PUTTING INDUSTRIAL CYBER SECURITY AT THE TOP OF THE CEO AGENDA

CONNECT:

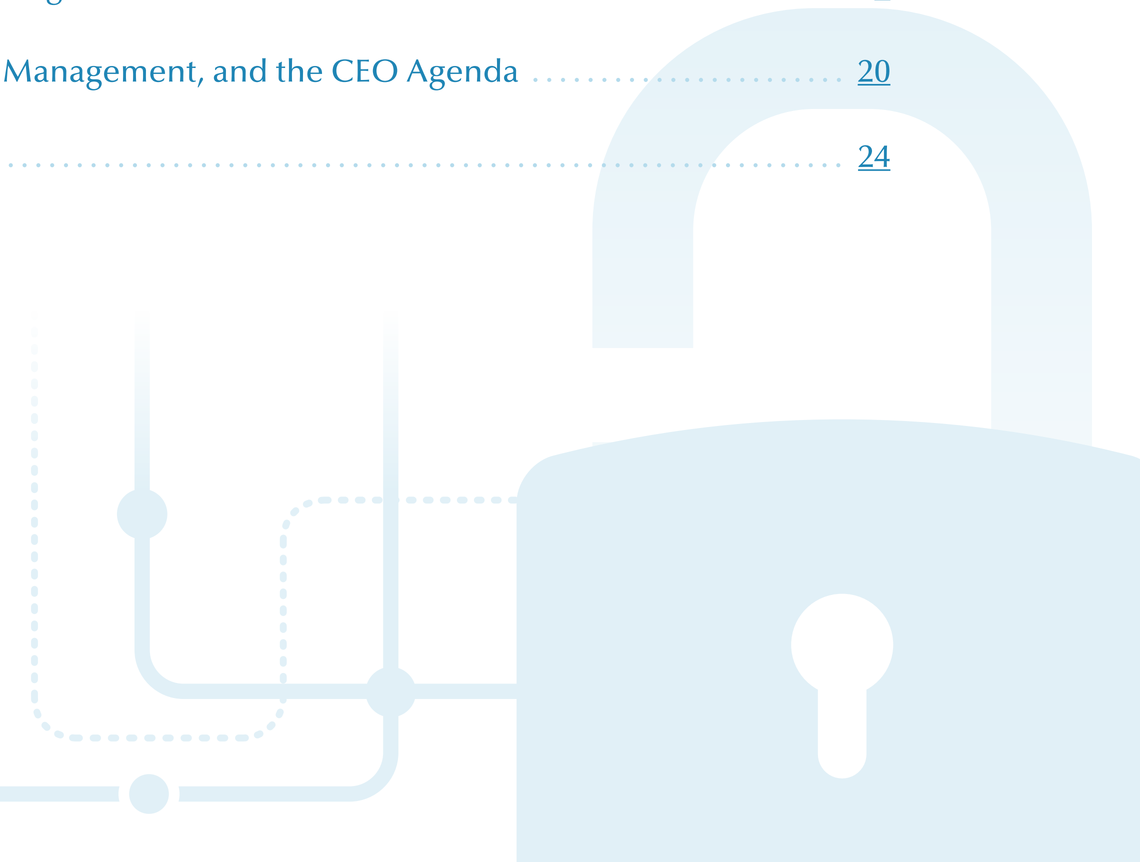
lnsresearch.com

LNS research

PUTTING
INDUSTRIAL CYBER SECURITY
AT THE TOP OF THE CEO AGENDA

LNS research

TABLE OF CONTENTS



ACRONYM
QUICK REFERENCE
VIEW ON BLOG

lnsresearch.com

SECTION 1

Introduction

Introduction

Leading industrial companies have moved headlong into pursuing Digital Transformation strategies with initiatives like Smart Manufacturing and Industry 4.0. CEOs have put these initiatives at the top of their agenda, not as technology projects, but for the business opportunities they present. Among them are gain competitive advantage through new service enabled business models, disruptive new products, a more agile supply chain, and efficient operations.

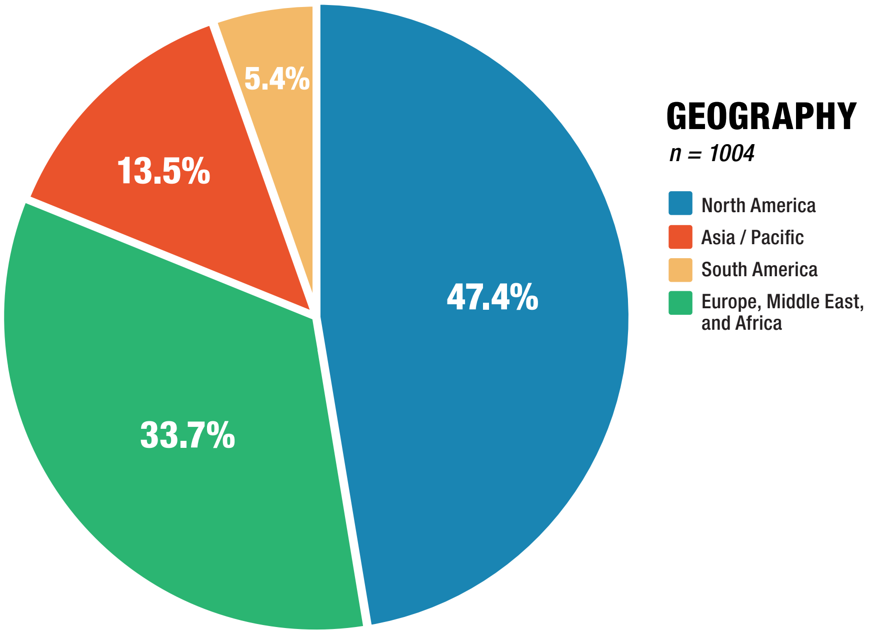
Unfortunately, legacy automation and control systems are not inherently secure. Although next-gen systems have built-in security, industrial companies can't afford to wait until they refresh the entire fleet of assets – they must ensure secure operations and enable Digital Transformation today. In this eBook, LNS Research examines results from over 1000 survey respondents regarding their approach to the Industrial Internet of Things (IIoT) and the use of industrial cyber security technologies and best practices. The research will show that the majority of companies today are exploring or planning Digital Transformation initiatives, but the adoption of industrial cyber security capabilities and technology is shockingly low.

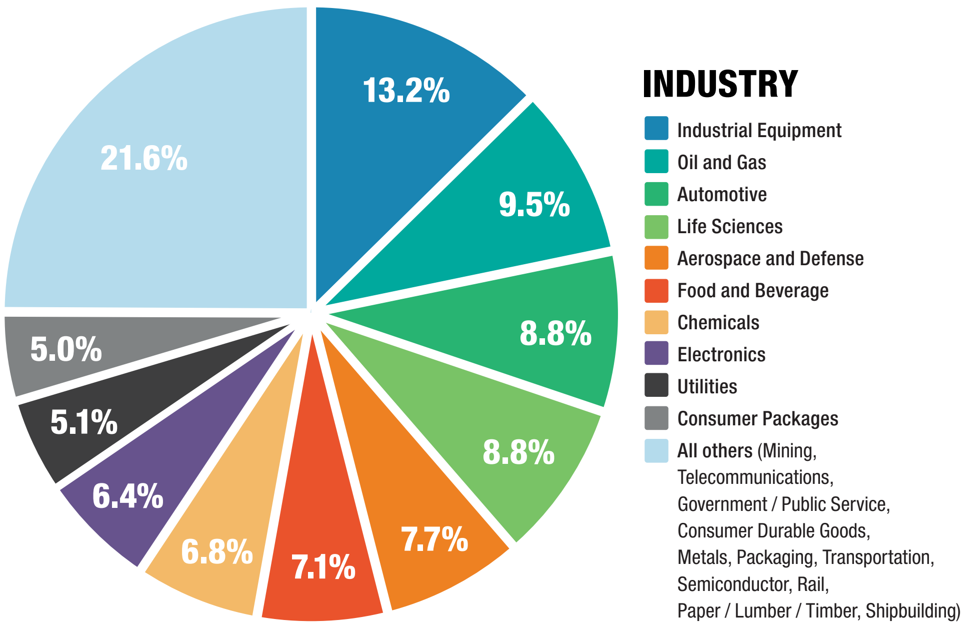
The research will also show how leading companies are building industrial cyber security into the fabric of the IIoT, and delivers actionable recommendations for a risk-based approach to optimize industrial cyber security investments and to put industrial cyber security at the top of the agenda.

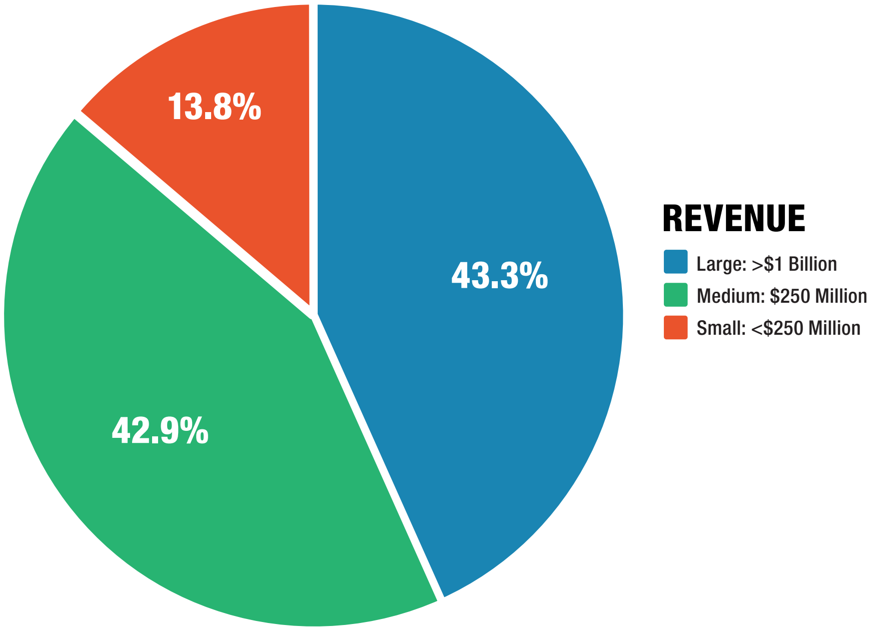
Next-gen systems have BUILT-IN SECURITY, but companies CAN'T AFFORD TO WAIT until they refresh the entire fleet of assets.

