bsi.

IoT and Operational Technology:

Who should close the security gap?

An insights paper

An introduction

A new forecast from the International Data Corporation (IDC) estimates that there will be 41.6 billion connected IoT devices, or "things," generating 79.4 zettabytes (ZB) of data in 2025[1].

A significant proportion of this data comes from industrial IoT systems and this presents a different set of challenges when it comes to security and privacy.

According to David Reinsel, senior vice president, IDC's Global DataSphere. "With every new connection comes a responsibility to navigate and manage new security vulnerabilities and privacy concerns. Companies must address these data hazards as they advance to new levels of efficiency and customer experience."

According to Norton Security[2], cybercriminals will continue to use IoT devices to facilitate Distributed Denial of Service (DDoS) attacks.

Malware attacks on industrial systems became headline news a decade ago, when malware named 'Stuxnet' was discovered attacking national infrastructure. It is believed to have collected information from systems and damaged nuclear centrifuges, leading to an increase in interest from security professionals and malicious actors in industrial system security. Whilst this was a high-profile sophisticated attack, its design could be used to control a range of modern machinery and industrial processes.

Since Stuxnet, there has been a marked increase in malware targeting industrial systems, and this has been made easier due to the increase in connectivity. Attackers can create botnets and perform DDoS and ransomware attacks, as well as targeting the systems themselves.

Recently discovered issues, for example Ripple20, have shown that systems are still vulnerable. The industry must now work together to address these and other security concerns.

This paper will explore who is accountable for security and safety in industrial IoT devices, and how these complex relationships should be approached to achieve effective security through the life cycle.

1 IDC.com, 2019 - The growth in connected IOT devices is expected to generate 79.4ZB of data in 2025, according to a new IDC forecast

2. Norton.com 2020 - https://us.norton.com/internetsecurity-iot-5-predictions-for-the-future-of-iot.html

A more connected world

So many recent advances in technology have made our lives easier, and the Internet of Things is no exception. Whilst smart cities are building towards a brighter and a more futuristic tomorrow, the industrial world is not far behind with advances in manufacturing, utilities and energy.

However, these fantastic advantages come with new risks, and the entire supply chain must work together to manage the security and resilience of our Operational Technology (OT).

This paper provides an overview of the different roles within the 'cradle to grave' lifecycle, and how they work together to create greater security for OT systems.

Defining the terminology

Industry 4.0
This is considered the fourth revolution in industry, with the first three being the introduction of machines, electricity, and then digital.

IT – Information Technology
Traditional corporate technology.

OT - Operational Technology
Catch-all term to describe systems used to manage industrial equipment, assets, processes and events.

IoT – Internet of things
Connected systems that form a network, with some form of automation and a defined purpose.

ICS – Industrial Control Systems
Systems used to monitor and control industrial processes.

Industry 4.0

Our lives depend on well-run infrastructure, most of which we don't see day-to-day; from power grid control rooms to traffic signalling devices, and everything in between. Until recently most of these systems (collectively referred to as Operational Technology) were standalone i.e not connected to corporate IT systems or the Internet that operated in one geographical location. This could often mean a team of skilled maintenance engineers travelling round the country to perform ongoing maintenance.

With the convergence of OT and IoT, these systems can now be connected to corporate IT, the cloud and central management systems. Systems are suddenly easier to monitor, maintain and manage – creating a more efficient infrastructure with faster response times.

With ‘grid’ power comes ‘grid’ responsibility

Whilst increased connectivity provides faster more efficient management with lower costs, it comes with additional risks. Connecting devices increases the likelihood that a device is compromised, as there are more ways to access the interfaces. In addition, the impact of an attack increases if multiple devices can be compromised with the same attack, particularly if the devices contain Personally Identifiable Information (PII), increasing the number of people affected and any potential fines. Any organization with connected OT needs to be responsive to vulnerabilities in the ecosystem and have processes to address and manage risks.

