bsi.

Industry 4.0

How long can you continue to ignore this cybersecurity risk?

An insights paper

Introduction

In recent years, many businesses have heightened their enterprise technology security and technology risk management measures to protect against huge cyber-intrusion and hacking increases. However, enterprise technology is only one side of the business cyber resilience equation. Operational technology (OT)—the manufacturing systems and software that control business processes and the production of goods and services—is the other. The lifeblood of business, OT arguably faces security threats even more grave than classic "enterprise IT."

The advent of 5G wireless and other trends is starting to bring far more digital intelligence into business production processes. As the Internet of Things (IoT) meets legacy OT, an entirely new set of vulnerable targets emerge. Although many companies are newly inspired by their pandemic experiences to recommit to digital transformation, these vulnerabilities could impede progress if the risks are not recognized and addressed.

2025

By 2025 there are expected to be 75 billion IoT devices connected to the Internet, resulting in even greater risks and challenges facing CISOs

Author:

Mark Brown

Global MD, BSI Cybersecurity & Information Resilience

Mark has more than 20 years of expertise in cybersecurity, data privacy and business resilience consultancy. He has previously held leadership roles at Wipro Ltd., and Ernst & Young (EY), amongst others. He brings a wealth of knowledge including extensive proficiency on the Internet of Things (IoT) and the expanding cybersecurity marketplace having worked for Fortune 10 and Fortune 500 firms as Global CISO and Global CIO/CTO respectively. He has worked, and provided services to clients across numerous sectors and industry verticals from Consumer Products, Retail/ eCommerce, Legal, Oil and Gas, Mining, Technology, Media, Manufacturing, IT and Real Estate.

mark.brown@bsigroup.com

bsigroup.com/cyber-uk

linkedin.com/in/markofsecurity

twitter.com/@markofsecurity

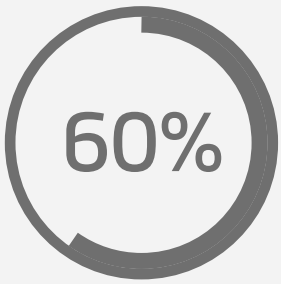
Attacks on the OT environment

When hit by a cyber-attack on their enterprise IT, most companies (although crippled) keep operating. They still have phones and pens and paper to move things along. However, the industrial environment is different. If systems go down, the impact can be instantaneous and paralyzing. If a large company's manufacturing operations are hit, costs can run into millions of dollars per hour. Troublesome evidence of such vulnerability came evidently to the fore in 2017 when the WannaCry virus hit such companies as Nissan Motors and FedEx. Another attack and well documented ransomware variant NotPetya, assaulted shipping giant Maersk and pharma leader Merck, among many others.

These ransomware attacks awakened companies, their boards, and the security community to perceived new risks, and that awareness led to significant reforms. For example, traditionally, the Chief Information Security Officer (CISO) in a company was not responsible for industrial security. However, over the past three years, more than 60% of organizations have added that responsibility to the CISOs' portfolio, with about 80% of organizations say they are now starting to address OT and IoT cybersecurity. In 2018, less than 20% of companies had any cybersecurity monitoring in their industrial environments. Today, almost two-thirds have started to do this, which is a remarkable improvement in such a short space of time, evidencing the level of organizational concern.

A concerning statistic, however, is also starting to emerge. For all their new vigilance, only 20% of organizations feel they have sufficient visibility into the assets and related systems that could be affected by an OT attack.

Organizations understand that 'you cannot secure what you cannot see' and the other 80% is right to be concerned and confused. OT is a rapidly evolving environment in which two fundamentally different sorts of technology are increasingly linked. OT is generally comprised of legacy technology often installed 20 or even 30 years ago. It's not uncommon to find Windows 7, XP, or even other legacy Windows operating systems (OS) even though Microsoft no longer supports them. Such "antiques" increasingly co-exist alongside state of the art IoT technology, and as 5G wireless takes off in the next few years, IoT will become easier to deploy and far more ubiquitous. By 2024, the world will no longer be talking about OT because it will all be the Industrial Internet of Things (IIoT).