Research Demographics

Over 1000 respondents from industrial companies have completed the LNS Research general demographic and technology survey over the last 18 months. Of these respondents, 130 have completed the more detailed IIoT survey. Nearly two-thirds of respondents come from North America and Europe, but no region makes up a majority of respondents. Across industries, there is a broad range across process, batch, and discrete, with no industry making up more than 15% of respondents. Regarding company size, there is an almost even split between large and small companies at 43%, with the smallest percentage of respondents being medium-sized businesses.







Digital Transformation Momentum

The industrial sector has never been afraid to adopt new technologies in the pursuit of improving operations. It has just been slower to adopt than other industries – often purely based on economic realities, with its asset-intensive nature, risk aversion, and slow technology refresh cycles. Today, these economic forces specific to the industry are being overwhelmed by the competing technology-driven economic forces external to the industry, including the dramatic drop in costs of connectivity, sensing, computing, and storage.

These technology trends have sparked the imagination of industry executives and are the technology enablers driving future visions for the industry like Industry 4.0, Smart Manufacturing, and the Digital Refinery, all of which are varying flavors of Digital Transformation initiatives. In the latest survey data from LNS Research, these initiatives are no longer visionary; 40% of companies already have a Digital Transformation initiative in place, and another 24% will start one this year.

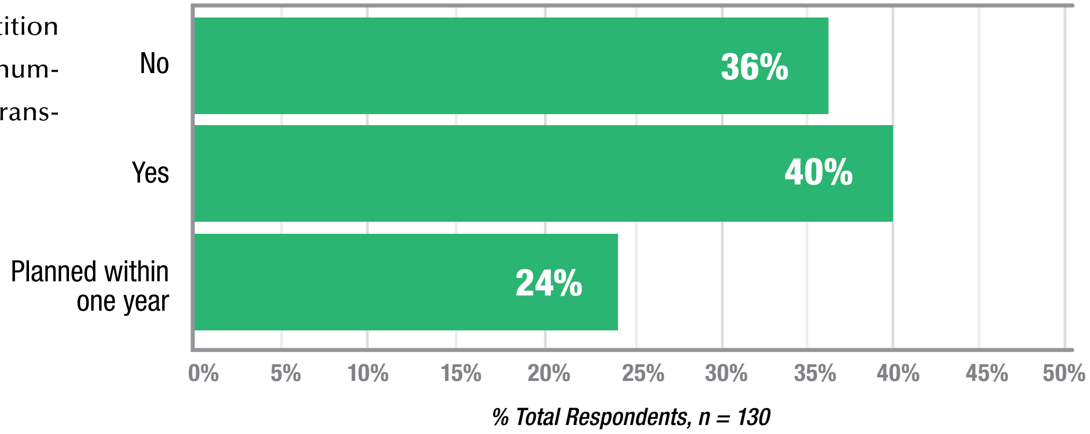
Digital Transformation is not a 1- or 2-year technology project; instead, it's a long-term business initiative. To be successful, companies must start today and avoid common pitfalls, or risk quickly falling too far behind the competition to catch up. Furthermore, the research shows that the number one technology pitfall companies face in Digital Transformation is industrial cyber security.

40% OF COMPANIES
have a Digital Transformation initiative

24% OF COMPANIES
will start one this year

#1 PITFALL is
INDUSTRIAL CYBER SECURITY

Has your company started an IIoT initiative (i.e. smart manufacturing, Industry 4.0, etc.)?

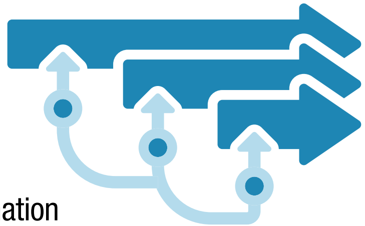


Digital Transformation Framework

Any digital strategy must be more than just the CEOs vision or initiative; it must have support throughout the organization, with each level having specific responsibilities and feedback loops. From the executive team at the top setting strategic objectives, to the business leaders aligning people, process and technology capabilities with Operational Excellence, to technology leaders establishing a scalable and flexible Operational Architecture, to functional managers conducting specific solution selection.

By the very nature of digital strategies, technology is fundamental, not an afterthought. The entire exercise is driven by any change in the realm of possibilities because of technological innovations like the IIoT, and new business models, operating models, and customer engagement models. By the same token, industrial cyber security is now central to business strategy, not an afterthought. Security at every level should be a prerequisite for the deployment of new technologies.

DIGITAL TRANSFORMATION FRAMEWORK by LNS Research describes a systematic approach to simultaneous and interconnected digital initiatives, in order to manage transformation across all levels and functions of the organization.



Click to learn more about the
Digital Transformation Framework

INDUSTRIAL CYBER SECURITY
is now central to business strategy, not an afterthought.

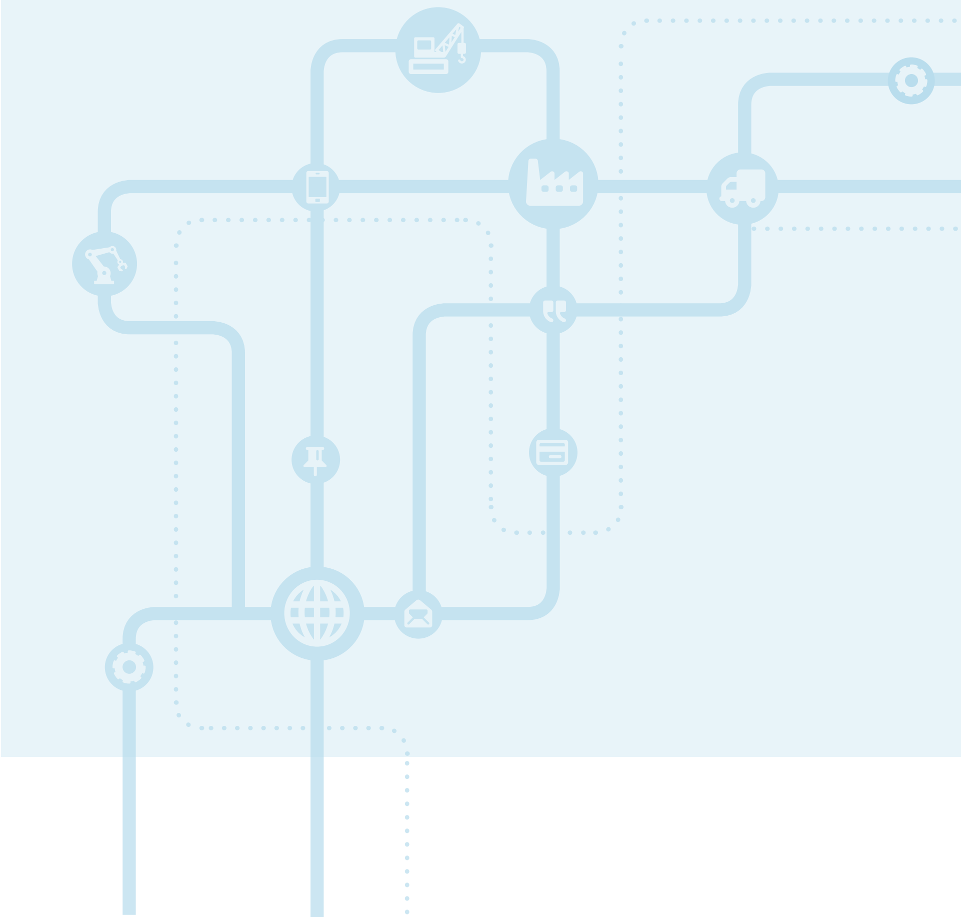
SECURITY AT EVERY LEVEL SHOULD BE A PREREQUISITE for the deployment of new technologies.

Emergence of Industrial Internet of Things Platform

There has been much talk about the Internet of Things (IoT) and its impact on the industrial sector over the past several years. As the space has matured and vendors have focused on and specialized in the industrial arena, an IIoT platform market is emerging, along with a supporting ecosystem of technology and service providers.

Today, IIoT platforms use next-gen technology to provide a platform-as-a-service (PaaS) that delivers connectivity across the value chain and enables flexible next-generation applications using both Cloud and Big Data analytics capabilities. As companies continue to embrace a platform approach to the IIoT, it is critical that industrial cyber security capabilities are embedded as part of the platform foundation, and not considered add-on pieces of functionality.

> As companies continue to embrace a platform approach to the IIoT, **IT IS CRITICAL THAT INDUSTRIAL CYBER SECURITY CAPABILITIES ARE EMBEDDED AS PART OF THE PLATFORM FOUNDATION,** and not considered add-on pieces of functionality.



