50 Years of Growth, Innovation and Leadership

Securing with Trust to Achieve Cybersecurity Peace of Mind

The imperative for cybersecurity in industrial markets

A white paper by Frost & Sullivan

FROST & SULLIVAN

CONTENTS

EXECUTIVE SUMMARY

Cybersecurity: A New Mandate for Manufacturing

Digital is striking a creative expansion of traditional processes and business models. As every industrial market undergoes tectonic transformation, the genesis lies in connecting assets, collecting data and driving outcomes from them. The value creation linkage from data sources to dashboard visualization is critically important for enterprises of the future, but an often overlooked aspect in this value chain is cybersecurity.

Piecemeal approaches implemented today are myopic in nature and the industry needs to change to embrace a rich and deep plant-wide security posture. The imperative that lies before the industry is to be better informed about the ways the markets are changing and how to better embrace that change successfully. The paper explores best-in-class solution provider Baker Hughes (BH), which brings forth a comprehensive suite of technology offerings and services while providing a trusted roadmap to securing enterprises of the future.

In an effort to catalyze industry adoption of best-in-class practices, we have put together a paper that outlines the following:

- The Cybersecurity Imperative
- Introduction—Technology Transformation
- The New Cyber Landscape
- Strategic Rationale & Operational Benefits
- Roadmap for a Secure Future

1. INTRODUCTION: TECHNOLOGY TRANSFORMATION

Shifts in Technology/Shifts in Security

The traditional separation between the information technology (IT) and the operational technology (OT) functions is disappearing rapidly with the introduction of industrial internet of things (IIoT). As a result, there is a narrowing gap between industrial safety and information security in industrial processes. Industrial firms are connecting more and more legacy OT assets (e.g., control systems) to IT technologies in the name of operational efficiency and business performance enhancement.

As OT and IT functions merge, the data architecture requirements of IT have become integrated with OT asset needs for system availability, operational safety, and cybersecurity. Legacy assets are at the epicenter of this convergence. Legacy assets control critical operational processes, but their aptitude for cybersecurity within the IIoT world is often lacking. OT/IT teams typically work together to refresh legacy control systems with suitable capabilities needed for protection in the digital world. However, the application of new capabilities and solutions must be performed securely to avoid additional risk to safety, productivity, and quality.

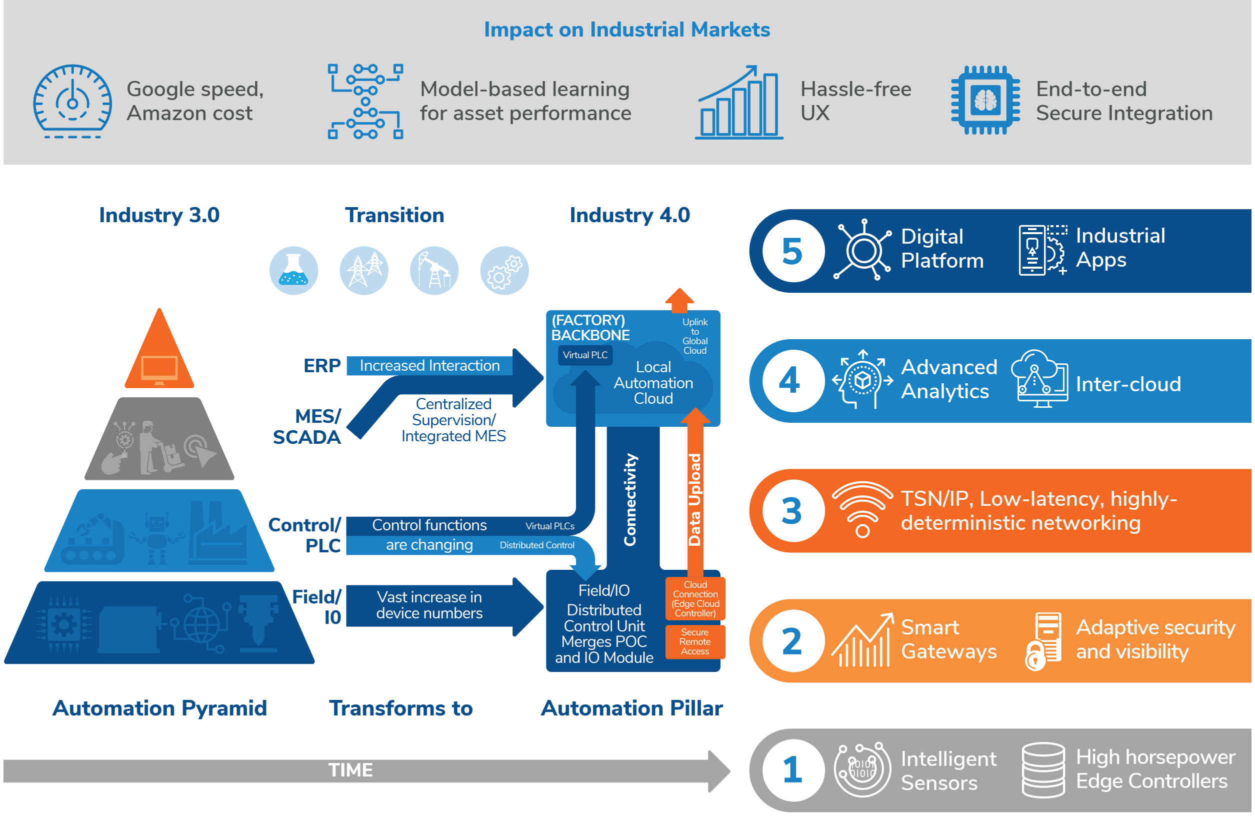
> “OT/IT teams typically work together to refresh legacy control systems with suitable capabilities needed for protection in the digital world.