A thorough risk assessment should be undertaken when connecting OT assets to a network, ensuring these are understood and addressed. A risk assessment should consider the assets, function and data in the network and identify threats. The likelihood and impact of threats occurring can be used to calculate the overall risk profile for the Operational Technology. This ensures relevant and appropriate controls are put in place.

Safety, Security, Resilience and Risk

From the outside, these all feel like similar concepts. It is useful for us to understand what we mean when we use these terms, and how they interact.

Safety is about preventing physical harm.

Security is about the confidentiality of data, ensuring information is correct and accurate, and available when we need it. It also includes ensuring we are confident about who is interacting with a system (also called ‘authentication’ or ‘non-repudiation’).

Information Resilience, a domain of Organizational Resilience, empowers organizations to safeguard its information – physical, digital and intellectual property – throughout its lifecycle from source to destruction. This requires the adoption of information security-minded practices enabling stakeholders to gather, store, access and use information securely and effectively.

Risk is how we measure the likelihood and consequences of something going wrong. It is helpful to understand risks and to put controls in place to either stop the risk happening as often or reduce the impact if it does happen.

In the OT world, safety is typically the number one concern.

Breaches in security can impact safety, for example, if a signalling box has poor security, data could be modified by an attacker and result in a collision on a track. Security breaches can also impact resilience, for example, Denial of Service attacks can cause unintended downtime and interruptions to service.

Resilience is also important for safety, where the availability of safety systems such as gas detectors are critical within dangerous environments.

Risk measures these things, so they can be prioritized and addressed in a reasonable and proportionate way.

Stakeholders and interested parties

There are multiple stakeholders involved in the life cycle for IoT and OT and relationships between these are usually complex, which can create issues and gaps in responsibility. A thorough understanding of the stakeholder roles and responsible parties is essential to maintaining 'cradle to grave' security.

Each of these are explained in more detail in the value chain below.

Suppliers to the manufacturers:
Suppliers may be used to provide components of software and hardware, from third-party code to PCB manufacture.

Manufacturers:
The teams which design and build the software, firmware and hardware. This also encompasses testing and fault management functions.

Installers and resellers:
The teams who work with the consumers to install the solution and set up any ongoing management or maintenance procedures. They may be part of the same organization which manufactures the solution.