INDUSTRIAL INTERNET OF THINGS PLATFORM by LNS Research describes the connectivity, network styles, and applications framework to support smart connected operations and smart connected assets; within and across a plant, facility or production network in a manufacturing or other industrial operations setting.

Click to learn more about the
Industrial Internet of Things Platform

SECTION 2

Industrial Cyber Security is a Major Roadblock to Digital Transformation

Industrial Cyber Security is Top Technical Challenge Facing IIoT

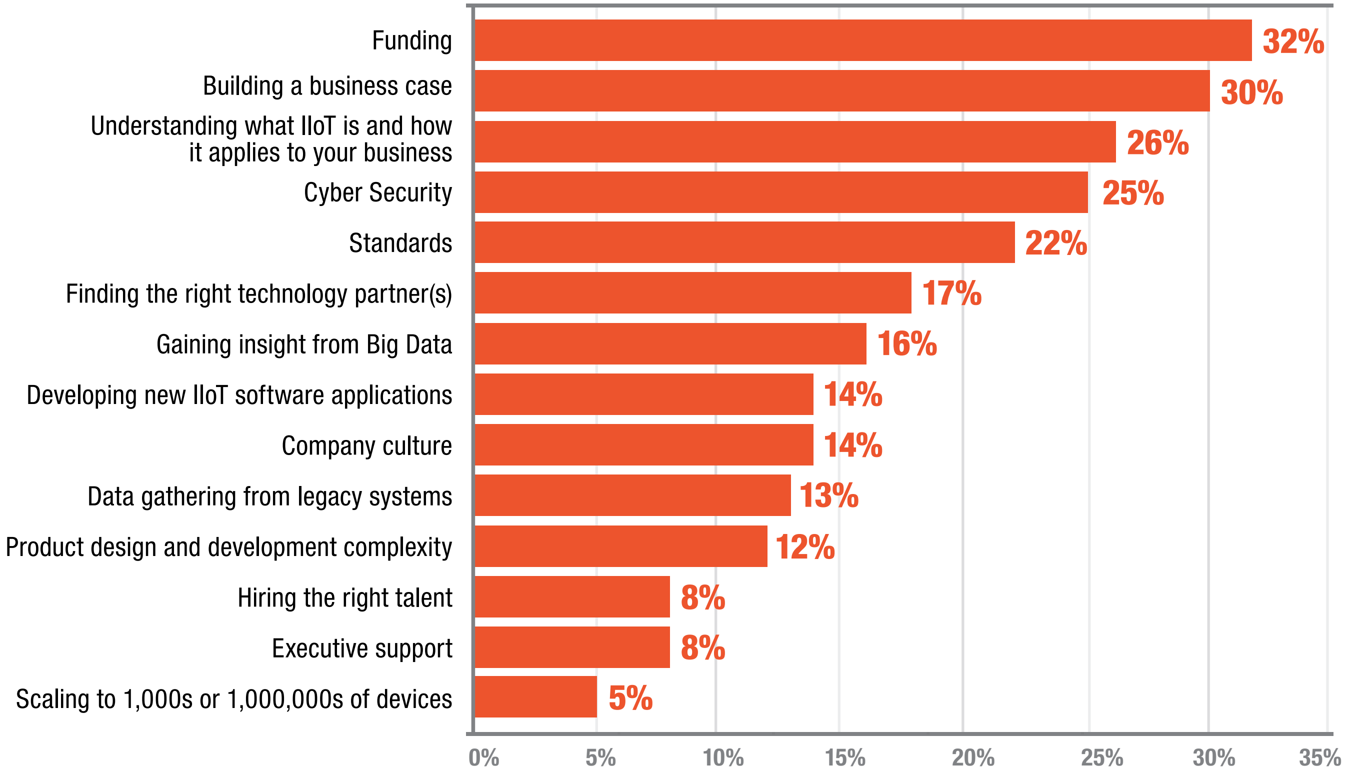
Previous LNS Research reports have focused on helping industrial companies address the top three IIoT challenges, which are all business-related. Early adopters struggled to understand how the IIoT was different from then-current technology and how to build a business case around this technology.

Once a company moves beyond building a business case and starts examining technology challenges, industrial cyber security rises to the top of the list and fourth overall. This is not surprising for a host of reasons, which we will dive into throughout the rest of this section:

- **Pervasiveness of the threat**
- **Lack of IT-OT convergence**
- **Severely limited adoption of industrial cyber security best practices across people, process, and technology capabilities**

What are the top challenges your company faces in deploying IIoT technology?

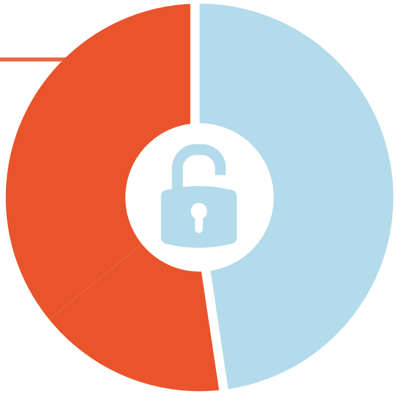
(N=269, all respondents)



Pervasiveness of Threat

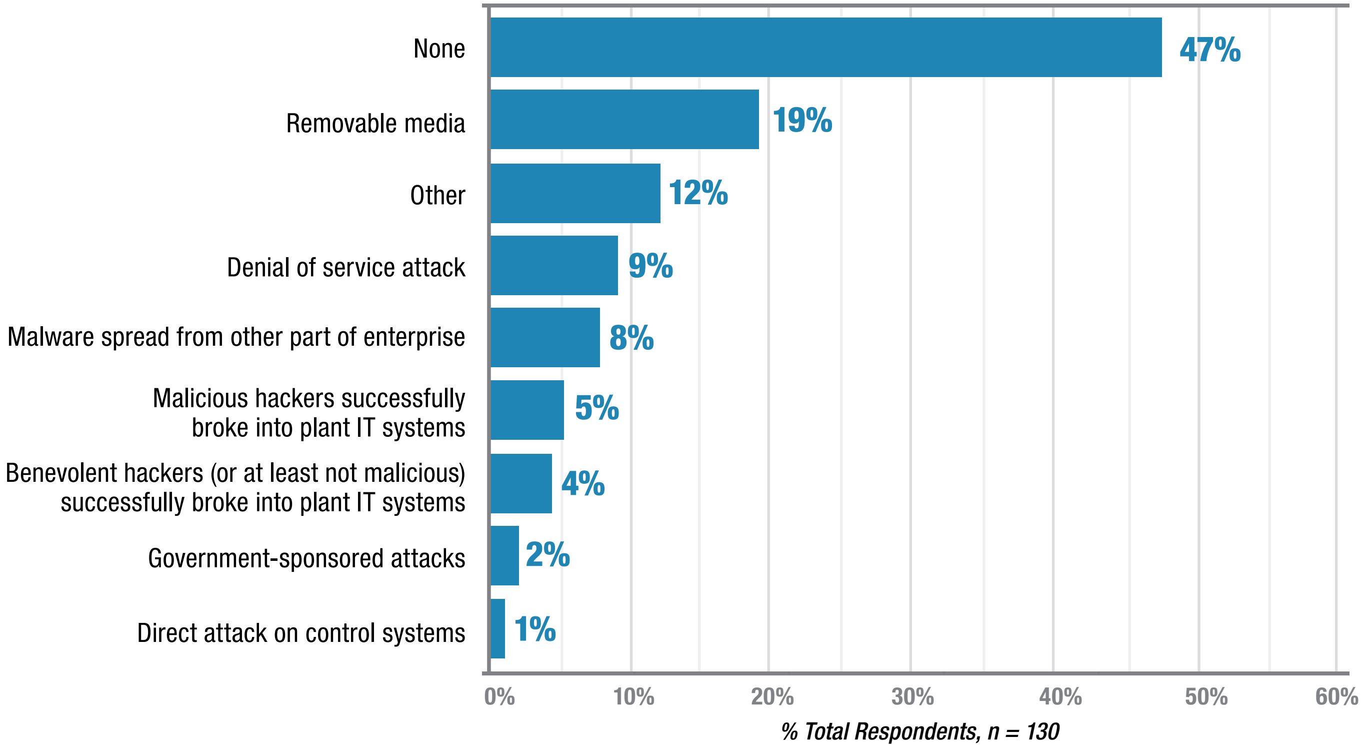
For many companies, a "public" dialogue on industrial cyber security is still taboo; often for legitimate legal or public relations concerns, but nevertheless many industrial facilities don't or won't talk about breaches publicly. For organizations that have not yet experienced a breach, the consequence is often a dramatic underestimation of threat; rest assured that the risk is overwhelming.

Shocking to many, but in an anonymous setting, like an LNS Research survey, over half of respondents report working in an industrial facility that has already had a cyber security breach. It is also important to note that attack sources come from a broad set, some IT-focused, some OT-focused, some malicious, others accidental. Direct attacks are rare, but what is surprising is that 19% of companies report a source that doesn't even require internet connectivity for infection – removable media.



53% REPORT CYBER SECURITY BREACH IN THEIR FACILITY.

Have you had any plant cyber security breaches? If so, from what source?