Integration and scale issues are but speed bumps for organizations on the path to manufacturing transformation. Business cases across verticals worldwide are demonstrating the powerful potential of OT/IT convergence and highly valuable benefits for industrial firms. For example, within the oil & gas industry, upstream firms have optimized operations by analyzing data from diverse sources—from drilling factors to geological maps. Data-enabled infrastructures have also facilitated greater network reliability and innovative commercial opportunities for midstream pipeline and storage firms.

Organizations will continue to implement new technologies, capabilities, and solutions to leverage their data sources and drive value creation through optimization. OT/IT convergence has enabled a connected world, stretching across geographies, individuals, and machines. In the process, the organization's traditional pyramid architectures have shifted to pillar architectures (Exhibit 1).

EXHIBIT 1: TECHNOLOGY TRANSFORMATIONS

Purdue model (ISA-95) gives way to "Pillared" model. Five key transformations enabling a smarter future.


Impact on Industrial Markets
Google speed, Amazon cost
Model-based learning for asset performance
Hassle-free UX
End-to-end Secure Integration
Industry 3.0
Transition
Industry 4.0
ERP
Increased Interaction
MES/ SCADA
Centralized Supervision/ Integrated MES
Control/ PLC
Control functions are changing
Virtual PLCs
Distributed Control
Field/ IO
Vast increase in device numbers
(FACTORY) BACKBONE
Virtual PLC
Local Automation Cloud
Uplink to Global Cloud
Connectivity
Data Upload
Field/IO Distributed Control Unit Merges POC and IO Module
Cloud Connection (Edge Cloud Controller)
Secure Remote Access
Automation Pyramid
Transforms to
Automation Pillar
TIME
5
Digital Platform
Industrial Apps
4
Advanced Analytics
Inter-cloud
3
TSN/IP, Low-latency, highly-deterministic networking
2
Smart Gateways
Adaptive security and visibility
1
Intelligent Sensors
High horsepower Edge Controllers

Source: Frost & Sullivan, Industry Analysis

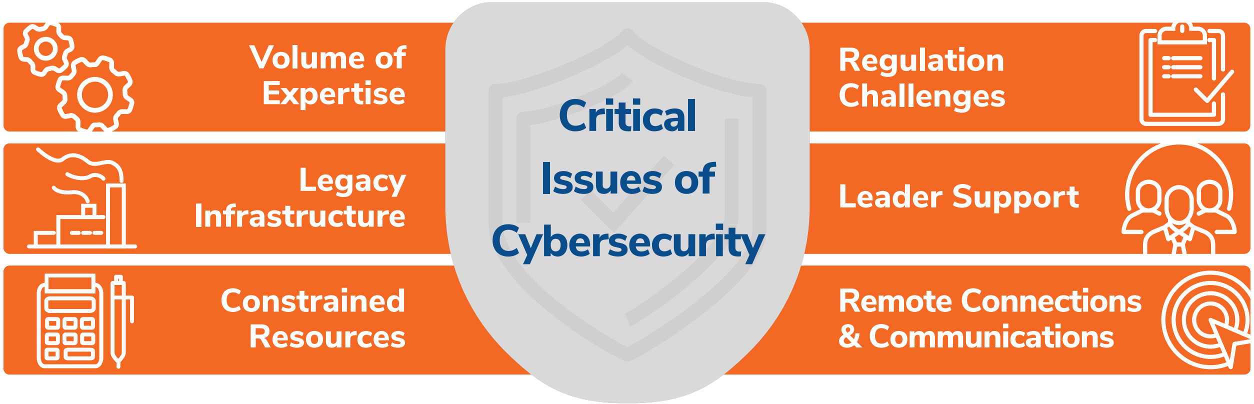
While such connections have helped us become smarter, stronger, and more productive, they have also created new vulnerabilities—both known and unknown. Technology transformations have created an attractive landscape for cyber-attackers as the complexity of IT infrastructure increases alongside steep growth for internet penetration of individual users. Thus, security for the connected IIoT world must be agile, regenerative, and digital.

Critical Issues: Risk & Connectivity

Despite new and widening cybersecurity needs of IIoT environments, many industrial control system (ICS) infrastructures are not sufficiently protected against cyber threats. Such insecurity is caused by a mismatch between the original ICS function and modern digital requirements. Process equipment and control systems, historically run by remote networks, are now based on internet technology, and no industrial vertical has been immune to the connectivity revolution of IIoT. The ICS was designed prior to the digital era to manage and monitor physical industrial processes. For instance, oil pipelines and refineries deeply depend on industrial control systems to ensure operations run smoothly without interruption.

Now, however, the purpose of an ICS is twofold. Not only must an ICS provide reliable and safe real-time operation with maximum uptime, it must also shield against cyber threats. As organizations respond to the new, dual role of ICS, they will encounter several critical issues (Exhibit 2).

