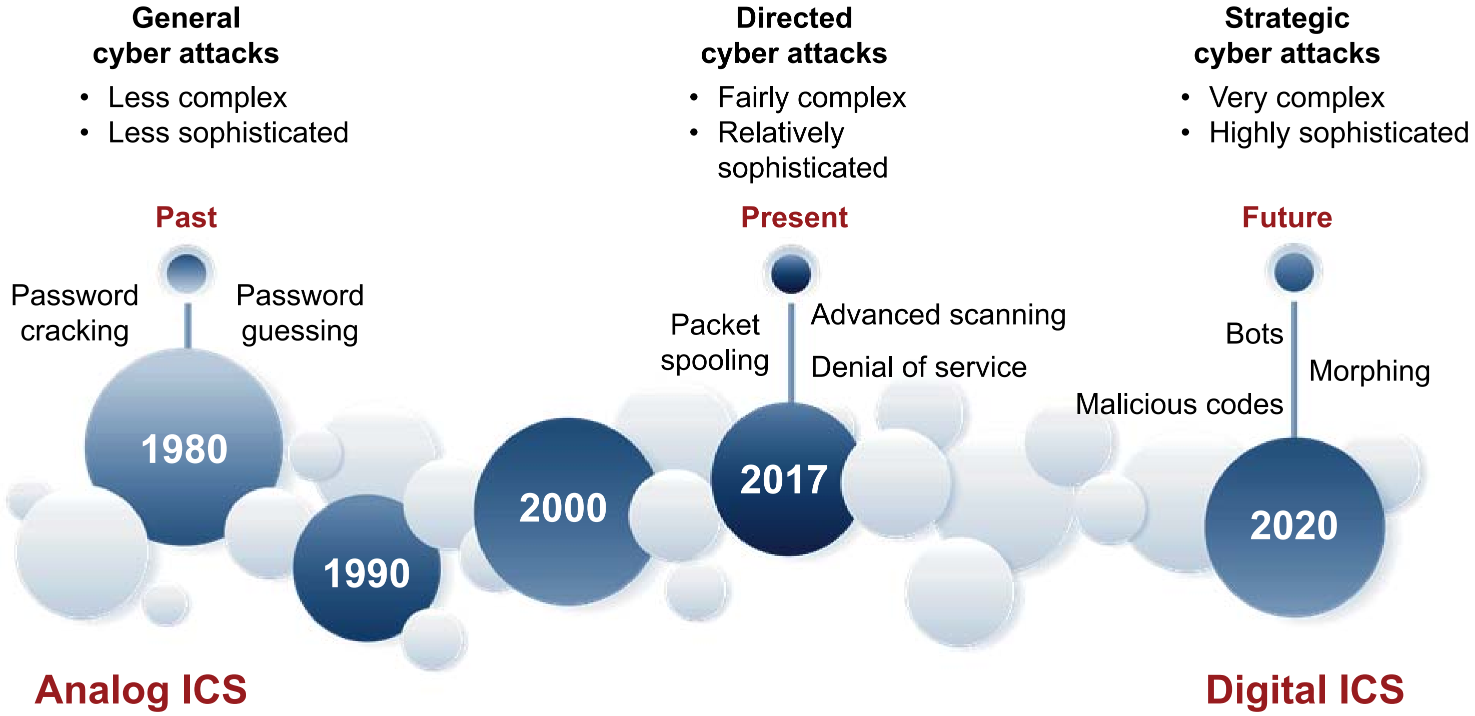
Source: Frost & Sullivan

Whether they are factories producing smartphones or oil and gas refineries, industrial enterprises involve a multitude of devices, systems, assets, and human resources. Traditionally, industrial networking that connected devices and systems was achieved through proprietary protocols. The exclusive nature of these protocols made them isolated and inaccessible for any external intrusion. This natural cyber-attack defense mechanism began to thin down with the ascent and adoption of IP (Internet Protocol)-based communication in industrial environments. For instance, adopting IP-based connectivity between industrial equipment has increased security risks, a fact that has been largely ignored until now. The other development that further expands security risks is the growing use of microprocessors in industrial equipment. This has made industrial control systems (ICS) the most vulnerable assets for attacks in the industrial world.

Legacy ICS systems were designed as isolated best-of-breed solutions with little or no apparent connection to the external environment. However, with the introduction of IP-based communication, isolated control networks began to expand and cross traditional boundaries. The unchecked nature of this expansion has now made it possible for potential third-party intrusions to disrupt ICS through the Internet. Some examples of at-risk ICS systems are programmable logic controllers (PLC), supervisory control and data acquisition (SCADA), distributed control systems (DCS), and intelligent electronic devices (IEDs) (used specifically in the power industry).

In many ways, the Stuxnet event was a wake-up call to an impending industrial need that required industry acknowledgement and planned investment. This attains a greater significance with the increasing complexity and intensity of cyber-attacks that is expected in the future. Exhibit 7 indicates how cyber-attacks have evolved over the years and what the industry is likely to see in the years ahead.