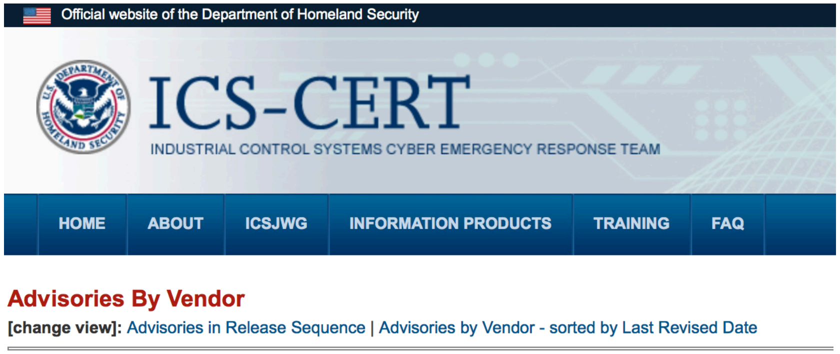


Pervasiveness of Threat *(Cont.)*

Even though direct attacks on control systems are rare, a company is fooling itself if it believes its control system is inherently secure. According to the US Department of Homeland Security ICS-CERT Advisories by Vendor list, every major automation vendor has known vulnerabilities, and companies should always assume that all controls systems are inherently insecure (as are all systems).

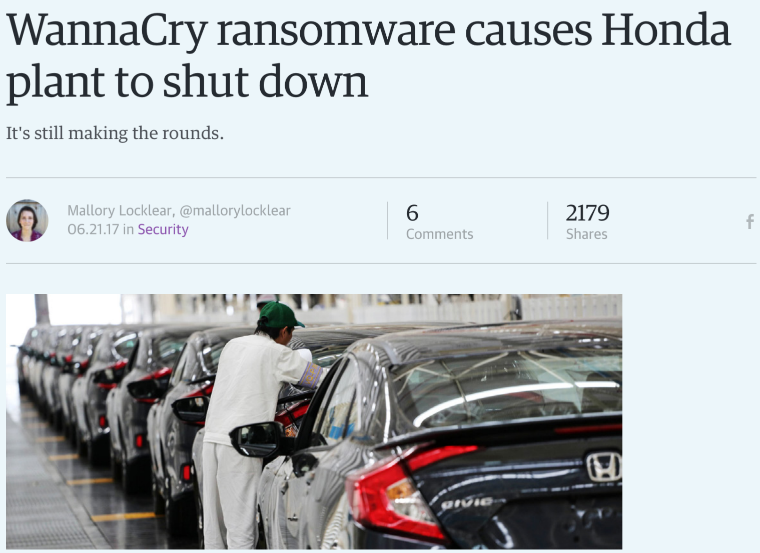
Organizations should also note that within a plant network, many IT assets also have known vulnerabilities. According to LNS Research survey data, Microsoft is the market share leader providing software for the plant floor. With so many plants relying on Microsoft technology, when there are major IT security events, they undoubtedly impact the industrial sector. Just consider the recent WannaCry attack and the impact on industrial companies; that's just the tip of the iceberg compared to what's on the horizon because of the Shadow Broker NSA leaks. With what is now publicly available information, even unsophisticated bad actors have access to military grade tools.

All of this means that industrial companies must maintain and update IT and OT systems to ensure basic industrial cyber security in the plant. However, given the pervasiveness of the threat, ensuring IT-OT convergence is just the start.


Official website of the Department of Homeland Security
ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM
HOME
ABOUT
ICSJWG
INFORMATION PRODUCTS
TRAINING
FAQ

Advisories By Vendor

[change view]: Advisories in Release Sequence | Advisories by Vendor - sorted by Last Revised Date



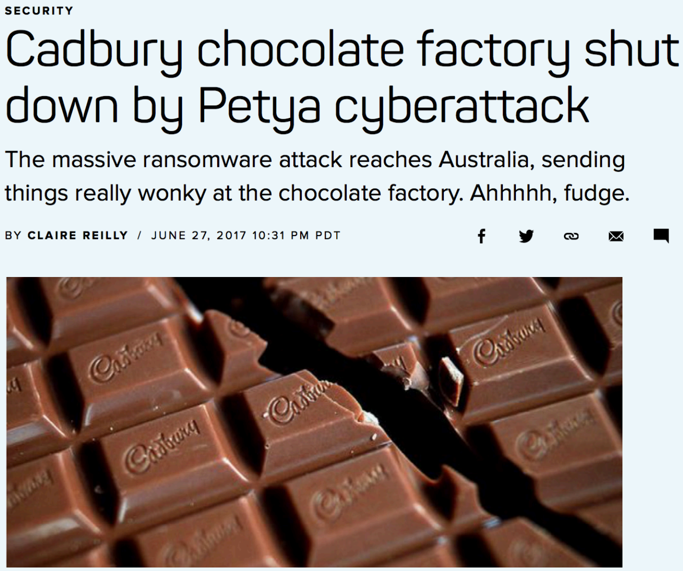
WannaCry ransomware causes Honda plant to shut down

It's still making the rounds.

Mallory Locklear, @mallorylocklear
06.21.17 in Security

6 Comments

2179 Shares



SECURITY

Cadbury chocolate factory shut down by Petya cyberattack

The massive ransomware attack reaches Australia, sending things really wonky at the chocolate factory. Ahhhhh, fudge.

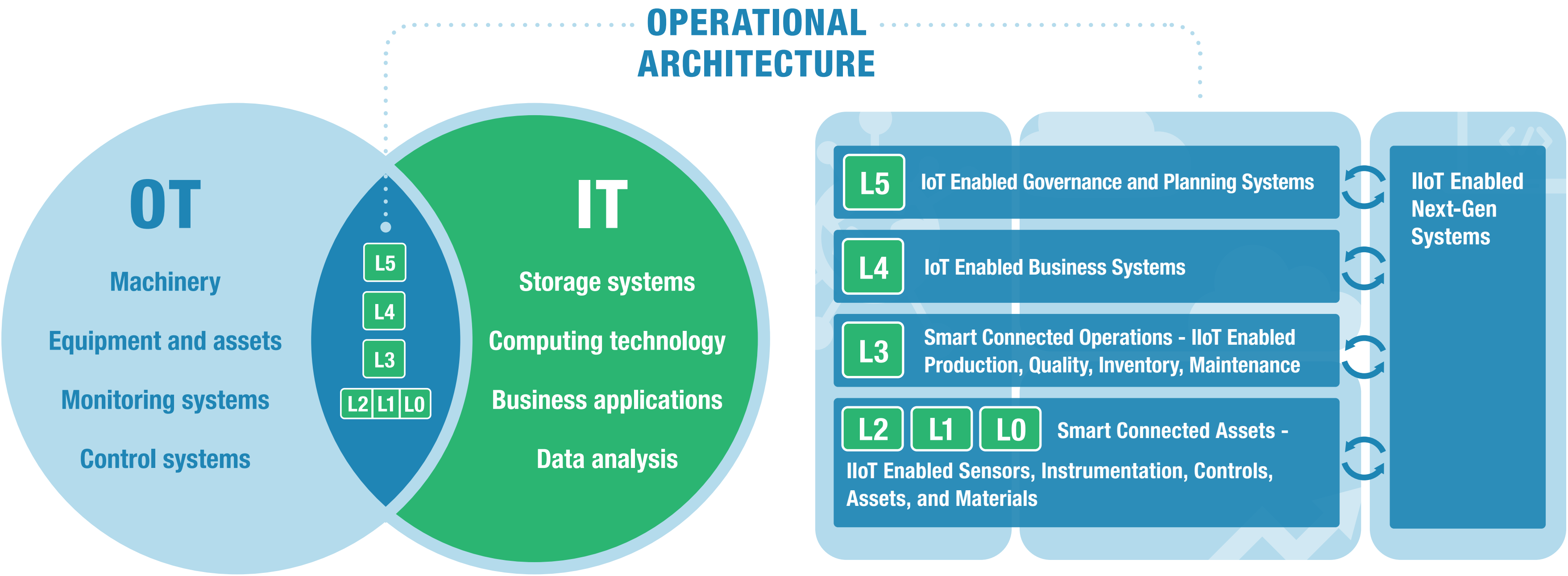
BY CLAIRE REILLY / JUNE 27, 2017 10:31 PM PDT

Industrial Cyber Security: IT-OT Convergence Flash Point

IT-OT convergence is necessary to manage traditionally IT-centric automation equipment (or operational technology) and organizations in a holistic and harmonized way in order to deliver an optimized technology solution to the business. In many areas of industrial operations, IT and OT silo's have persisted for decades, and although it is not optimal, many companies continue to allow these separate groups and technology to operate almost entirely independently.

As organizations begin to take industrial cyber security seriously, they cannot adequately address it without true collaboration between IT and OT. IT organizations are the group most likely to take a leadership role in securing plant equipment, both IT and OT. However, if only IT security tools are used by IT personnel, the company will never adequately address the OT equipment and network. To secure these systems, it takes IT security skills and know-how, but specifically targeted and configured for the OT environment – this is the heart of industrial cyber security.