EXHIBIT 2: CRITICAL ISSUES OF CYBERSECURITY



Source: BH; Frost & Sullivan

1. Volume of expertise. Organizations are often uncertain of their specific vulnerabilities, related cybersecurity needs, and which solution will best address key problem areas. Their lack of clarity is compounded by a vast marketplace of available cybersecurity solutions. Navigating the sea of potential partners can be challenging, especially if an organization does not have a clear understanding of its current cybersecurity posture and level of risk exposure.

2. Legacy Infrastructure. Frost & Sullivan research indicates the relative shelf asset life cycle of controllers is approximately 15 years, and the average age for most industrial control environments today is an estimated 20 years. Obsolescent legacy infrastructures have not commonly been refreshed or hardened with cybersecurity capabilities or solutions. This creates vulnerabilities that can be targeted by cyber-attacks or exacerbated by human errors. Industrial processes can be negatively impacted by a range of factors from buffer overflows to untimely patches to lax password management policies.

3. Constrained resources. Organizations may have limited resources available for assessing vulnerabilities and applying adequate solutions to meet their cybersecurity needs. There is also a sizeable talent gap as industrial firms can find it difficult to procure qualified analysts with skills needed to design, implement, and maintain IT/OT systems of critical infrastructures.

4. Regulation challenges. There is a multitude of regulatory agencies and standards across industries and geographies. Organizations must first map which standards to adhere to and understand the key benefits of compliance.

5. Leader support. Although there is a clear need for cybersecurity, business leaders can often be uncertain of where and how to begin implementing applications and solutions. Key drivers for enabling leader support on cybersecurity include managing risks, protecting assets, maintaining value for shareholders, avoiding media scandals, and meeting regulatory and compliance targets.

6. Remote connections & communications. The need to leverage production data has caused a shift in connectivity requirements for organizations. Assets, which were once physically separate from networks, are now connected remotely to potentially vulnerable IT systems. For example, more and more oil & gas organizations use remote operations from an onshore location or nearby platform via shared computer networks. The practice is potentially exposing production equipment to network-related vulnerabilities.

Challenges in Securing ICS with a Traditional Approach

Traditional defensive tactics can be ineffective in an IIoT environment for two key reasons. First, they are often not executed with a high level of consistency—even when firms confront external and internal audits. Second, the application of such tactics can be limited. Consider restricted access through mechanized locks. Such measures may be circumvented digitally by highly sophisticated third parties or by malicious internal employees with access to key passwords or codes. Organizations can address their vulnerabilities and strengthen their cybersecurity responsiveness by implementing integrity assurance solutions to enable a deeper and broader level of security. The ideal approach for ICS cybersecurity is a layered approach, where commonly occurring attacks are blocked and responses are modulated as needed for sophisticated and evolving threats.

2. THE NEW CYBER LANDSCAPE

Key Terms & Definitions

To create a well-rounded defense, organizations must first comprehend the cyber landscape. There are several key terms to understand when discussing digital security, including threats, vulnerabilities, and events.

- **Threats** include anything with the potential to harm a network system and its infrastructures. Threat actors (e.g., individual hacktivist or nation state) execute cyber-attacks and possess a variety of different motivations and capabilities.

- **Vulnerabilities** are security inadequacies or flaws inherent to a system, network, or asset. These weak points are targeted and leveraged by threat actors to produce undesirable outcomes. A firm's vulnerabilities stem from its technology, people, processes, and agilities (e.g., an inability to detect cyber-threats, weak authorization protocols, or interconnections with external entities).

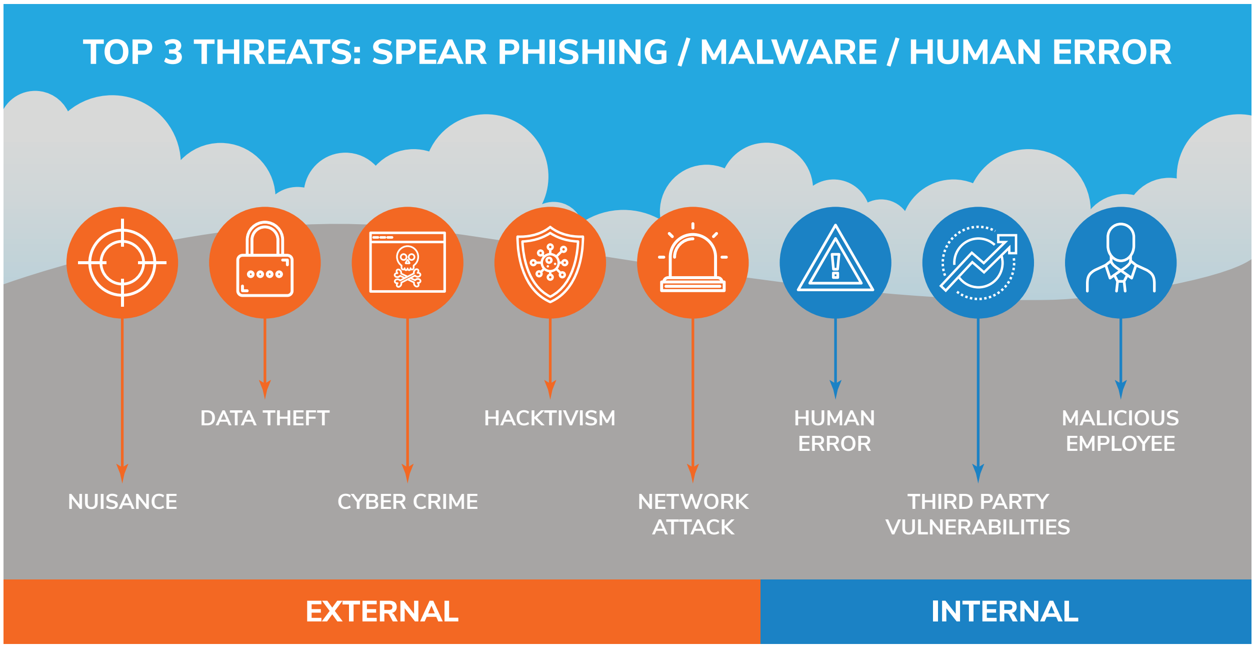
- **Events** are defined by the National Institute of Standards and Technology (NIST) as "any observable occurrence in a system or network." Normal, non-disruptive events include routine activity on a network (e.g., email correspondence). Adverse events, however, include undesired or unauthorized activities (e.g., data access, distribution, or extraction by an unapproved user).