Exhibit 7: Evolution of Cyber-Attacks



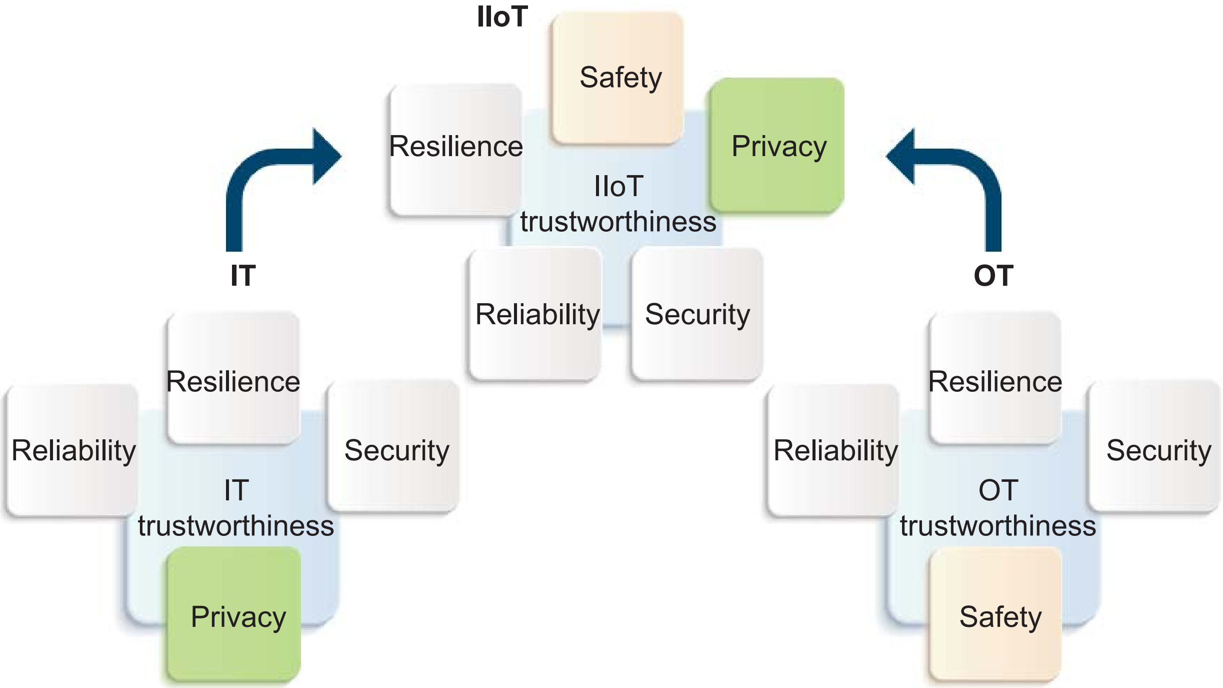
Source: Frost & Sullivan

THE DIFFICULTY IN DEFINING INDUSTRIAL CYBER SECURITY

Defining cyber security, however, has been a major challenge for the industry. Industrial cyber security is primarily about the coming together of the principles of safety from the OT environment and the ideals of security from the IT environment. A lack of clarity in this aspect has made it difficult for end users to understand and identify security as a critical issue that needs systematic investment. The advent of IIoT and digitalization within manufacturing has been helpful in driving a need for clarity on this subject. In this regard, the IIC - a key organization on IIoT that we discussed earlier- has come out with a common industrial security framework called the Industrial Internet Security Framework (IISF). The IISF was designed to enable the convergence of IT's and OT's trustworthiness and sets the architectural framework and direction for the Industrial Internet. The IISF emphasizes the importance of the five characteristics of IIoT: safety, security, reliability, resilience, and privacy.

Trustworthiness for the OT environment implies safety, reliability, and availability of services at all times during the day. This trustworthiness is more about securing the physical safety of the plant under lock and key. On the other hand, trustworthiness for the IT environment implies securing the plant's assets, network, and the data generated by these connected devices. The onus of trustworthiness is higher on the IT environment where the downside of security is very high. With the convergence of these two environments, the definition of trustworthiness has converged as well.

Exhibit 8: Converging IT and OT Trustworthiness in IIoT



Source: Industrial Internet Consortium

In addition, the IISF framework would help manufacturers keep track of risks, assessments, threats, metrics, and performance indicators that guard the security of their organizations. To date, safety has been the first priority in the OT world that includes the safety of human life, plant facilities, and the operating environment. Following safety, reliability and resilience are other related priorities for industrial end-users. Given that current OT systems are not connected, security has not been in the radar of most end-users. In contrast in the IT world, security, privacy, and reliability are extremely important to IT systems. Safety is rarely an issue, and resilience is more of a priority for cases where business continuity is critical.

The IISF comprises the following components, each addressing the different needs and aspects of security for IIoT:

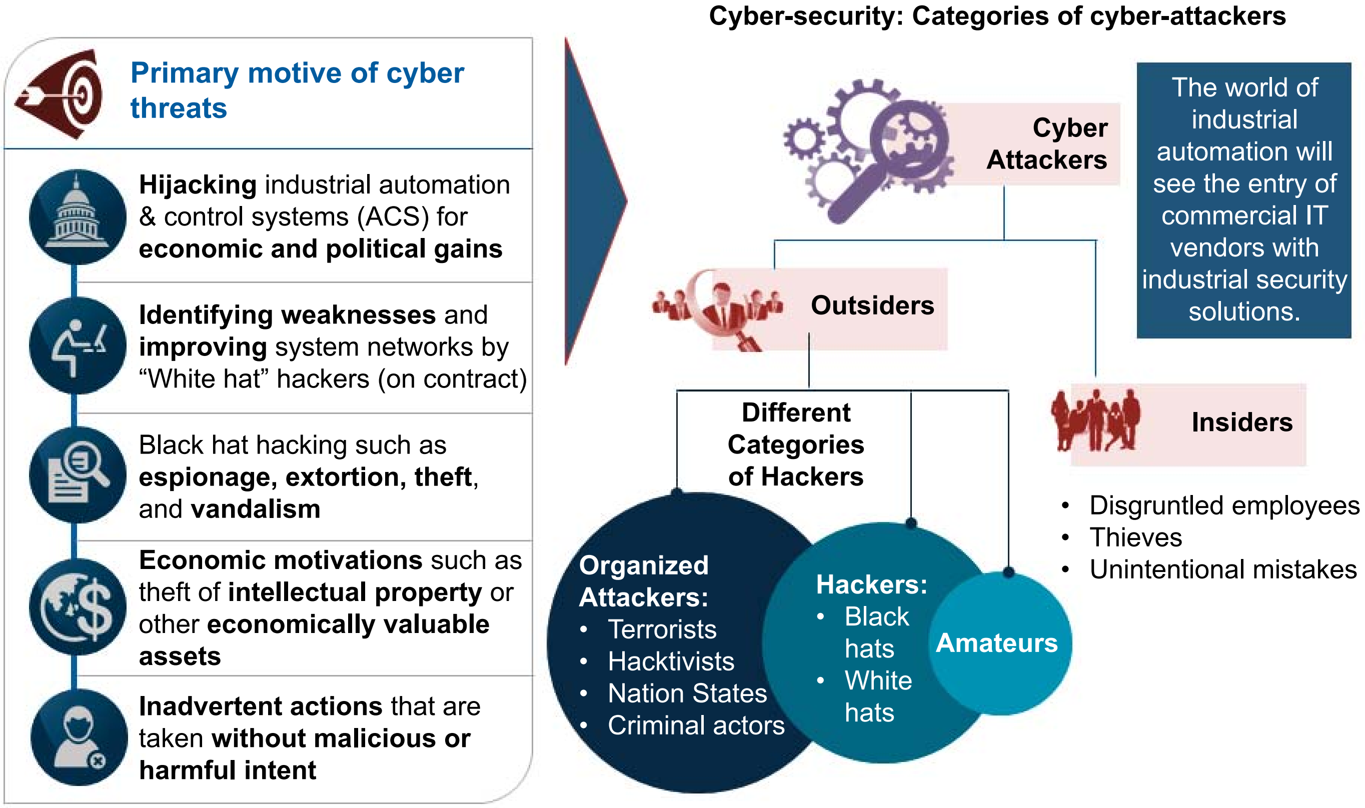
- Introduction of key system characteristics for IIoT and examination of the requirements that make these systems trustworthy.
- Identification, communication, and management of risks associated with security, along with the assessment approach for the security of organizations, architectures, and technologies.
- Definition of best practices for safeguarding endpoints, communication, connectivity, configuration management, and monitoring

Apart from critical IT and OT data, the smart industrial infrastructure (and the environment built around it) is prone to external security threats as well. For example, data centers increasingly use smart infrastructure such as heat, ventilation, and air conditioning (HVAC) equipment; power conditioning; video security; and fire safety systems, all of which are prone to cyber-attacks. These systems are vulnerable points in the industrial infrastructure that can allow black hats to infiltrate an enterprise's confidential data. These attacks could occur either through employee negligence or through intentional damage.