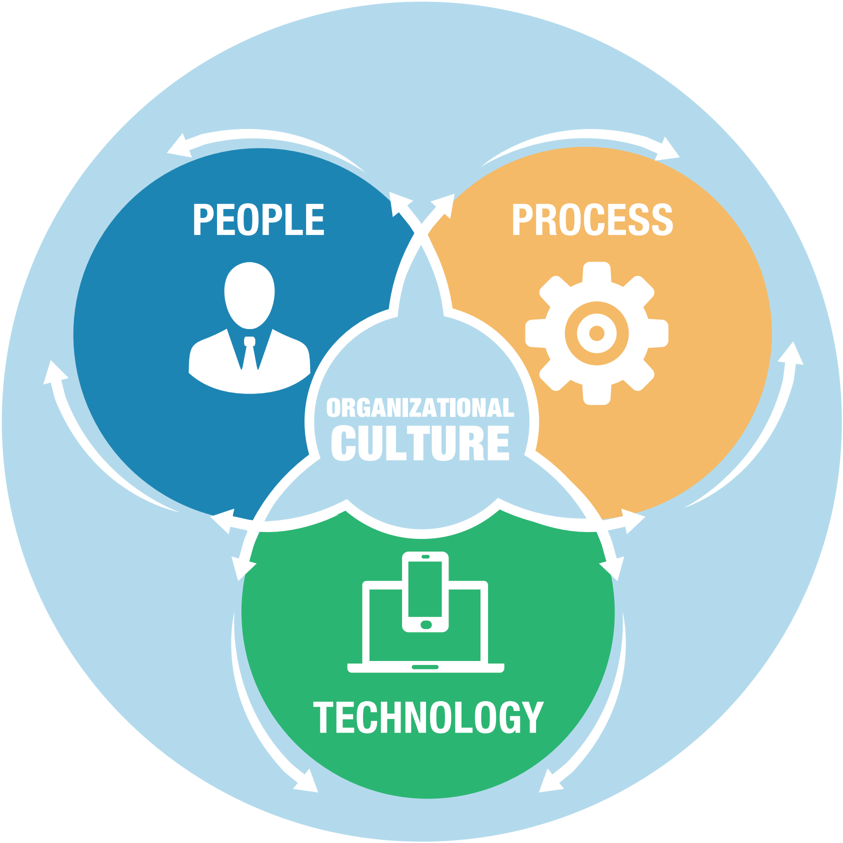
> Companies that take industrial cyber security seriously use IT security skills and know-how TARGETED AND CONFIGURED FOR THE OT ENVIRONMENT.


OPERATIONAL ARCHITECTURE
OT
Machinery
Equipment and assets
Monitoring systems
Control systems
L5
L4
L3
L2 L1 L0
IT
Storage systems
Computing technology
Business applications
Data analysis
L5 IoT Enabled Governance and Planning Systems
L4 IoT Enabled Business Systems
L3 Smart Connected Operations - IIoT Enabled Production, Quality, Inventory, Maintenance
L2 L1 L0 Smart Connected Assets - IIoT Enabled Sensors, Instrumentation, Controls, Assets, and Materials
IIoT Enabled Next-Gen Systems

Operational Excellence also applies to Industrial Cyber Security: People Process and Technology Capabilities

Industrial cyber security is clearly a technology issue – but that doesn't mean the key learnings from Operational Excellence don't apply. To have success in any area of technology – and improve business performance, it is critical that people and process come together with technology to drive a successful organizational culture that takes industrial cyber security seriously. As a general statement, industrial companies woefully under-invest in industrial cyber security best practices across people, process, and technology, and survey results illustrate shortcomings across all of these areas.

INDUSTRIAL COMPANIES WOEFULLY UNDER-INVEST in industrial cyber security best practices across people, process, and technology.



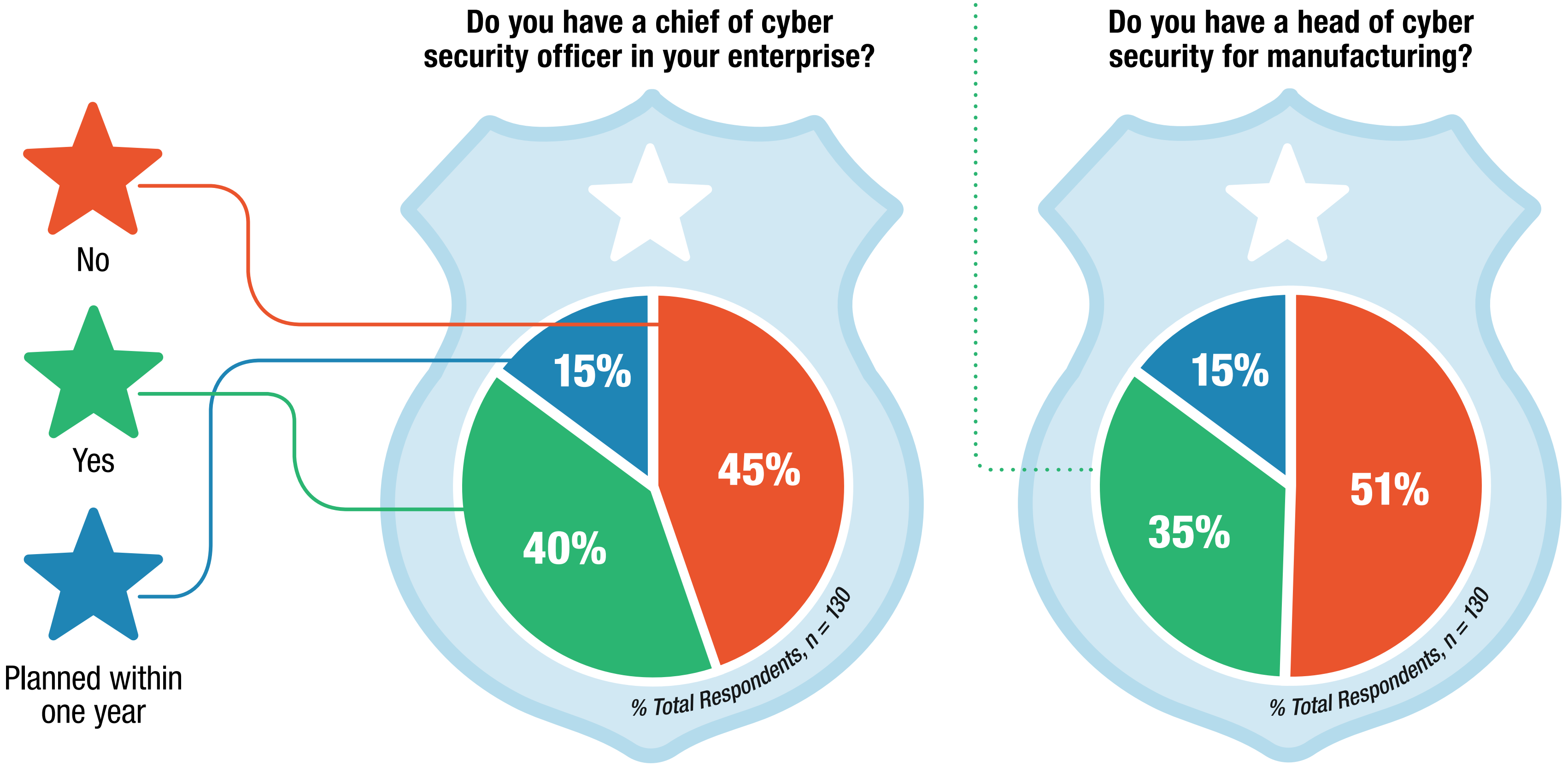
Lack of Best Practices Adoption: People

When it comes to having a defined role for security at the enterprise level, companies are doing a relatively good job; 40% of organizations currently have an established role for chief of cyber security, and another 15% have plans for it. Traditionally this has fallen under the purview of the CIO, but more frequently we see a dedicated role for security, like a Chief Information Security Officer (CISO).

When it comes to having a defined role in charge of security for the plant, companies are further behind, with only 35% of them having an established role and the same percentage planning one at the enterprise level.

Overall, for IT-OT convergence to become a reality and for a company to implement an effective industrial cyber security solution, both of these roles must exist and work collaboratively towards the success of a strategic initiative like Industry 4.0 or Smart Manufacturing.

ONLY 35% OF COMPANIES have an established role for cyber security.



Do you have a chief of cyber security officer in your enterprise?

Do you have a head of cyber security for manufacturing?

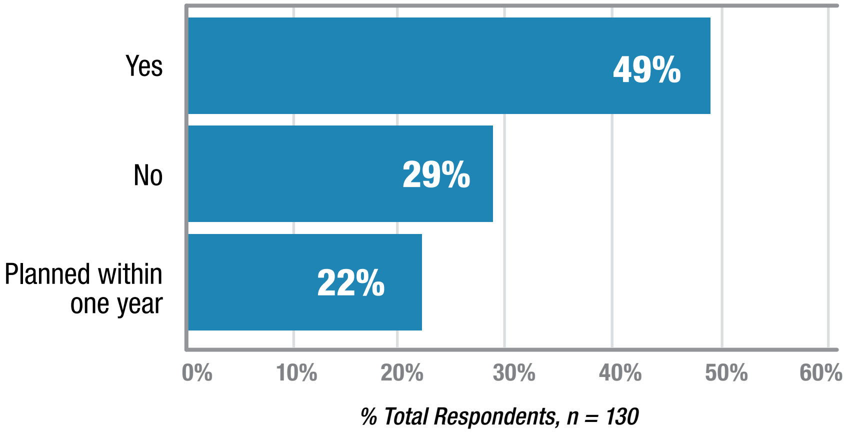
Lack of Best Practices Adoption: Process

Compared to other best practices for industrial cyber security, documentation and policy management is a relatively bright point, with close to two-thirds of companies either having them in place or planning to implement an enterprise-wide account management policy for industrial plants.