According to the US Department of Homeland Security (DHS), cybersecurity risk transpires when a threat manipulates a vulnerability to cause an adverse event with the end goal of negatively altering an organization or its network.

Threat Landscape

Organizations across verticals are struggling to sustain minimal cyber resilience and ensure cybersecurity in the IIoT environment; as a result, public scrutiny of ICS security policies has risen in recent years. Syndicated reports worldwide indicate lack of cyber-preparedness and a significant increase in frequency of attacks on critical infrastructures. For instance, a 2016 US DHS report named 290 incidents of cyber invasions or breaches with 63 in Critical Manufacturing and 59 in Energy. In 2019, the US power grid is struck by a cyber or physical attack every one in four days. As shown in Exhibit 3, firms confront both external and internal threats from eight major sources.

EXHIBIT 3: THREAT LANDSCAPE



Source: BH; Frost & Sullivan

A single weak security point creates an opening for would-be cyber-attackers to access a plant (e.g., pipelines, refineries, and other critical infrastructure) and its sensitive data. Because hacktivists pinpoint digital security vulnerabilities with increasingly sophisticated precision, organizations must continually adapt their ability to respond to cyber-threats. Unfortunately, most organizations merely react once a security breach has already occurred, and this is suboptimal. Detecting and preventing cyber-attacks is far more cost-effective for organizations than taking corrective actions after the fact as a host of adverse outcomes are possible through cyber-attacks. While it is impossible to address all cyber risk, organizations must make informed decisions on which threats are most likely and optimize resource allocation to effectively reduce risk. According to Frost & Sullivan research, the top three threats impacting organizations today include spear phishing, malware, and human error (Exhibit 3). Likelihood is a key part of the cybersecurity equation, but consequences of risks must also be determined. Industrial control systems often manage critical infrastructures (e.g., power generation, oil & gas or industrial equipment). The side effects of a critical infrastructure failure or corruption could be detrimental for individuals, organizations, economies, and environments.

Although the impact of cyber-attacks depends on the severity and source, potential consequences may include:

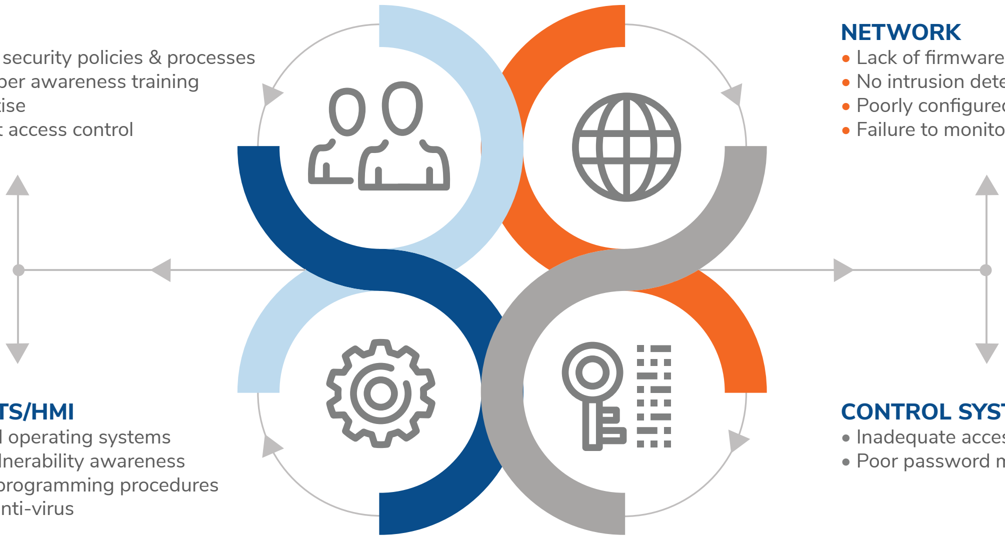
- Loss of information (sensitive and/or proprietary).
- Loss of public trust.
- Plant closure or failure.
- Operational interruption (e.g., utilities outages).
- Production circle stoppage.
- Inferior product quality.
- Undetected performance errors (e.g., oil spills).
- Equipment destruction.
- Foregone safety protocols (resulting in injuries, deaths, and/or environmental damages).