EXAMINING THE CYBER RISK GAP: THE END-USER PERSPECTIVE

The common notion that industrial assets are immune to cyber-attacks if parts of them are isolated from the Internet (or other vulnerable corporate networks) is no longer practical in a hyper-connected enterprise. Although total air gapping of an industrial network is possible, there are several reasons why this may not be a reliable security measure for industrial enterprises. For example, Wi-Fi, Ethernet ports, and USB ports present vulnerable attack surfaces. File transfers between the company and outsiders are inevitable as a hacker can infiltrate the organization's network by installing malicious software through such file transfers. An increasing number of companies are encouraging their employees to adopt the bring-your-own-device (BYOD) trend; however, the probability of a cyber-attack through compromised personal devices is high. Even if an industrial network is completely air gapped, it is still vulnerable to potential threats from accidental or intentional damage from its internal workforce. The only way to control this internal attack vector is by continuously monitoring the network and by implementing rigid access control mechanisms.

Exhibit 9: Cyber-Attacks—Types and Motives



Cyber-security: Categories of cyber-attackers

Primary motive of cyber threats

- **Hijacking** industrial automation & control systems (ACS) for **economic and political gains**
- **Identifying weaknesses** and **improving** system networks by "White hat" hackers (on contract)
- Black hat hacking such as **espionage, extortion, theft**, and **vandalism**
- **Economic motivations** such as theft of **intellectual property** or other **economically valuable assets**
- **Inadvertent actions** that are taken **without malicious or harmful intent**

Cyber Attackers

Outsiders

Different Categories of Hackers

Organized Attackers:
- Terrorists
- Hacktivists
- Nation States
- Criminal actors

Hackers:
- Black hats
- White hats

Amateurs

Insiders
- Disgruntled employees
- Thieves
- Unintentional mistakes

The world of industrial automation will see the entry of commercial IT vendors with industrial security solutions.

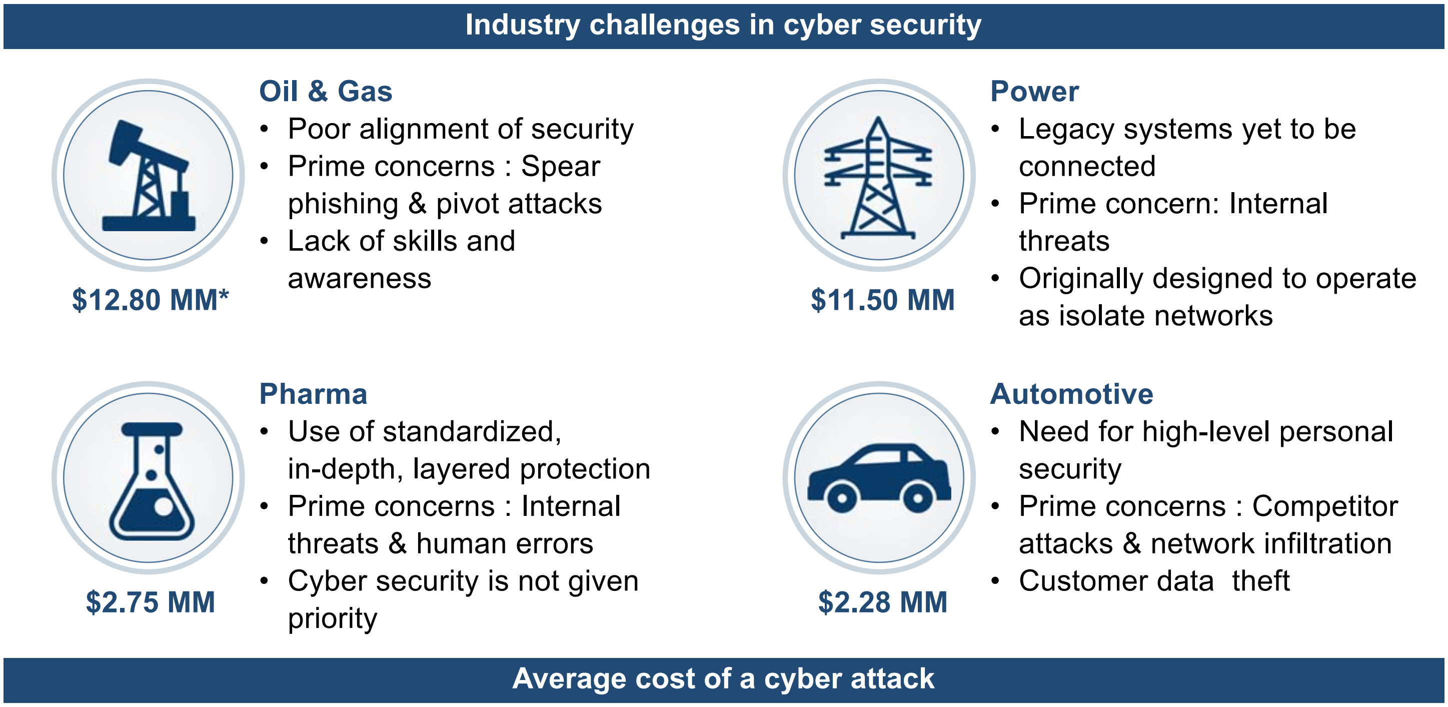
Source: Frost & Sullivan

Traditionally, IT and OT have been two different silos, each operating in its own environment. However, with companies' pursuit to increase operational efficiencies and profit margins, the convergence of IT and OT is inevitable. A converged IT-OT scenario will hence be a major driver for implementing industrial cyber security. Every organization must carefully assess and identify vulnerabilities through which black hats can potentially infiltrate the system. Cyber-attacks are triggered by several sources such as competition, political rivalry, and hostile employees who want to disrupt the plant operations. The most dangerous trigger, however, is state-sponsored attacks, which can have an environmental impact and are specifically intended to create destruction on a massive scale.

Critical infrastructure such as the power grid depends on massive IT networks. Most current cyber defense mechanisms are outdated and vulnerable to potential hacking attempts. The frequency of attacks on critical infrastructure that can potentially cause large-scale destruction has been increasing at an alarming rate.

Even though attacks are spread across the manufacturing industry, data suggests that energy organizations are more prone to these attacks, which have become more sophisticated over the years. At least 75%[4] of companies in the oil and gas and power sectors have experienced one or more successful attacks in the past year. More than 15%[5] of cyber-attacks come from the energy sector. In the past, the energy sector has been targeted in the form of attacks such as Stuxnet, Duqu, Shamoon, and Night Dragon.