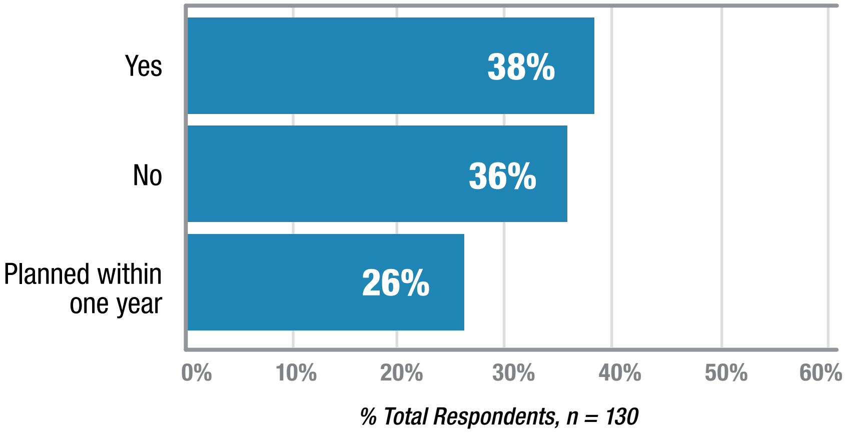
However, when we examine documentation and policy management processes that are more likely to be managed by OT than IT, the results are not as strong. For example, only 38% of companies have a definitive list of plant connections and what data can flow through.

Overall, the IT side of the house is slightly ahead of the OT side of the house when it comes to industrial cyber security best practices adoption – but both have significant room for improvement. It's important to note that policy-focused processes are generally foundational and only deliver real value and risk reduction if they have support from other industrial cyber security leadership and technology best practices.

Do you have an enterprise and plant-wide IT account management policy in place?



Do you have a definitive list of connections to the plant and what data can flow through them?



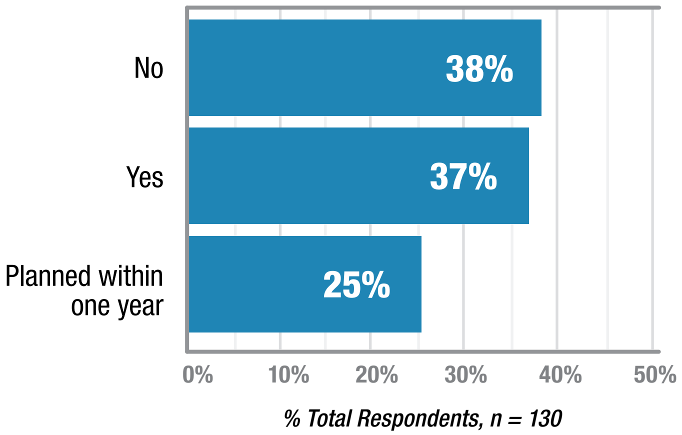
Lack of Best Practices Adoption: Process *(Cont.)*

The percentage of companies that regularly conduct risk assessment and penetration testing was the only positive note in the survey results, with 70% and 63% of the market doing them at least once per year, respectively. Although the other adoption numbers are low, this shows that the majority of manufacturers are at least aware of the issues and taking some steps to address them.

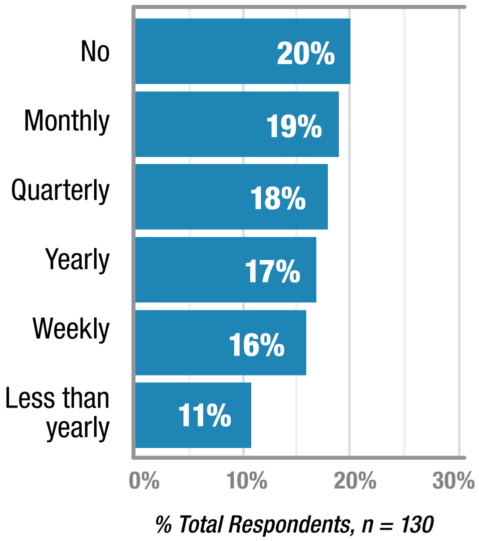
Unfortunately, less than half of those surveyed (37%) reported adoption of real-time monitoring of network activity. Although based on the results, the market is aware that this is an important area to focus on with the highest planned adoption rates over time, at 25%. These results may not be all that surprising, considering some of the newer solution providers are offering passive monitoring for the industrial control systems and networks; the benefits are clear and the upfront costs have been dramatically slashed.

38%
OF INDUSTRIAL COMPANIES
do not monitor networks for suspicious behavior.

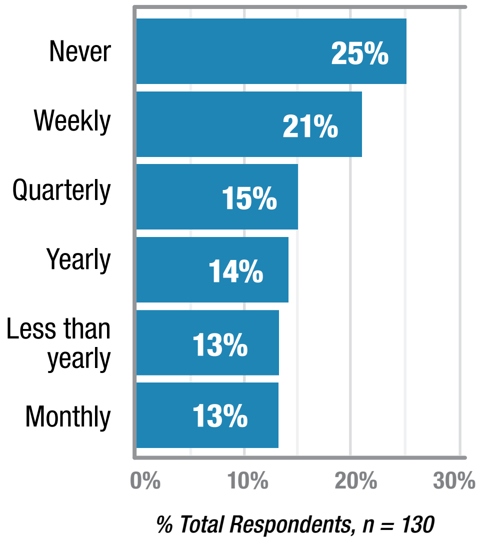
Do you continually monitor plant systems and networks for unusual behavior?



Do you conduct regular risk assessments?



How often do you carry out regular penetration testing on your firewalls?



Lack of Best Practices Adoption: Technology

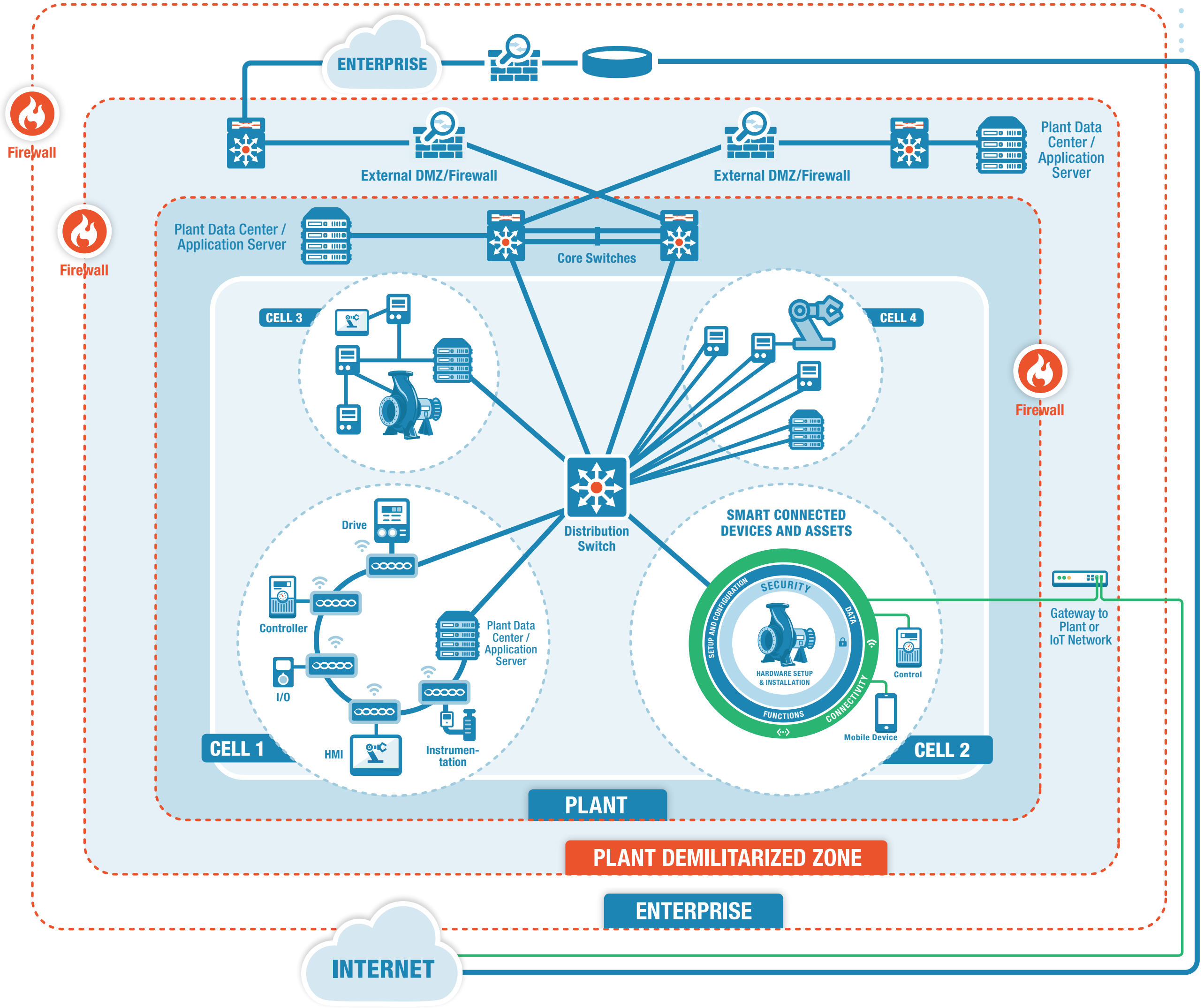
The starting point for many on the technology side when it comes to industrial cyber security is starting with networking architecture and securing the industrial network and control systems. Over the past decade, there have been a variety of reference architectures become available that illustrate how to segment the network. In every case, the guidelines advocate for a Defense in Depth Architecture.

By segmenting the network and separating the plant from the enterprise and public internet, companies minimize the risk of damage when intrusions do happen.