Cybersecurity is needed to assure security across all levels of plant operations. The workforce, plant processes, technical systems, and physical systems must all be evaluated as Frost & Sullivan studies indicate most cybersecurity events of the past occurred because of lack of awareness across the organization.

Key Areas of Vulnerability to Address

There are four key areas organizations can address for the greatest impact on cyber posture: people, networks, endpoints, and control systems (Exhibit 4).

EXHIBIT 4: AREAS OF VULNERABILITY



PEOPLE
- Ineffective security policies & processes
- Limited cyber awareness training and expertise
- Insufficient access control

NETWORK
- Lack of firmware updates
- No intrusion detection
- Poorly configured firewalls
- Failure to monitor & log

ENDPOINTS/HMI
- Unpatched operating systems
- Limited vulnerability awareness
- Unsecure programming procedures
- Obsolete anti-virus

CONTROL SYSTEM
- Inadequate access control
- Poor password management

Source: BH; Frost & Sullivan

As the interconnectivity of devices, systems, and enterprises mushrooms, organizations must address each connected point. The goal is to minimize the potential exposure to operational processes and mitigate additional risk when possible. A layered approach will lessen the likelihood of vulnerabilities.

Agency Resources and Capabilities

In response to the growing number of ICS cybersecurity incidents, agencies developed structured guidelines for organizations. Their standards moderate trade-offs between safety, availability, integrity, and data confidentiality. Exhibit 5 contains a table overview of key agencies and corresponding policies in the United States.

EXHIBIT 5: KEY REGULATORY AGENCIES & STANDARDS

AGENCY	STANDARD	DESCRIPTION
National Institute of Standards and Technology (NIST)	NIST ICS Supplemental Guidance	• Supplementary material on the appropriate application of security controls and control enhancements to ICS environments. • Contains information on specific security controls or control enhancements and their corresponding ICS applications.
National Institute of Standards and Technology (NIST)	NIST ICS Enhancements	• Outlines instructions for refreshing legacy controls - an essential requirement for most industrial control systems.
National Institute of Standards and Technology (NIST)	NIST ICS Enhancement Supplemental Guidance	• Provides directions on control enhancements and how to apply them successfully within ICS environments.
National Institute of Standards and Technology (NIST)	NIST ICS Risk Management Framework (Special Publication 800-53)	• Delineates key security-control selection procedures for federal information systems • Contains a corresponding framework for security requirements found in Federal Information Processing standard (FIPS) 200. • Defines how firms set primary baseline security controls in accordance with FIPS 199 worst-case impact analysis. • Standardizes security control policies and balances security controls with organizational risk assessments for seventeen featured areas (e.g., incident response, access control, disaster recovery, and business continuity).
International Electrotechnical Commission (IEC)	IEC 62443	• Forms standard process criteria for the safe introduction of products used in industrial automation and control systems. • Diagrams a secure development life cycle (SOL) for the creating and sustaining of secure products. • Defines parameters for secure design, implementation, coding, verification, validation, deficiency management, patch management, and product end-of-life. • Guides emerging or existing processes for advancing, conserving, and withdrawing hardware.
North American Electric Reliability Corporation (NERC)	NERC-CIP v3-6	• Sets security criteria for electric infrastructure and corresponding operational assets in North America. • Establishes accountability for guarding against compromises preceding the mismanagement or volatility of the bulk electric system (BES). • Outlines 9 standards and 45 requirements for safely and defense critical cyber assets. • Plans for personnel and training, security management controls, and disaster recovery.
Nuclear Energy Institute (NEI)	NEI 08-09	• Defines cybersecurity plan for nuclear power reactors. • Guides the application of requirements in the Code of Regulations 10 CFR 73.54 (“Protection of digital computer and communication systems and networks at nuclear sites”). • Provides information on how organizations can attend to peripheral access control, inspections, event responsibility, event reaction management, and system integrity concerns.

Source: NIST; IEC; NERC; NEI; Frost & Sullivan

Variance across Standards & Geographies

Although cybersecurity challenges impact organizations across verticals and geographies, strategic responses to them vary. A firm’s cyber posture or responsiveness is normally dictated by the amount of regulation present in its sector. Government regulations often drive standards in heavily regulated industries, while corporate initiatives set standards in less regulated industries.

Cybersecurity initiatives on a policy level and adoption rates also vary globally. North American industries, including power generation, utilities, and manufacturing, constitute the largest portion of cybersecurity solution adopters. These organizations are making major investments in industrial cybersecurity, as mandated in part by NERC-CIP regulations for both cybersecurity processes and budgets. However, it is important to note that even in the case of North American utilities, only a small portion meet regulation requirements. For instance, most generation plants do not meet regulatory thresholds to qualify for NERC-CIP requirements (e.g., too few lines inflowing/outflowing or the maximum megawatt production).

Europe also has a substantial penetration of cybersecurity solution adoption, especially in manufacturing and utilities sectors. As part of its cybersecurity strategy, the EU passed its NIST Directive—legislation requiring all EU member countries to develop national cybersecurity capabilities, collaborate across borders, and supervise the cybersecurity of critical market operators. The high awareness of cybersecurity and corresponding geopolitical implications will drive cybersecurity adoption rates across Europe.