Exhibit 10: Internal and External Challenges That Plague Critical Infrastructure



Industry challenges in cyber security

Oil & Gas
- Poor alignment of security
- Prime concerns : Spear phishing & pivot attacks
- Lack of skills and awareness

$12.80 MM*

Power
- Legacy systems yet to be connected
- Prime concern: Internal threats
- Originally designed to operate as isolate networks

$11.50 MM

Pharma
- Use of standardized, in-depth, layered protection
- Prime concerns : Internal threats & human errors
- Cyber security is not given priority

$2.75 MM

Automotive
- Need for high-level personal security
- Prime concerns : Competitor attacks & network infiltration
- Customer data theft

$2.28 MM

Average cost of a cyber attack

**1 MM = 1,000,000 USD*

Source: Frost & Sullivan, HP Enterprise

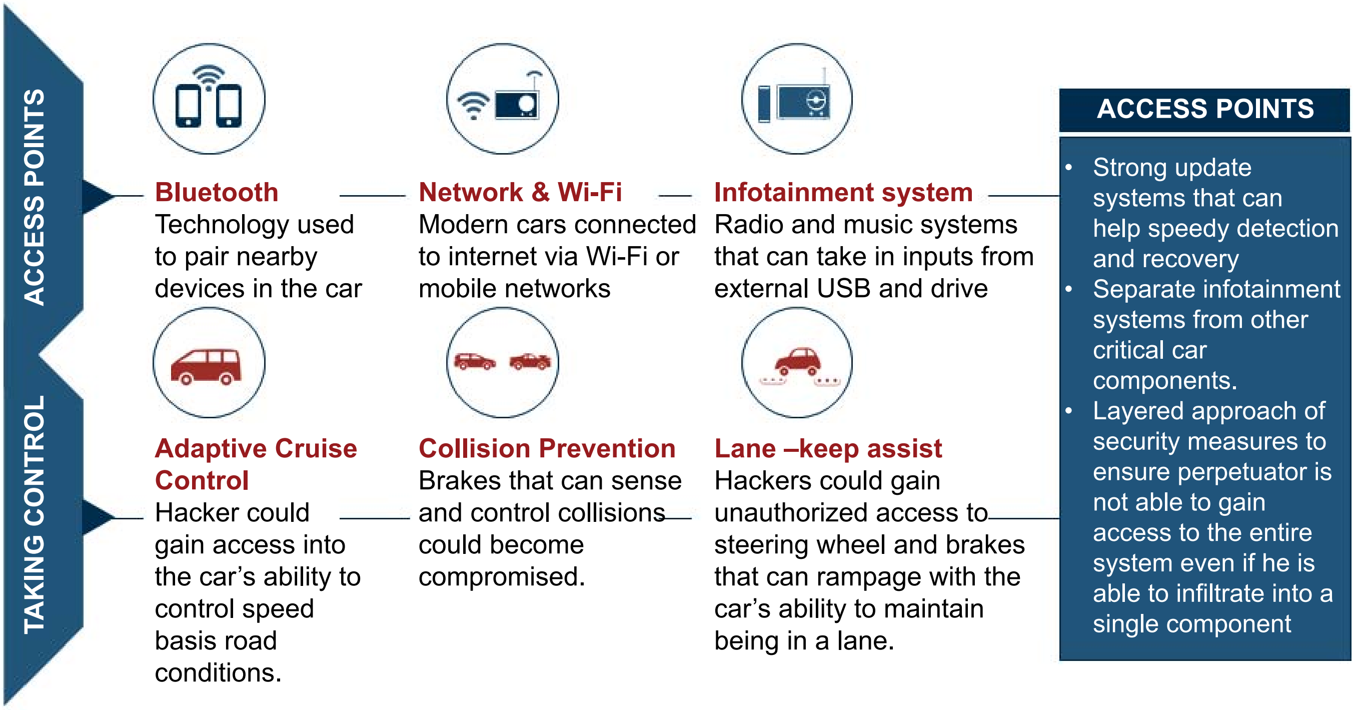
One of the biggest attacks that rang as a wake-up call for the rest of the industry was the infamous Stuxnet attack (which was also referred in the earlier section). This targeted attack on uranium enrichment facilities in Iran was a clear indicator of the potential mayhem that could be caused by cyber-attacks.

The energy sector is not free from generic attacks such as ransomware that locks systems or Trojans that steal financial information. For instance, in 2013, a US based fuel distribution company was victimized by financial fraud worth US$800 million[6]. Every industry has its own vulnerabilities, but an attack on the energy sector can be in particular very severe and expensive. It is therefore extremely important to be aware of industry-relevant policy regulations and be prepared to respond proactively. Globally, the cost of a cyber-attack in the energy sector is second only to an attack on financial services.

Case Example - Ukrainian Power Grid Attack, December 2015 / December 2016
The cyber-attack on the Ukrainian power grid caused a massive power shutdown, affecting a large number of consumers in western Ukraine. The organized attack was carried out with the intent to create maximum disruption. The malware used was directed at the ICS and employed several infiltration techniques such as spear phishing, malware-carrying software documents, and BlackEnergy 3. Gaps in security had arisen from the availability of a company's internal information online and a failure in implementing a two-step authentication framework on its VPN. Despite power returning within a few hours, destructive programs destroyed a great deal of valuable data. Exactly a year later, in December 2016, the Ukrainian power grid was once again suspected to be hacked, leaving the entire city of Kiev in darkness. The attack was suspected as a result of external interference through the data network

An increasing dependence of automotive on technology has opened avenues for cyber threats, predominantly in the motor vehicle industry. Advancements in automotive capabilities continue to forge ahead with connected and driverless vehicles. With an anticipated boom in automotive manufacturing, the incidence and risks for cyber threats is certainly poised to increase in the coming years.

Exhibit 11: Potential cyber-threats in a connected car



ACCESS POINTS

Bluetooth
Technology used to pair nearby devices in the car

Network & Wi-Fi
Modern cars connected to internet via Wi-Fi or mobile networks

Infotainment system
Radio and music systems that can take in inputs from external USB and drive

TAKING CONTROL

Adaptive Cruise Control
Hacker could gain access into the car's ability to control speed basis road conditions.

Collision Prevention
Brakes that can sense and control collisions could become compromised.

Lane –keep assist
Hackers could gain unauthorized access to steering wheel and brakes that can rampage with the car's ability to maintain being in a lane.

ACCESS POINTS

- Strong update systems that can help speedy detection and recovery
- Separate infotainment systems from other critical car components.
- Layered approach of security measures to ensure perpetuator is not able to gain access to the entire system even if he is able to infiltrate into a single component

Source: Frost & Sullivan

It might take several years for manufacturers to actually assimilate a strong security culture within the organization. Increasingly, auto manufacturers are also turning to external security researchers to help identify vulnerabilities ahead of hackers. Tesla, for instance, launched a "Bug Bounty" program to motivate external security researchers to identify weak links in their system.