The starting point for industrial cyber security is

NETWORK ARCHITECTURE:

secure the industrial network and control systems.



Lack of Best Practices Adoption: Technology *(Cont.)*

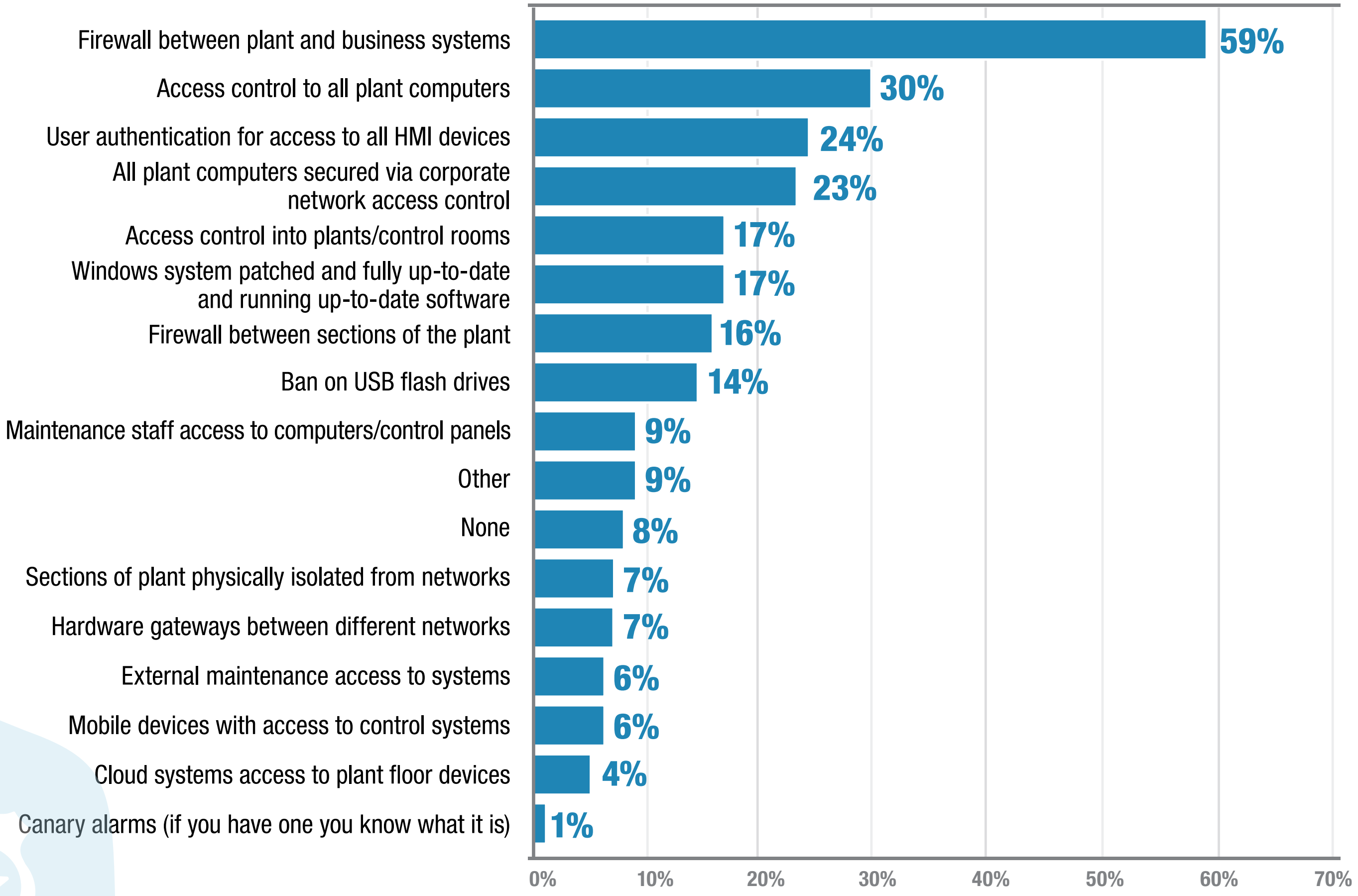
Going beyond architecture, when considering specific industrial cyber security technology best practice adoption rates, the situation becomes even more dire than either people or process capabilities. In fact, the only technology that a majority of companies has adopted is a corporate firewall between the plant and enterprise, and after that not even a third of companies has adopted each of the other measures.

Of all the best practices, the only capabilities a majority of companies has implemented today is:

- **Account management policy in place for the plant**
- **Conduct regular risk assessments**
- **Conduct regular penetration testing**
- **Firewall between plant and enterprise networks**

This combination doesn't even scratch the surface to address the pervasive threat industrial companies face today.

Today, what security measures are implemented in your manufacturing plants?
(N=269, all respondents)



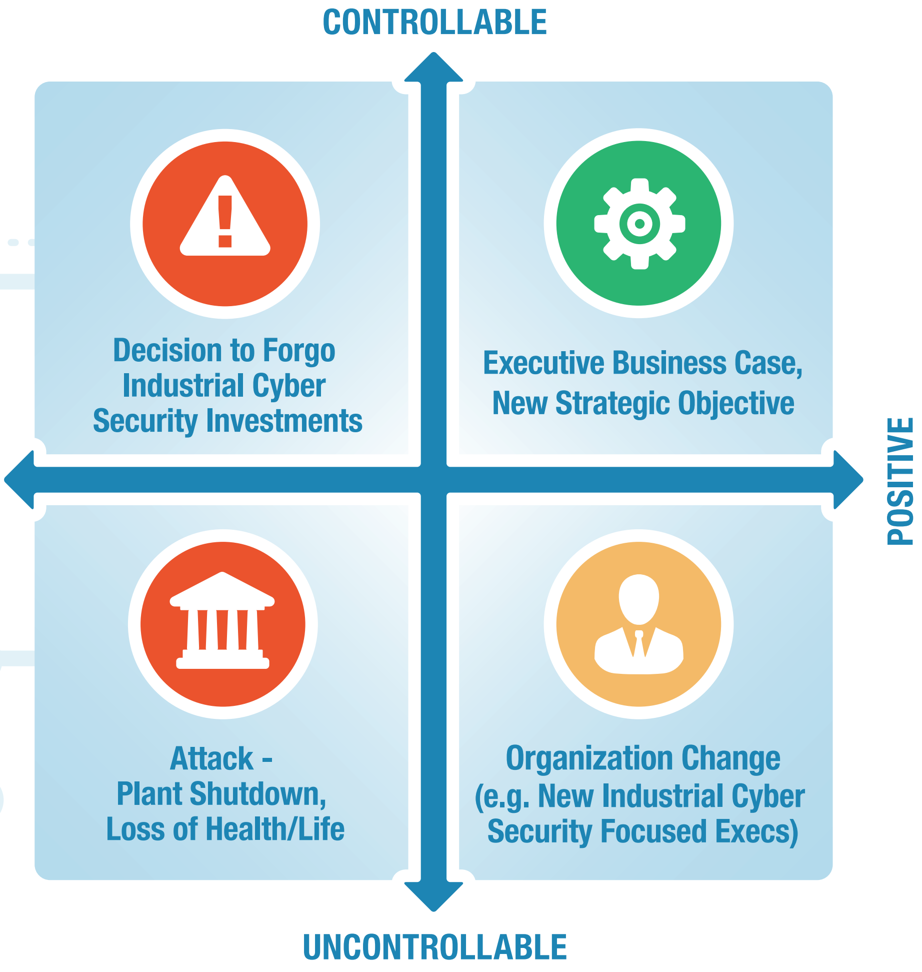
SECTION 3

Industrial Cyber Security, Change Management and the CEO Agenda

Don't Wait for Disaster

There are four types of events that drive a particular issue to the top of a CEOs agenda: a negative or positive event, and a controlled or uncontrolled event. When it comes to industrial cyber security, it is critical that companies take a proactive not reactive approach, and move to take a positive controlled approach to dealing with industrial cyber security, not negative uncontrolled.

The threat is real and pervasive, and almost every industrial company today is under-invested in necessary industrial cyber security capabilities. A company that makes industrial cyber security a top priority and invests accordingly to support Digital Transformation is in a far better position than one that finds itself on the front page of The New York Times because of a major industrial cyber security breach.