Cybersecurity policy preparedness is developing in ASEAN countries. Current policies and governance standards need to mature to meet market challenges. The lag is causing limited transparency of cyber-attacks, which has led to lower levels of cybersecurity awareness.

3. STRATEGIC RATIONALE & OPERATIONAL BENEFITS

Cybersecurity: What needs to be done?

Organizations face an increasingly complex business environment, and improving operational efficiency will remain a central driver for industrial firms. As technologies evolve and disrupt value chains, strategic investments will be needed to compete and safeguard integrity from potential cyber-attacks. No single product or solution can protect an organization from all cyber threats. To level the cybersecurity landscape, firms must 1) understand threats will continue to exist, 2) identify their vulnerabilities, 3) select integrity assurance providers with a comprehensive range of solutions, and 4) commit to recurrently assessing their cyber posture.

Although not all cyber risks can be eliminated, synchronized countermeasures provide organizations with the ability to mitigate a significant portion of their cybersecurity risks. Such practices determine cyber posture or readiness to respond to possible cyber risks and threats. Systematic assessments of vulnerabilities and responses to cyber-attacks will enable firms to navigate the cyber chaos and result in a manageable level of remnant ICS security risks.

Baker Hughes Portfolio: Cybersecurity solutions and service offerings

While there are several best practices to strengthen cybersecurity, like application whitelisting and patch management, comprehensive risk management often is an umbrella approach to drive effectiveness. This effort also requires a holistic portfolio of solutions that can be implemented within a customer's site.

Baker Hughes brings a rich history of cybersecurity solution design, development, implementation and management to the industry. The organization has installed cybersecurity solutions at more than 230 companies in over 45 countries with more than 3 million operating hours. Its journey started in 2008, when the Cyber Asset Protection (CAP) program was introduced for control system software updates. Over the past 11 years, it has engineered and structured cutting-edge solutions that have plant-wide monitoring capabilities. Its portfolio of offerings is shown in Exhibit 6.

EXHIBIT 6: BH'S PORTFOLIO OF SECURITY SOLUTION OFFERINGS

A HOLISTIC GROUP OF SOLUTIONS TO MITIGATE RISK

SECURITY DESIGN	ASSESS CONTROLS	CONTROLS SECURITY LIFECYCLE	MAINTENANCE	SECURITY TRAINING
SERVICES	SERVICES	PRODUCTS	SERVICES	TRAINING SERVICES
• Reference architecture consulting services	• Cyber vulnerability assessments • Create/review policy documents • Perform gap analysis to review compliance reporting	**SecurityST Appliance** • Access/password management • Centralized patch management • Automated backup and recovery • Secure information event management • Firewall network intrusion detection • Security FAT - Cyber secure lab	**Cyber Asset Protection (CAP)** • Subscription of updated patch and signature updates replicated in a control system ennronment • Patch applicability reports and ports and services documentation	• Securitv awareness training for responsible plant personnel

Source: BH; Frost & Sullivan

There are three key solutions that are unique and differentiated in the market

- **SecurityST Platform:** SecurityST offers centralized security management for customers. Other benefits include patch management, intrusion detection, Security Information Event Management (SIEM), application whitelisting, automated backups recovery, network segmentation, monitoring and more.

  SecurityST helps customers in three key ways:

  - *Reduces labor costs and resources:* The ability for the customer to log into one portal for centralized updates and backups leads to at least $10,000 to $20,000 in savings per site monthly.

  - *Strengthens overall security posture:* Virtualization and strong access management allow customers to have traceability on activities.

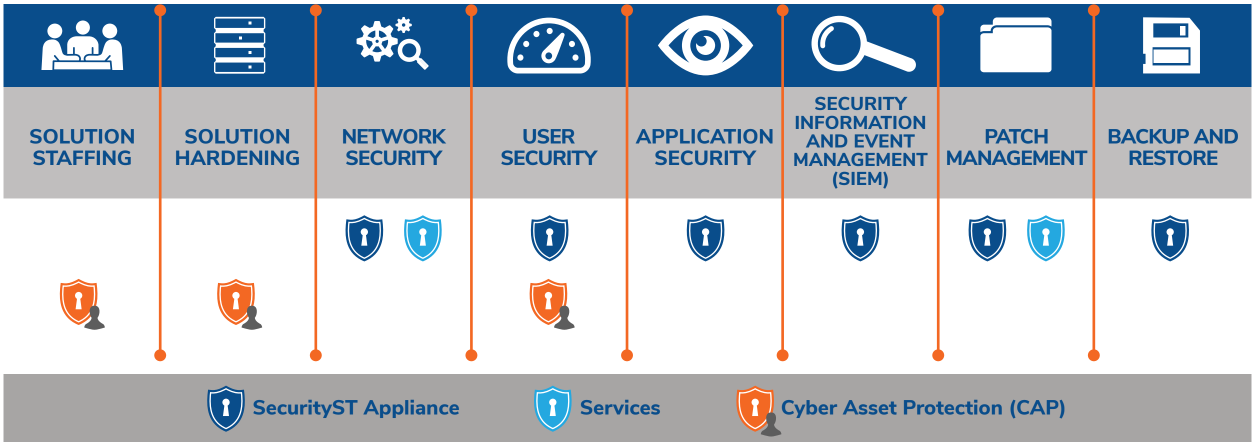
- *Comply with regulations:* As cyber regulations continue to evolve and mature, it is important to work with an organization that has the ability to stay ahead of the market while understanding the nuances of cybersecurity. Today, SecurityST can help in compliance with NERC CIP Rev. 5 & 6, NEI 08-09, WIB, ISA and IEC 62443-2-4 standards.