The pharmaceutical industry is a treasure trove of information that is extremely sensitive and confidential from a business standpoint. Nothing is more vulnerable than the formula of a new drug or highly sensitive patient information. Stolen intellectual property, drug formulae, R&D data, trade secrets, corporate strategies and merger and acquisition information details can literally destroy a pharmaceutical company.

Customer Data Theft in a Niche Pharmaceutical Company, 2015

A big pharma company had a database of more than 50,000 customers compromised by a hacker who demanded a ransom and threatened to sell the data on a common forum to the highest bidder. Cyber-attack techniques such as SQL injection were used to conduct this attack. The compromised data included details such as customers' personal information and DEA numbers. A failure to adopt appropriate encryption techniques was found to be one of the main reasons behind this attack

It is therefore not surprising that pharmaceutical is among the top 3 industry verticals prone to cyber-attacks. Cyber-attacks on the pharmaceutical industry have increased at a faster rate than other industries. According to recent reports, investments in research and development continue to be the mainstay for major pharmaceutical companies. In 2015, the industry spent $92 billion[7] dollars (OECD, 2015) on R&D alone. According to Frost & Sullivan research, more than two-third of the pharmaceutical industry has suffered severe data breaches while the rest have had the experience of being hacked at least once.

Interestingly, cyber threats in a pharmaceutical enterprise are more internal than external. More than two-thirds of recorded IP thefts involve company insiders and not external hackers. Driven by opportunism, revenge, greed or competitive advantage, these insiders exploit their positions to gain access to the company's digital assets. Organizations should actively do their part in securing their digital assets. This can be achieved to a certain extent by educating employees on security and other protocols and ensuring convenient ways for employees to report suspicion. Manufacturers would need to ensure adequate protection of proprietary information and regularly monitor computer networks for suspicious activity. Companies would also need to ensure access to security measures, tools and frameworks for their personnel and ensure that access to company data and the network is revoked for any employee who has left the organization.

Pharmaceuticals must take suitable precautionary measures to protect themselves from cyber-attacks. They should take key steps in identifying potential vulnerabilities in their system and put in place appropriate security measures and policies. A proper response plan and sufficient foresight into how they would handle a potential cyber-attack needs to be in place. Business planning also would need to include a review of internal insurance policies to check to see if this also includes coverage for cyber-attacks.

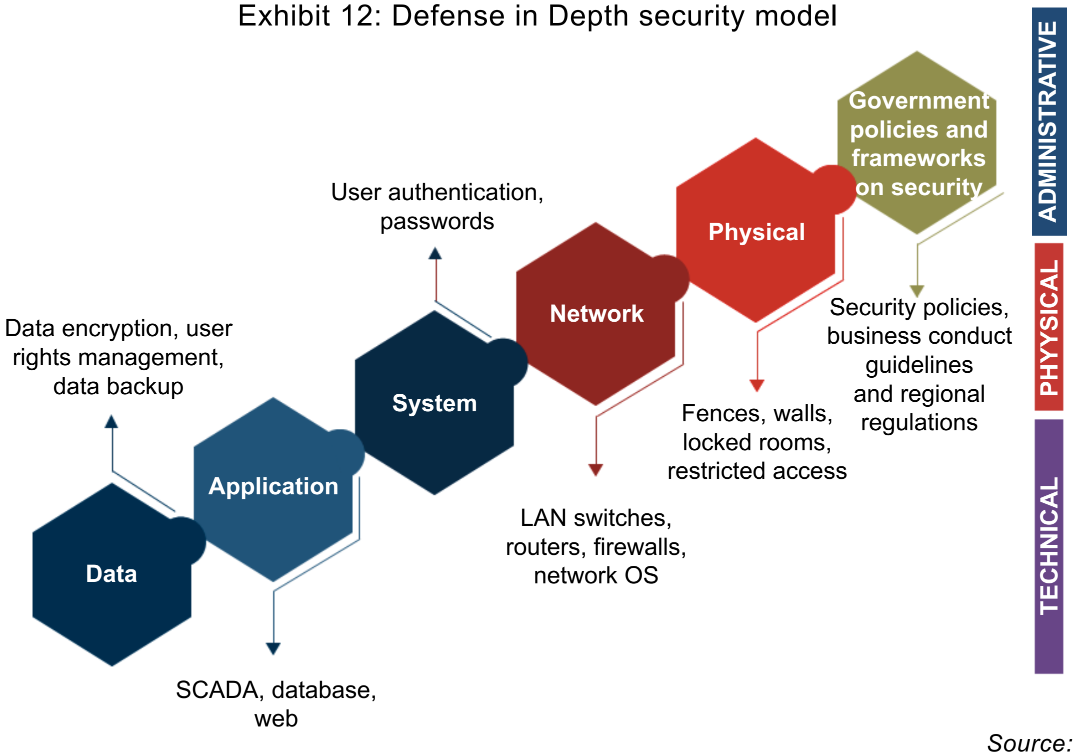
The deeper analysis on the industries of automotive and pharmaceuticals in this section is, but a limited reflection of the cyber security scenarios that plague the manufacturing world. It is possible for us to make such similar analysis on multiple industry verticals. The larger message that we will eventually come to reach is that cyber-attacks are a reality and there is a dire need for all industrial customers to attend to it urgently.

GETTING STARTED WITH INDUSTRIAL CYBER SECURITY

The growing significance of industrial cyber security is a consequence of several security breaches that could happen in a manufacturing environment. These include incidents such as denial of access to systems (DDoS attacks), loss or manipulation of data, large scale disasters that could have a negative impact on the environment and impaired systems and networks. All these security breaches could result in loss of control over production which in turn could lead to revenue loss and damages to brand reputation.

Before applying industrial cyber security within a plant unit, it is imperative that companies understand the different layers of security that need to be applied in order to completely protect a manufacturing plant. In here, we would like to delve on the method of "Defense in Depth" or the "Castle Approach". The Defense in Depth philosophy is aimed at securing multiple aspects of a plant including personnel, procedural, technical and physical. The various layers of security controls include government policies and security frameworks, physical, network, system, application, and data layers as indicated in exhibit 12.

Exhibit 12: Defense in Depth security model


Government policies and frameworks on security
Physical
Network
System
Application
Data
User authentication, passwords
Data encryption, user rights management, data backup
Security policies, business conduct guidelines and regional regulations
Fences, walls, locked rooms, restricted access
LAN switches, routers, firewalls, network OS
SCADA, database, web
ADMINISTRATIVE
PHYSICAL
TECHNICAL

Source: Frost & Sullivan

Adopting defense in depth involves a sequential and conditional approach. The different levels of security adoption include the following.

1. Security measures at the administrative level

These include the laws, regulations, policies, rules and guidelines that govern the informational security practices of the organization. Manufacturers looking to adopt cyber security should look at understanding in detail the cyber security laws and frameworks governing the specific region where the organization is operating.