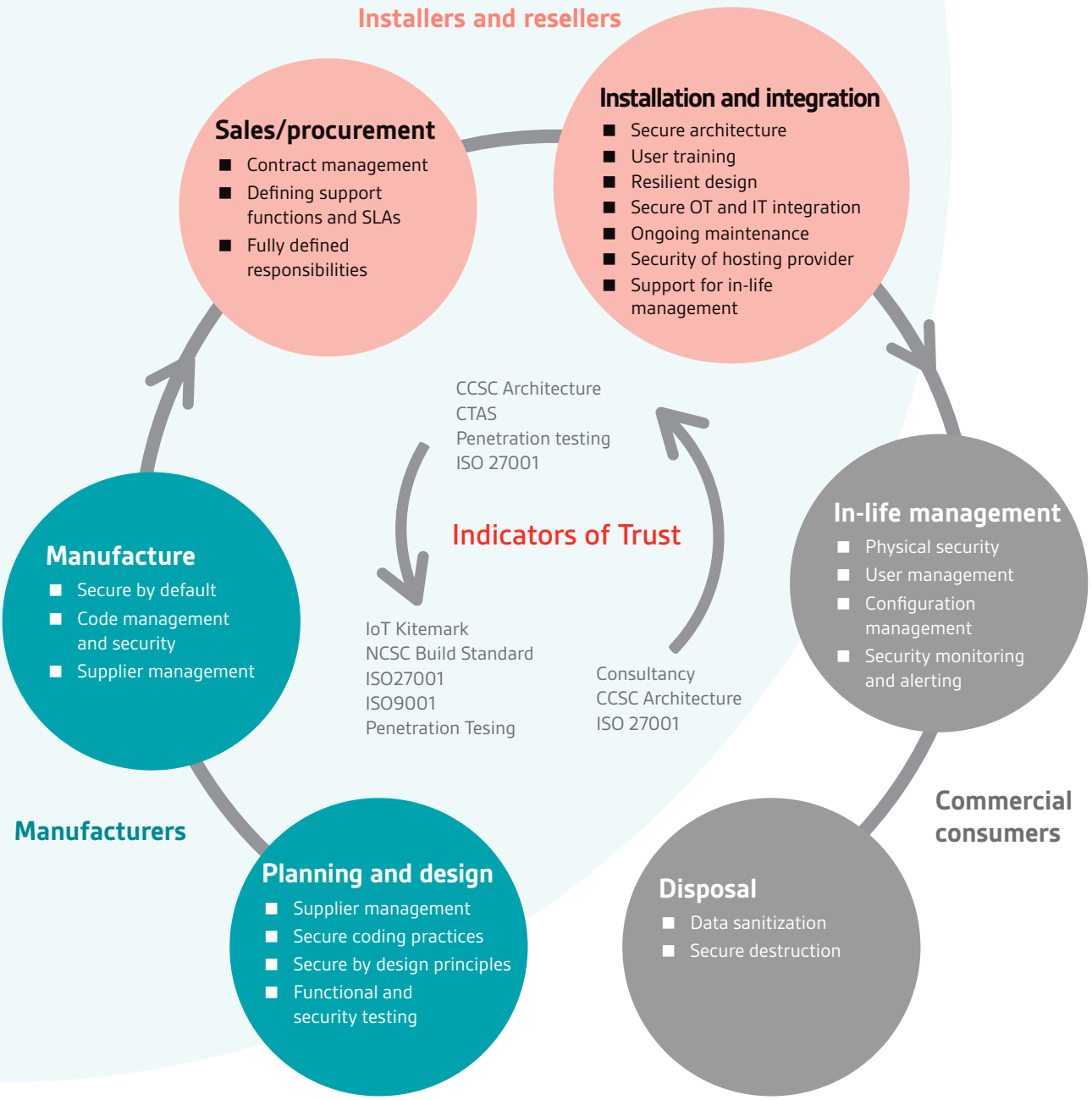
Consumers:
The commercial organizations which purchase the system. For some devices, particularly smart home devices, this group could also include individuals.

End users and employees:
The people who interact with the system day-to-day, and may have administrative access.

Accountability mapping

To address the increased risks of connected assets, the full asset lifecycle needs to be properly managed, in the same way we do for more traditional IT. The asset lifecycle covers 'cradle to grave' management and accountability. The figure below shows which organization is accountable for each stage in the lifecyle, with good practice identified for each stage. Trust needs to flow down the lifecycle, with the commercial consumers trusting the installers and resellers, who rely on good practice from the manufacturers.

Devices spend most of their lives in the 'in-life management' stage. The controls and processes for managing assets at this point rely on the previous stages being well executed. Indicators of trust can be used to help each stakeholder gain assurance around their up-stream and down-stream third parties. This allows all parties to deliver safe and secure solutions with confidence that security is managed throughout the full lifecycle.



Responsibility mapping

The table below shows how each stakeholder group is responsible for contributing to the effective implementation of the in-life security controls. This can be referenced by all parties to ensure controls provide defense in depth and are baked into the system and its ongoing operation.