Over the past three years, more than 60% of organizations have added industrial security responsibility to the CISOs' already overflowing portfolio

IoT vulnerability

Many offices and enterprise campuses also deploy several insecure commercial IoT systems: smart cameras, TVs, access control systems with biometrics, even smart coffee machines. Commercial IoT systems have historically been highly vulnerable as the products are predominantly consumer-focused and typically installed in homes and offices. They are plug-and-play—all you must do is download an app on your phone to control a speaker, camera, or lighting system—with little or no user authentication or password. Luckily, security will improve, at least for new IoT devices, because recent legislation in Europe and the U.S. requires it. For systems sold in America after 1 January 2020, the original equipment manufacturer (OEM) is responsible for securing them for life, and their new aftermarket responsibilities will focus attention on the evolving "license to operate."

In 2013, Target gave us all a lesson in the risks that emerge when multiple systems become interconnected. Cyber-criminals obtained vast amounts of consumer personal and financial data through a clever attack. They entered through an HVAC system connected to the internet, crossed over into OT, and accessed transaction systems connected to cash registers and point of sale (POS) systems: The kind of scenario that haunts any corporate security expert.

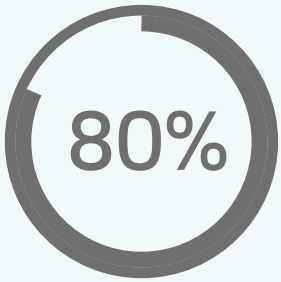
Much of OT in the past has been pretty "dumb." Actuators and sensors in a typical manufacturing environment, for example, were not digitally smart systems. They were disconnected, or in the parlance of OT and Purdue networking models, level 0 in a hierarchy that goes up to level 5 in digital sophistication. As 5G takes off, it will enable all sorts of new business capabilities, but in the process, disconnected production-level devices will rapidly be replaced with connected IoT ones. Suddenly, what was level 0 becomes level 5, maybe even connected to the cloud. Companies will go almost overnight from a highly-contained architecture where each device plays a straightforward role to smart systems with features like warnings if a machine is about to overheat. Therefore, cybersecurity risks will grow exponentially.

Upgrading OT without disruption

When a company recognizes these complex, interrelated risks, what is it to do? Our clients go through three phases. First, they must identify their assets and the risks those face in the industrial environment. Using that analysis, they set a strategy and roadmap to create new architectures and operating models. Finally, they must take concrete action to implement it all – sustainably!

It sounds good until you recognize that it is extremely tough to upgrade OT security without disrupting business, unlike in an enterprise IT environment. Those of us who work in the OT world often describe the challenge as akin to changing the wheels on a Formula One car whilst it's moving.

A commonplace occurrence when working with clients is to identify a completely converged network—all its OT, IoT, and enterprise IT is interconnected. Our task is segmenting that to give them full separation between their industrial OT and their enterprise IT. That's the kind of effort many companies need to contemplate. And, this time, we'll do it without shutting down the factory. After all, few organizations can afford to take factories out of production, even for a few days.



80% of organizations say they are now starting to address OT and IoT cybersecurity.

Commercial IoT systems have historically been highly vulnerable as the products are predominantly consumer-focused and typically installed in homes and offices.

Industry 4.0 – how long can you continue to ignore this cybersecurity risk?
Call: +1 800 862 4977 (US) / +44 345 222 1711 (UK) / +353 1 210 1711 (EMEA)
Email: cyber@bsigroup.com

Industrial OT versus Enterprise IT

Security management in industrial environments differs from the enterprise in several key ways. First, it is far harder to test incremental improvements because of the risk that errors might result in a production halt. Another key difference is the attitude of employees. They don't have to be convinced of the importance of cybersecurity. In enterprises, the security focus is on confidentiality, integrity, and availability. However, in industrial environments, that list is reversed. Availability of systems is paramount, and the only thing more important than the three is safety.