Common Misconceptions about Cyber Security

- It will not happen to me.
- Not all end points require protection.
- Antivirus and firewalls are sufficient.
- End-point security cannot provide

For instance, the Department of Homeland Security (DHS) has recently issued strategic guidelines that emphasizes on IIoT security. As a mushrooming number of connected devices are increasingly being relied upon by the national critical infrastructure, securing these systems has become a major priority. Manufacturers can adopt these principles as they design, manufacture and use connected systems. These guidelines are extremely important to help industrial enterprises make informed security decisions. The main high-level principles as defined by the DHS include the following:

a. Incorporating security at the design phase - With an intention to maximize profits in less time, manufacturers fail to suitably secure their systems and processes. This leaves room for black hats to manipulate information in the network. The guidelines set by DHS however instruct manufacturers to incorporate these principles of cyber security right from the design stage.
b. Enable security updates and manage vulnerabilities - Legacy industrial machines are still prone to attacks. These vulnerabilities can be addressed by thorough patching, delivering security updates and effective management of vulnerabilities.
c. Employ proven security best practices - Proven and tested security best practices can be the starting point for implementing effective security measures in IT and OT environments.
d. Prioritize security according to impact - Risks arising from cyber threats and the corresponding counter measures vary with the kinds of things being connected to the internet. These security measures would need to be prioritized based upon the intensity and nature of the potential impact.
e. Promoting transparency - Increased transparency and visibility into plant processes can help determine where and how to apply security measures.
f. Careful consideration of connectivity - Industrial enterprises should carefully analyse their businesses and understand whether continuous connectivity is needed considering the risks associated with connectivity.

2. Security measures at the plant (physical) level

Plant security measures can help companies build and maintain a positive reputation among their customers. Improved plant security is also synonymous with improved productivity as it helps prevent unwanted theft or loss of data. This in turn can help in expanding business opportunities. At all times, manufacturing organizations are required to secure the physical aspects of their plant facilities including identifying and monitoring individuals who enter and leave the plant premises. Organizations also need to keep track of movement of industrial assets across the plant floor and supply chain and control access to sensitive areas within the plant facility. They also need to be constantly alert by optimizing response time to potential threats and alarms.

3. Security measures at the technical level

This includes technology components of a cyber-security system that helps in securing connected assets. These include security measures such as firewalls, anti-virus, data encryption, data back-up, user rights management etc. Many IT security vendors offer endpoint protection solutions, but not all of them offer comprehensive security to ICS endpoints and networks. For industrial end-users, any attack on the ICS could mean downtime and hence loss of business. The increasing complexities and intensity of cyber-attacks is driving the need to not just prevent a possible attack, but also to sufficiently predict and pre-empt an attack. In addition, the convergence of IT and OT further necessitates a demand for security solutions that can be applied to legacy infrastructures as well.

INDUSTRIAL CYBER SECURITY- THE VIEWPOINT OF BAYSHORE NETWORKS

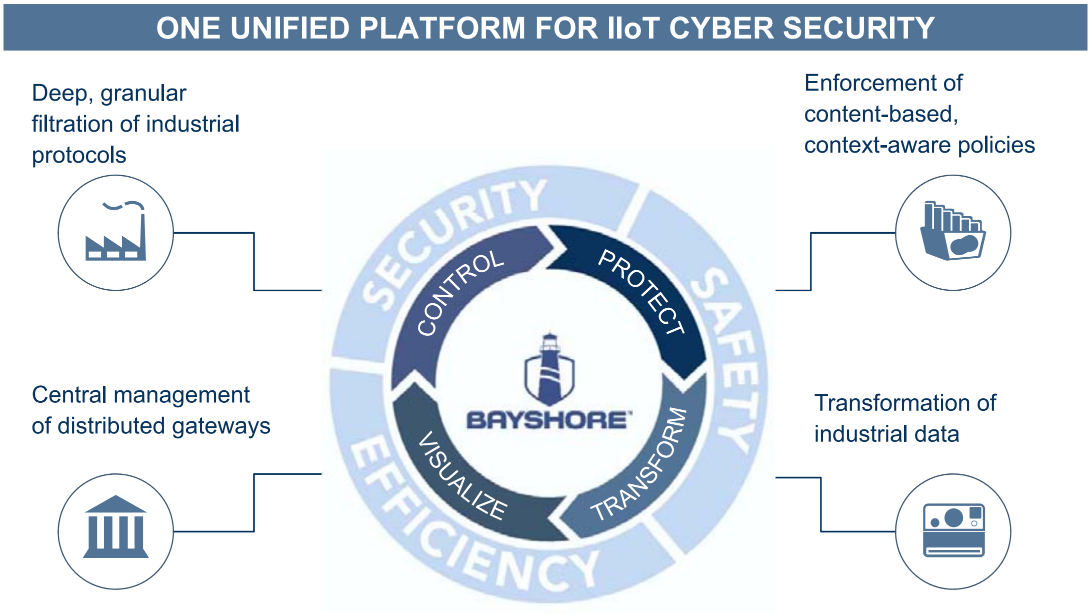
The increasing digitalization of industrial assets is driving the market for industrial cyber security. Popular industrial cyber security software provider Bayshore Networks has been rapidly advancing in this area, and has emerged as a very prominent player in this space. The company's IT/OT Gateway is designed to protect industrial assets in converged IT-OT environments. It currently provides cyber security to several global industrial enterprises and delivers pre-emptive visibility into their OT networks.

Among other security features, the Bayshore gateway performs deep content inspection, granular filtering of network flows, and policy building and enforcement. It also detects, parses, and segments industrial protocols.

Threats to OT are fundamentally different than traditional threats to IT security. Threats to the OT environment can affect aspects such as workforce safety, production downtime, and process disruptions and even inflict physical damage to the plant and assets. Traditional IT security technologies, such as firewalls, were not designed to protect OT environments. The IT security technologies' lack of industrial domain knowledge is one of the major cultural challenges faced by traditional cyber security firms looking to secure industrial assets.

Today's enterprise IT security technologies lack the ability to scale to support huge networks of OT machinery. Furthermore, IT technologies lack the ability to conduct the granular deep packet inspection required to enforce OT policies. They also lack the ability to customize safety and security policies based on established standards and known threat intelligence. In short, IT security technologies are unable to protect machine transactions, which is the common vector for OT cyber-attacks. The following is a example of how these advanced cyber security capabilities can help industrial enterprises overcome potential security threats in their operating environments.

Exhibit 13: The Bayshore Networks' Unified Platform for IT/OT Convergence


ONE UNIFIED PLATFORM FOR IIoT CYBER SECURITY
Deep, granular filtration of industrial protocols
Enforcement of content-based, context-aware policies
Central management of distributed gateways
Transformation of industrial data
SECURITY
SAFETY
EFFICIENCY
CONTROL
PROTECT
TRANSFORM
VISUALIZE
BAYSHORE

Source: Bayshore Networks

The following is an example of how these advanced cyber security capabilities can help enterprises overcome potential security threats in their operating environments.