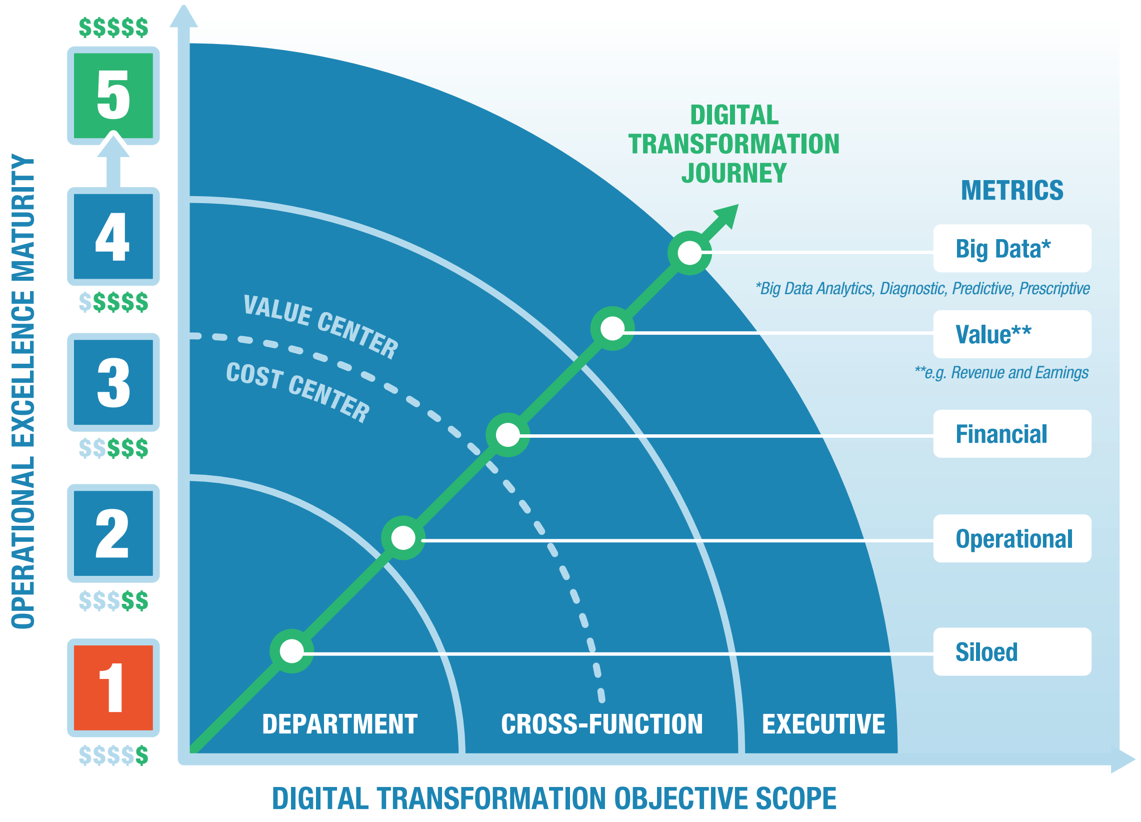

CONTROLLABLE
Decision to Forgo Industrial Cyber Security Investments
Executive Business Case, New Strategic Objective
NEGATIVE
POSITIVE
Attack - Plant Shutdown, Loss of Health/Life
Organization Change (e.g. New Industrial Cyber Security Focused Execs)
UNCONTROLLABLE

Industrial Cyber Security on Critical Path for Digital Transformation

To succeed at putting industrial cyber security on the CEOs agenda with a positive controlled event, include it on the critical path for Digital Transformation. In almost every case, companies view Digital Transformation as a journey to consider how new technologies like the IIoT can change the way data flows and business operates. Nearly every journey starts small – in departmental pilots, but as the scope increases to transforming the entire business the company must also invest in the needed people, process, and technology capabilities – especially in industrial cyber security capabilities.

Any significant industrial cyber security event could completely derail all the progress and potential success of a corporate initiative like Digital Transformation, and for this reason it is important to realize that success in Digital Transformation depends on success with industrial cyber security.

INDUSTRIAL CYBER SECURITY SUCCESS
=
DIGITAL TRANSFORMATION SUCCESS

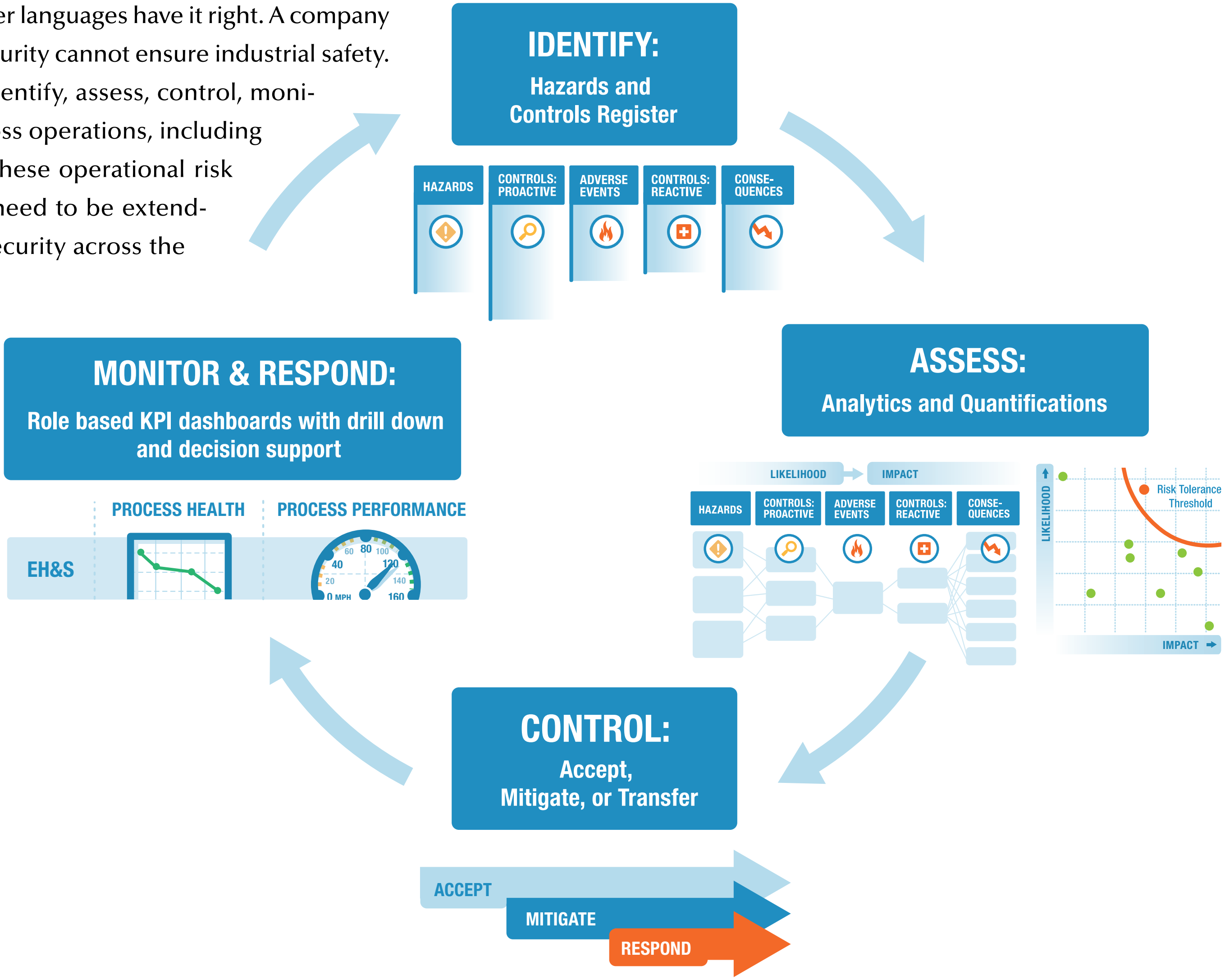

OPERATIONAL EXCELLENCE MATURITY
$$$$$
5
4
$$$$$
3
$$$$$
2
$$$$$
1
$$$$$
VALUE CENTER
COST CENTER
DIGITAL TRANSFORMATION JOURNEY
METRICS
Big Data*
*Big Data Analytics, Diagnostic, Predictive, Prescriptive
Value**
**e.g. Revenue and Earnings
Financial
Operational
Siloed
DEPARTMENT
CROSS-FUNCTION
EXECUTIVE
DIGITAL TRANSFORMATION OBJECTIVE SCOPE

Security = Safety

Finally, investing in industrial cyber security capabilities is an investment reducing risk.

In many languages other than English, "security" is the same word as "safety." Over the past 30 years, safety has moved from being an afterthought and inconvenience in industrial operations to a core value of the utmost importance. Unfortunately, most industrial companies have not yet realized that the other languages have it right. A company that doesn't ensure industrial security cannot ensure industrial safety.

Risk has long been used to identify, assess, control, monitor, and respond to hazards across operations, including and especially safety hazards. These operational risk management frameworks now need to be extended to include industrial cyber security across the lifecycle. Such a risk management framework can also be used to communicate the value of industrial cyber security investment to senior leadership because almost all senior executives are well-versed in the language and value of risk management.



IDENTIFY: Hazards and Controls Register

ASSESS: Analytics and Quantifications

CONTROL: Accept, Mitigate, or Transfer

MONITOR & RESPOND: Role based KPI dashboards with drill down and decision support

SECTION 4

Recommendations

Recommendations

To set your industrial organization up for long-term success and capture the value of next-generation technology, it is critical that industrial cyber security finds its spot on the CEO agenda. Set your company on the path with these recommended actions:

Make industrial cyber security part of the Digital Transformation Strategy. Use an Operational Excellence model of people, process, and technology capabilities to enable Digital Transformation and build industrial cyber security capabilities into the model.

Focus on best practices adoption – across people, process, and especially technology capabilities. Start with the basics like firewalls and access controls; over time move to more advanced topics like network architecture, risk management, and activity monitoring. Build a roadmap based on increasing people and process maturity that considers risk and equates safety with security. If people capabilities are limited to start, consider augmenting with external professional services that have IT and OT experience.

Focus on empowering leaders and building an organizational structure that breaks down the silos between IT and OT. A common approach across these disciplines is critical for success in industrial cyber security and it can only be done by investing time and energy in the soft skills of change management.

Author:

Matthew Littlefield
President and Principal Analyst
matthew.littlefield@lns-global.com

Connect:

ACRONYM QUICK REFERENCE
VIEW ON BLOG

Presented by:

LNS research

License to distribute this research report has been granted to:

Honeywell
THE POWER OF **CONNECTED**