Security policies	IT network	OT/IoT controls network
Focus	Protecting intellectual property and company assets	24/7 operation, high overall equipment effectiveness (OEE)
Priorities	1. Confidentiality 2. Integrity 3. Availability	1. Safety 2. Availability 3. Integrity 4. Confidentiality
Types of data traffic	Converged network of data, voice and video	Converged network of data, control, information, safety and motion
Access control	Strict authentication and access policies	Strict physical access Simple network device access
Implications of a device failure	Continues to operate	Could stop operations and have catastrophic impact upon the wider environment depending upon process supported
Threat Protection	Shut down access to detected threat	Potentially keep operating with a detected threat
Upgrades	ASAP – during uptime	Scheduled – during downtime

In factories, genuine physical risks are abound. Employees are acutely conscious of this. As a result, they can be quite skeptical when someone from traditional enterprise IT comes in and starts instructing them in security practices.

Instead, companies with an enlightened view of OT security deploy clear and simple educational tools for employees. They might always give production workers a card to keep on them, listing the top ten tips for securing the industrial environment; things like, "Don't share your password." It's not hard to get employee cooperation if you emphasize that cybersecurity equals safety, which is, in most industrial environments, everyone's central concern.

OT Security post-pandemic

In May 2020, Fortune published the results of a survey of Fortune 500 CEOs, which found that a full 63% said one consequence of the pandemic would be a greater focus on corporate digital transformation. However, go back to our data that only 20% of companies understand the risks they face in their OT environments. If you don't know how to secure what you have, how will you implement a successful digital transformation? Either you're going to take huge risks, or you'll need an emergency program to secure the OT and IoT environment.

The World Economic Forum signaled the importance of this mindset in April 2019. They published a report, "Securing the Internet of Things is Crucial to the Fourth Industrial Revolution." As I go about my work, I remain continually surprised and disturbed how few cybersecurity and corporate risk management leaders have seen this report, even though it was released by the WEF and summarized the thinking of the world's business leaders.

Does the cybersecurity community want to help enable the Fourth Industrial Revolution? Traditionally, CISOs have had an internal reputation as naysayers, often saying, "No, you cannot do this. It would be too dangerous." However, this is a chance for security professionals to say "yes," and contribute to the heart of corporate digital transformation. By understanding and addressing the new risks, as lines blur between OT and IoT, they can enable their businesses to evolve, create more resilience, and ultimately lead to more revenue growth. It's a chance for security professionals to stand up, not just as technology leaders, but also as business leaders helping to drive their companies into a more-digital and efficient future.

By 2024, the world will no longer be talking about OT because it will all be the Industrial Internet of Things (IIoT)

How can BSI help?

At BSI, we have a large team of highly experienced, industry leading consultants that help ensure that you and your business have all the IoT security requirements you need. The team has years of industry relevant experience as well as expansive multiple sector experience, providing you with cutting edge and leading insights to ensure your IoT infrastructure and connected assets are secure and has information resilience.

BSI IoT capabilities

Our highly experienced team can support clients address their end to end IoT security requirements

- Built Environment
- Food and Retail
- Healthcare and Pharmaceuticals
- Aerospace and Automotive
- Energy and Utilities
- Banking, Financial Services and Insurance (BFSI)

Multi sector experience

Multi-faceted insights

- Connected products
- Consumerised IoT
- Industrialised IoT

- Asset scanning and identification
- On-site identification
- IoT management compliance reviews

IOT security risk assessments

Engineering & cyber skills

- IoT security strategy
- IoT security roadmap
- IoT security architecture design
- IoT security governance and controls framework

- IoT Asset and anomaly management
- IoT Firewall management
- IoT endpoint management
- IoT security operations & SIEM
- IoT vulnerability & exposure management

IoT cybersecurity technology

End to end integrated cybersecurity approach (IT, OT, & IoT)

Our approach is aligned to, but not confined to, the National Institute of Standards and Technology (NIST) cybersecurity framework which ensures that we identify threats to your IoT and connected assets through rigorous assessments and threat detection. We ensure that we can detect the threats to your organization and apply best practice governance to them. We protect you, your information, people and brand reputation via the development of an OT and IoT security roadmap and security controls framework. This is followed by responsive techniques that will move you toward success and security transformation. And lastly, we will ensure recovery in the event of a breach, which is ongoing aligned with IOT/OT asset inventory management providing assurance reporting and convergence enhancing your traditional IT security operations centre (SOC), to achieve the nirvana of CISO wants, a true single pane of glass of managed IT, OT and IoT risks.