Case Study - A large automotive manufacturer employs Bayshore Networks for security and safety

The Problem

The manufacturer wanted to create a secure, remote access to multiple production zones. This step was intended for managing unplanned outages remotely which would normally demand the physical/onsite presence of a skilled technician. The traditional method was inefficient, costly and unsecure.

The Solution

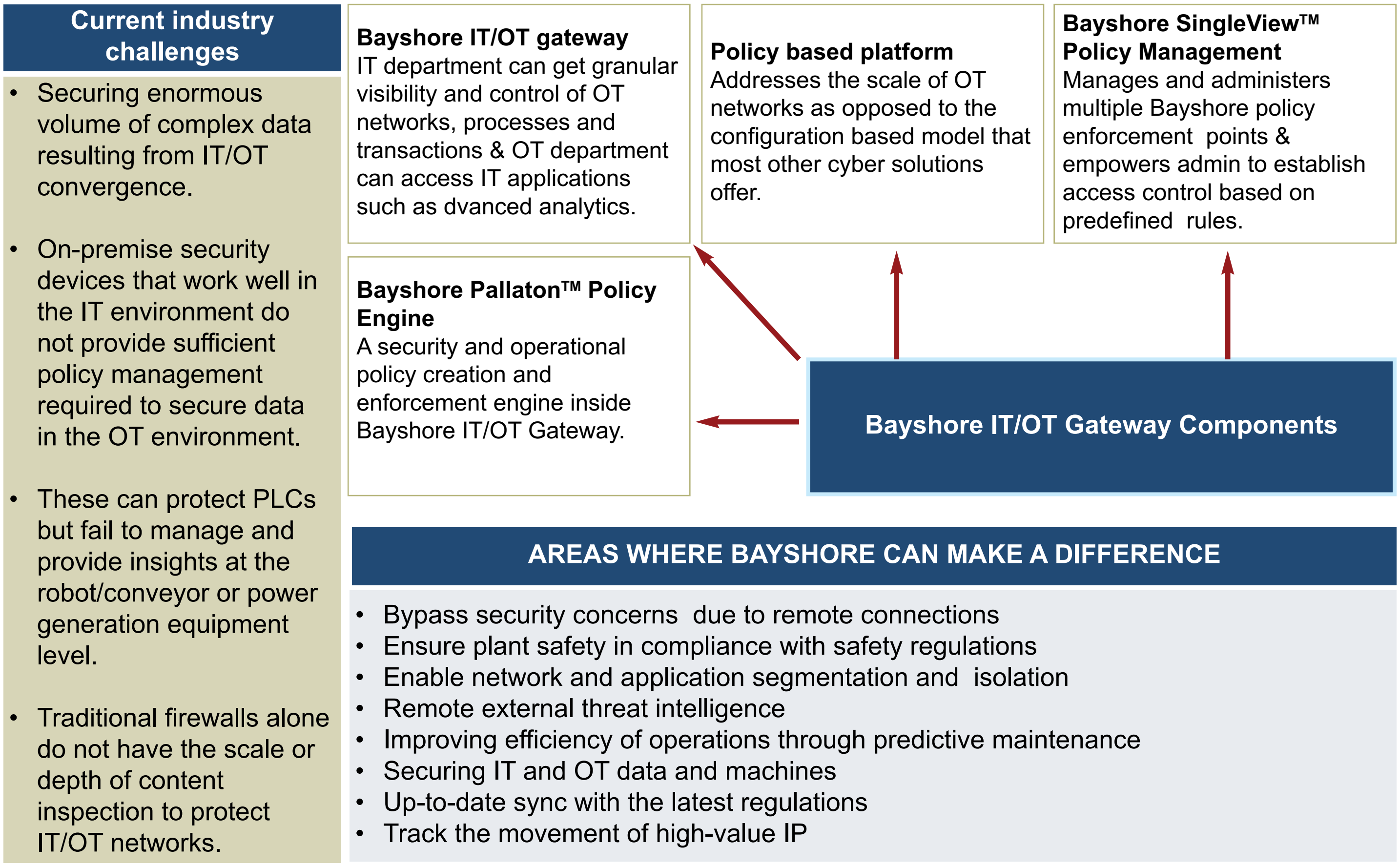
Remote users got line of sight access to assembly line robots to ensure they were managed safely. The implemented solution also prevented unplanned outages that arose out of impactful actions such as human error. In addition, production issues could be managed safely and securely through hand-held devices.

To combat the rising threats against industrial networks, IT and OT personnel need to collaborate closely. The measurement for required outcomes and success between IT and OT need to be aligned, considering security as well as safety from the OT perspective. Vulnerabilities of OT, data centers, building automation, and other relevant areas need to be assessed, and security best practices need to be implemented accordingly to address immediate vulnerabilities in the OT infrastructure. These vulnerabilities will need to be prioritized, and existing security gaps would need to be closed.

Industrial enterprises should seek the support of line of business, IT, and senior management to close these gaps, thus effecting immediate action to put OT security in place, including the capability to track and analyze the traffic on manufacturers' networks. Industrials should look at clearly itemizing their connected devices and establishing stringent baselines for industrial machine behavior. Clear policies need to be set in place to identify aberrations from the desired outcomes of machine performance.

Third-party views on security from IT/OT security experts such as Bayshore Networks is quite insightful in this regard. With their experience in IIoT security technology implementations, such experts can help provide cyber security, safety, and operational policies as well as safeguard plants from potential rogue programs and threats.

Exhibit 14: Facing Industry Challenges - The Bayshore Approach



Current industry challenges

- Securing enormous volume of complex data resulting from IT/OT convergence.
- On-premise security devices that work well in the IT environment do not provide sufficient policy management required to secure data in the OT environment.
- These can protect PLCs but fail to manage and provide insights at the robot/conveyor or power generation equipment level.
- Traditional firewalls alone do not have the scale or depth of content inspection to protect IT/OT networks.

Bayshore IT/OT gateway
IT department can get granular visibility and control of OT networks, processes and transactions & OT department can access IT applications such as dvanced analytics.

Policy based platform
Addresses the scale of OT networks as opposed to the configuration based model that most other cyber solutions offer.

Bayshore SingleView™ Policy Management
Manages and administers multiple Bayshore policy enforcement points & empowers admin to establish access control based on predefined rules.

Bayshore Pallaton™ Policy Engine
A security and operational policy creation and enforcement engine inside Bayshore IT/OT Gateway.