- *Scale based on needs:* Knowing customer preferences, Baker Hughes offers three tiers of the solution to meet the specific requirements of a plant of any size—SecurityST Compact (up to 10 HMIs), SecurityST standard (up to 30 HMIs) and SecurityST Pro (30+ HMIs). Its key value propositions are centered on being layered, scalable and configurable.

- **Cyber Asset Protection:** This is a software subscription offering that is aimed at securing HMIs from vulnerabilities with included antivirus signatures. Its key differentiation offered to customers is its ability to simulate updates/patches before actual implementation on the endpoint. Further, as customers manage multiple HMIs, it is important to monitor the nature of updates, regularity of implementation, etc. The solution from Baker Hughes helps customers with a comprehensive inventory of applicable updates and statuses. Against IEC 62443-2-4, Exhibit 7 outlines BH's solution presence and value creation.

EXHIBIT 7: CYBER SECURITIES CAPABILITIES

CYBER SECURITIES CAPABILITIES - IEC 62443-2-4



SOLUTION STAFFING	SOLUTION HARDENING	NETWORK SECURITY	USER SECURITY	APPLICATION SECURITY	SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM)	PATCH MANAGEMENT	BACKUP AND RESTORE
		SecurityST Appliance Services	SecurityST Appliance	SecurityST Appliance	SecurityST Appliance	SecurityST Appliance Services	SecurityST Appliance
Cyber Asset Protection (CAP)	Cyber Asset Protection (CAP)		Cyber Asset Protection (CAP)				

SecurityST Appliance Services Cyber Asset Protection (CAP)

Source: BH; Frost & Sullivan

As shown above, Baker Hughes can comprehensively support a customer's journey to a trusted, secure future from assessment services to patch management to back-up and restore services. Very few in the market can provide end-to-end solutions and service offerings. Many are point solution offerings, which often leave customers to patch solutions together. This is ineffective and leads to integration and information exchange issues.

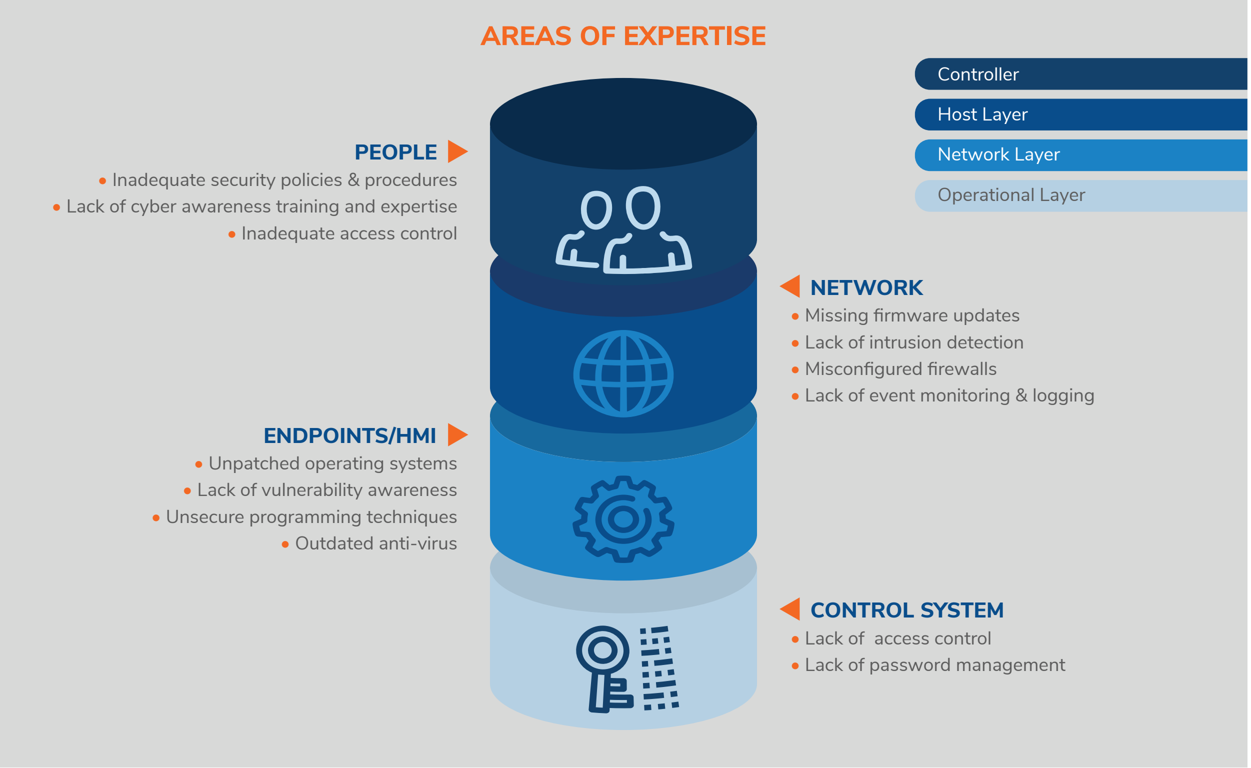
- **Nexus Control System Integrated Software:** Baker Hughes' Nexus OnCore control system is a state-of-the-art offering that leverages a redundant architecture and delivers a variety of modules that fit varied plant requirements. It is used to run critical applications like coal handling, burner management, boiler management, turbine performance management, etc. Additional benefit comes with its software solution offering; it combines multiple capabilities on one seamless platform to provide a total plant view of all assets. The best-in-class HMI screens offer system diagnostic information at precise refresh cycles. Historian is embedded within the software to perform comparative analytics and trending performance. The versatility of the HMI solution is shown in its ability to integrate information from multiple HMIs and showcase a single version of truth through a single window.