Multiphased approach to OT and IoT cybersecurity

Identify

- Self assessment
- On-site assessment
- Automated asset detection using tools
- SIEM & SOC
- Alert & analysis
- Vulnerability management
- OT and IoT assets

Detect

- Analyze asset base and identify risk tools
- Review existing governance model
- Cyber threats
  - Maturity
  - Risk
  - Impact
  - Likelihood

Protect

- Develop OT & IoT security strategy and roadmap
- Develop OT & IoT security controls framework
- Design OT & IoT security architecture
  - Policy
  - Standards
  - Guidelines

Respond

- Implement OT & IoT security transformation roadmap
- Deploy OT & IoT security architecture
- Implement OT & IoT Security governance model

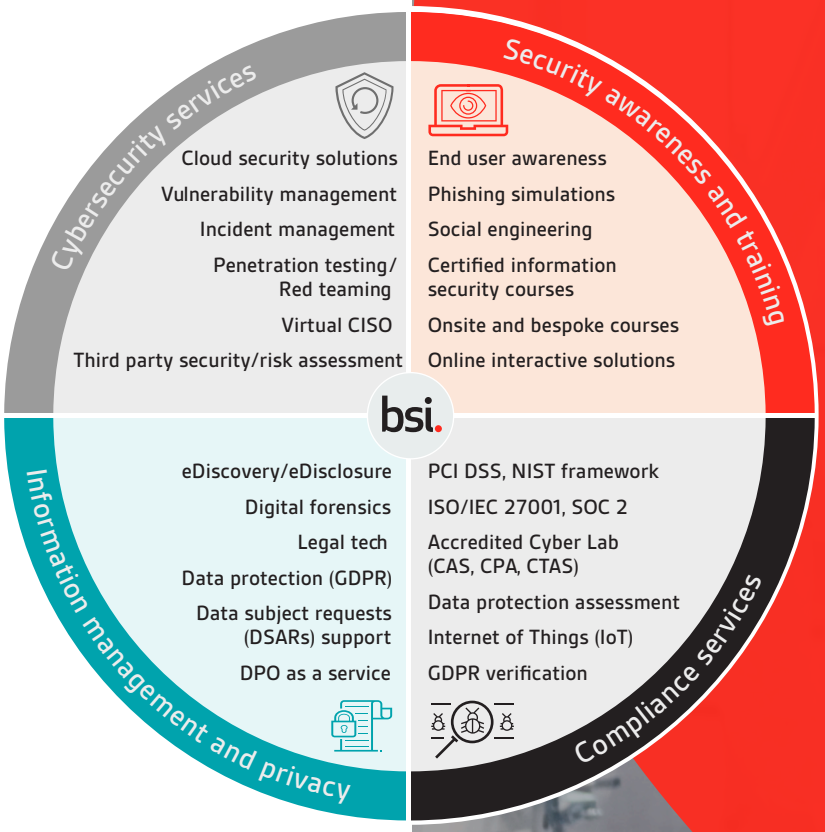
Recover

- OT & IoT asset inventory management
- OT & IoT security controls monitoring
- OT & IoT assurance reporting
- Fully convergent with traditional IT SOC design

Protect your information, people and reputation with BSI

Expertise lies at the heart of what we do. As trusted advisors of best practice, we empower you to keep your business safe through a diverse portfolio of information security solutions. Whether it's certification, product testing, and consultancy services or training and qualifying your people, we'll help you achieve your security goals.

Our Cybersecurity and Information Resilience Consultancy Services include:



Our expertise is accredited by:

Find out more

EMEA	UK	US
Call: +353 1 210 1711	+44 345 222 1711	+1 800 862 4977
Email: cyber.ie@bsigroup.com	cyber@bsigroup.com	cyber.us@bsigroup.com
Visit: bsigroup.com/cyber-ie	bsigroup.com/cyber-uk	bsigroup.com/cyber-us

bsi.