Bayshore IT/OT Gateway Components

AREAS WHERE BAYSHORE CAN MAKE A DIFFERENCE

- Bypass security concerns due to remote connections
- Ensure plant safety in compliance with safety regulations
- Enable network and application segmentation and isolation
- Remote external threat intelligence
- Improving efficiency of operations through predictive maintenance
- Securing IT and OT data and machines
- Up-to-date sync with the latest regulations
- Track the movement of high-value IP

Source: Bayshore Networks

Bayshore's patented IT/OT Gateway deploys from the cloud, as a virtual machine, or as an on-premise hardware appliance. The Gateway can protect industrial enterprises from potential cyber-attacks and can block attacks on OT assets that arise from internal or cloud-based sources. The Gateway can identify in advance the signs of any targeted or known attacks and provide suitable protective measures.

Bayshore software can suitably provide end-to-end visibility into the OT infrastructure, networks, applications, machines, and operational processes. The company's deep content inspection capabilities can help industrial enterprises detect security flaws across their networks. Bayshore follows a policy-based approach in securing industrial assets and builds this policy from various sources such as internal research; customer-set rules; trusted external sources such as ICS-CERT, OWASP, and STIX/TAXII; and established cyber-attack vendors and service providers.

Case Study - Overcoming Challenges in Securing the Oil and Gas Industry

The Problem

- Limited visibility into oil & gas operational data
- Safety and security concerns of industrial data, assets, and workforces
- System upgrade management
- Identification of process disruptions

The Solution

- Granular inspection of content and filtering of data
- Secure remote access to production zones
- Network and data segmentation and isolation
- Secure policy-based OT automation at the process level

Security continues to be the topmost challenge in the digitalization of industrial assets; however, the notion and value of securing these assets differ from organization to organization. As an increasing number of companies realize the importance of cyber security, they have rising concerns over tapping the return on investment (ROI) from these implementations.

Bayshore's in-depth understanding of the industrial environment and protocols could help enterprises overcome industrial security concerns and derive benefits that can help improve overall operational efficiency.

CONCLUSION

Industrial cyber security has been growing steadily in perception over the last two decades. Since the Stuxnet event in 2010, the industry has begun to acknowledge the lack of adequate attention that this topic rightfully deserves. In its current state, with the advent of new techno-business themes like IIoT, cyber security is set to take on a new dimension, necessitating a more rigorous and robust approach.

This white paper highlights how cyber security has evolved over the years and is growing to become the lynchpin of a connected enterprise. To establish this viewpoint, a holistic content approach has been pursued that includes shedding light on major policy-led initiatives (e.g., IIC), highlighting key industrial security incidents, and the changing demands of cyber security in a converged IT-OT scenario. A key outcome of this paper is to assert the increasing significance of cyber security for manufacturing and process industries that are undergoing a new wave of digitalization. In particular, with the advent of connectivity between devices, assets, processes and people, the boundaries that once separated safety and security are beginning to blur. Industrial cyber security is thus growing in complexity and becoming an inevitable strategic necessity for end-users across all industries.

We have also tried to ensure that our analysis in this paper had specific outcomes. As a result, the latter part of this white paper has been entirely devoted to articulating and exploring the best cyber security approach that industrial customers need to establish within their operating environments. This involved a deep dive into the concept of Defense-in-Depth and its implications for a converged IT-OT environment in the future. In an attempt to further validate and substantiate our analysis, we sought the example of the security approach from Bayshore Networks. According to Frost & Sullivan, Bayshore's value-proposition involves a comprehensive approach to the emerging security needs of the industry. In essence, we firmly believe that cyber security will finally get its due from the industrial world. The dawn of new digitalization narratives like IIoT will be singularly responsible for pushing this topic beyond boardroom discussions and making it a tangible, real and quintessential part of industrial infrastructure in the years to come.

References

1. This data point has taken into account a number of different elements that constitute IIoT. Research indicates that many existing manufacturing companies have already adopted elements of IIoT, such as advanced data-based services and Ethernet-based devices for example

2. https://www.iiconsortium.org/members.htm

3. http://opcconnect.opcfoundation.org/2016/12/opc-ua-for-120-million-devices/

4. From Frost & Sullivan Research

5. http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/targeted_attacks_against_the_energy_sector.pdf

6. https://www.sans.org/reading-room/whitepapers/analyst/practical-threat-management-incident-response-small-medium-sized-enterprises-35257

7. http://www.oecd-ilibrary.org/docserver/download/8115071e.pdf?expires=1485496655&id=id&accname=guest&checksum=0C2397C7A203BF7E08751DCB90B2A3D3

DISCLAIMER

The following materials were prepared by Frost & Sullivan. Frost & Sullivan does not make any representations or warranties to any third party with respect to the information contained in this report. While reasonable steps have been taken to ensure that the information in this report is correct, Frost & Sullivan does not give any warranty or make any representation as to its accuracy and do not accept any liability for any errors or omissions. The study should not be used or relied upon by anyone without independent investigation and analysis and Frost & Sullivan will not assume any liability for any such use or reliance by third parties. Any trademarks and other service marks contained in this document are the property of respective owners and may not be used without their prior written permission.

FROST & SULLIVAN

NEXT STEPS

SCHEDULE A MEETING WITH OUR GLOBAL TEAM TO EXPERIENCE our thought leadership and to integrate your ideas, opportunities and challenges into the discussion.

Visit our Digital Transformation web page.
Interested in learning more about the topics covered in this white paper?
Call us at **877**.GoFrost and reference the paper you're interested in.
We'll have an analyst get in touch with you.

Visit our **Digital Transformation** web page.

Attend one of our **Growth Innovation & Leadership (GIL)** events
to unearth hidden growth opportunities.

Auckland
Bahrain
Bangkok
Beijing
Bengaluru
Buenos Aires
Cape Town
Chennai
Dammam
Delhi
Detroit
Dubai
Frankfurt
Herzliya
Houston
Irvine
Iskander Malaysia/Johor Bahru
Istanbul
Jakarta
Johannesburg
Kolkata
Kotte Colombo
Kuala Lumpur
London
Manhattan
Mexico City
Miami
Milan
Moscow
Mountain View
Mumbai
Oxford
Paris
Pune
Rockville Centre
San Antonio
São Paulo
Seoul
Shanghai
Singapore
Sydney
Taipei
Taiwan
Tokyo
Toronto
Valbonne
Warsaw
Washington DC

Frost & Sullivan, the Growth Partnership Company, works in collaboration with clients to leverage visionary innovation that addresses the global challenges and related growth opportunities that will make or break today's market participants. For more than 50 years, we have been developing growth strategies for the Global 1000, emerging businesses, the public sector and the investment community. Is your organization prepared for the next profound wave of industry convergence, disruptive technologies, increasing competitive intensity, Mega Trends, breakthrough best practices, changing customer dynamics and emerging economies?

For information regarding permission, write:
Karthik Sundaram
Program Manager, The Industrial Internet of Things
P : +49 (0)69 77033 44
E : KarthikS@frost.com