BH's solution portfolio puts it in a unique position in securing critical assets and networks of the customers. It has a strong footprint in the power industry (including nuclear) and is well embraced in large facilities. As digital transformation disrupts and drives industry structural changes, legacy systems need security updates. Engineering hot changeovers and online security patch management are some of the key requirements for customers.

4. ROADMAP FOR A SECURE FUTURE

Vulnerability comes in many forms and complexities. As a best practice, layered approaches offer strong cyber preparedness for enterprises, as shown in Exhibit 8..

EXHIBIT 8: VULNERABILITIES AND THE IMPORTANCE OF DEFENSE-IN-DEPTH APPROACHES


AREAS OF EXPERTISE
Controller
Host Layer
Network Layer
Operational Layer
PEOPLE
• Inadequate security policies & procedures
• Lack of cyber awareness training and expertise
• Inadequate access control
NETWORK
• Missing firmware updates
• Lack of intrusion detection
• Misconfigured firewalls
• Lack of event monitoring & logging
ENDPOINTS/HMI
• Unpatched operating systems
• Lack of vulnerability awareness
• Unsecure programming techniques
• Outdated anti-virus
CONTROL SYSTEM
• Lack of access control
• Lack of password management

Source: BH; Frost & Sullivan

Unsupported OS, unpatched systems and network intrusions can create havoc in small, mid-sized and large enterprise organizations. Managing these comprehensively is increasingly becoming a significant challenge for customers worldwide. The cost of downtime is also significantly high and customers need to prevent attacks rather than reacting to threats.

CASE STUDIES FROM THE FIELD

Customer case study 1: Oil and Gas

A large oil & gas company wanted to strengthen its cyber infrastructure to protect its ICS network against sophisticated threats and achieve compliance with organizational cyber standards. To meet the needs of three distinct operational technology environments while maintaining full system functionality, the organization required a centralized security management solution with a defense-in-depth system. Only a trusted partner with expertise in both oil and gas and cybersecurity could provide a customized solution to meet its needs in a timely manner.

With local expertise in the region, BH was able to understand the organization's needs. BH customized its SecurityST solution to meet the oil and gas company's Software Identification (SWID) audit requirements and site configurations. Installed to protect three physically separated sites, BH's SecurityST solution helps mitigate cyber vulnerabilities at three levels: network, endpoint and controller. This centralized system employs modular defensive services and technologies to give the organization a single vantage point to see its cybersecurity posture and implement proactive strategies and policies to protect critical control systems and related networks. BH then provided validated patch management to fully test patches on the Windows operating systems through BH's Cyber Asset Protection (CAP) program and executed hardening of HMIs, as a best practice, to maintain system functionality.

Join us in our journey as we build secure enterprises of the future.

Customer case study 2: Power generation

A major North American electricity generator needed help to improve cyber posture from a recent breach as well as achieve compliance with NERC Critical Infrastructure Protection (CIP) plan standards for its more than 80 operational units. The project required expertise and execution within a short timeline due to an upcoming scheduled outage.

BH implemented its proven layered industrial control system (ICS) cybersecurity solutions. BH's centralized management system, SecurityST, is IEC 62443-2-4-certified, indicating the solution uses best practices for integration and maintenance. BH's Cyber Asset Protection (CAP) program further strengthened the security posture with real-time topography identification, patch management, and hardened HMIs as a best practice to maintain system functionality. The solution identified 15-20 unidentified network IP addresses within the first 2-3 hours of the operation.

Along with the customer use cases shown above, Baker Hughes differentiates itself in the cybersecurity market through its:

- Track record in designing and implementing control systems: BH has designed and implemented cybersecurity for a variety of control systems that run critical assets including compressors, steam and gas turbines. Even its latest solution, the Nexus OnCore control system, is state of the art and overcomes many of the industry's endemic issues with control system performance management.
- Comprehensive cybersecurity portfolio: From sensors to control systems to asset protection principles, BH leads the way in delivering a rich and secure plant-wide monitoring experience to its customers. This is shown in its installed base spread across end markets and geographical regions.

FROST & SULLIVAN

SILICON VALLEY | 3211 Scott Blvd, Santa Clara, CA 95054
Tel +1 650.475.4500 | Fax +1 650.475.1571

SAN ANTONIO | 7550 West Interstate 10, Suite 400, San Antonio, Texas 78229-5616
Tel +1 210.348.1000 | Fax +1 210.348.1003

LONDON | Floor 3 - Building 5, Chiswick Business Park, 566 Chiswick High Road, London W4 5YF
TEL +44 (0)20 8996 8500 | FAX +44 (0)20 8994 1389

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?