	Manufacturer	Installer/Reseller	End-user
Asset management	Have uniquely identifiable devices	Suggest options for managing the asset register	Maintain an asset register, and assign owners
			Understand what the assets do and what data they hold
			Identify any unauthorized 'shadow OT' systems
Physical security	Designing physically robust devices that are difficult to break open	Advising on suitable locations for the devices	Maintaining physical security day-to-day
	Including anti-tamper and alerting functionality		Recording the physical location of devices
User management	Building devices with good user-management functionality	Changing default passwords, if they exist	Ongoing user management when staff leave or change roles
	Not using default passwords	Handing over admin accounts	Setting complex passwords
	Strong password requirements	Using unique admin credentials for each installation	User education
	Separation of privileged access		
Encryption management	Not having master keys	Not holding master keys, or using strong management processes if needed	Regularly changing any master keys, particularly when admins leave organization
	Using well-established encryption protocols with a secure implementation		
Vulnerability and configuration management	Design a 'secure by default' device	Maintaining contact and communicating when things need to be updated	Updating the systems
	Build with update function that requires cryptographically signed updates	Updating the systems	Implementing mitigating controls as required
	Have a process for reporting issues and releasing patches	Secure architecture and network separation	Day-to-day troubleshooting and support
	Build with secure communication protocols	Secure configuration	
Security monitoring and alerting	Build with ability to monitor	Suggest monitoring options	Day-to-day monitoring
		Assist with alerting settings	Maintaining and responding to alerts
Backups and resilient design	Build with ability to back up	Suggest backup options	Day-to-day backups and managing any errors
		Design resilient installation	

Conclusion

Governance and support models

In a lot of real-life implementations of OT, the consumer responsibilities are performed as part of a managed service provided by the installer or manufacturer. A governance and support model should be created to properly define and manage roles and responsibilities, with service levels documented and regularly reviewed.

All activities listed in the table should be assigned to one of the stakeholders and this should be reviewed by the consumer to ensure their legal obligations are met.
The manufacturers and installers or resellers need to provide guidance and clearly defined support services to the commercial consumers, and the manufacturers must make a secure system, monitor for vulnerabilities, and update when needed.

The convergence of IoT and OT is a unique opportunity for us to have stronger and more resilient infrastructure, whilst increasing flexibility and responsiveness to new situations. This needs to be well-managed to ensure the systems are robust and the risks fully managed, and to maintain an equivalent level of security as we currently have for standalone devices.

We have frameworks and guidance in safety and corporate IT that can be translated to the OT world, and allow the risks to be appropriately and proportionately managed. These can be used by organizations to build a connected OT environment that is safe and secure.

Most importantly, the responsibility for security in Operational Technology relies on each stakeholder group contributing to the whole. Just as security within an organization is everyone's responsibility, all parties who are involved in the device lifecycle need to take responsibility for security and resilience. This will ensure that infrastructure which may be in place for decades is as robust and resilient as possible to cyber attacks and breaches.

Trust type

By providing flexible and pragmatic support, BSI's trusted advisors enable organizations to safeguard its information, people, and reputation, assuring organizational resilience and building trust in the long term.

Intrinsic – an activity which provides confidence in the process applied by the supplier during the development of the product, service or system. **BSI's trusted advisors work with you to define and implement processes which are demonstrably and measurably secure.**

Extrinsic – an activity independent of the development environment which provides a level of trust in the product, service or system. **BSI can independently assess products and systems in a formal test lab environment to achieve information resilience under a number of schemes including the BSI kitemark and National Cyber Security Centre (NCSC) schemes.**

Implementation – any activity which provides confidence that the product, system or service has been correctly implemented. **We carry out in depth technical penetration testing of a wide range of technology implementations. Our testing team is qualified to the highest industry standards including CREST and NCSC CHECK.**

Operational - the activities necessary to maintain the product, system or service's security functionality once it has entered operational use. **BSI's trusted advisors carry out cybersecurity assessments and audits of operational systems to identify cybersecurity weaknesses and offer pragmatic solutions.**

This level of trust instilled in our clients ensures that they can achieve the desired state of information resilience, meaning this can keep them, their business, people and reputation safe and secure for the long term, withstanding the test of time.

Cybersecurity Services

Robust, industry leading processes developed through expert engagement and training

Systematic security management processes with surveillance and validation

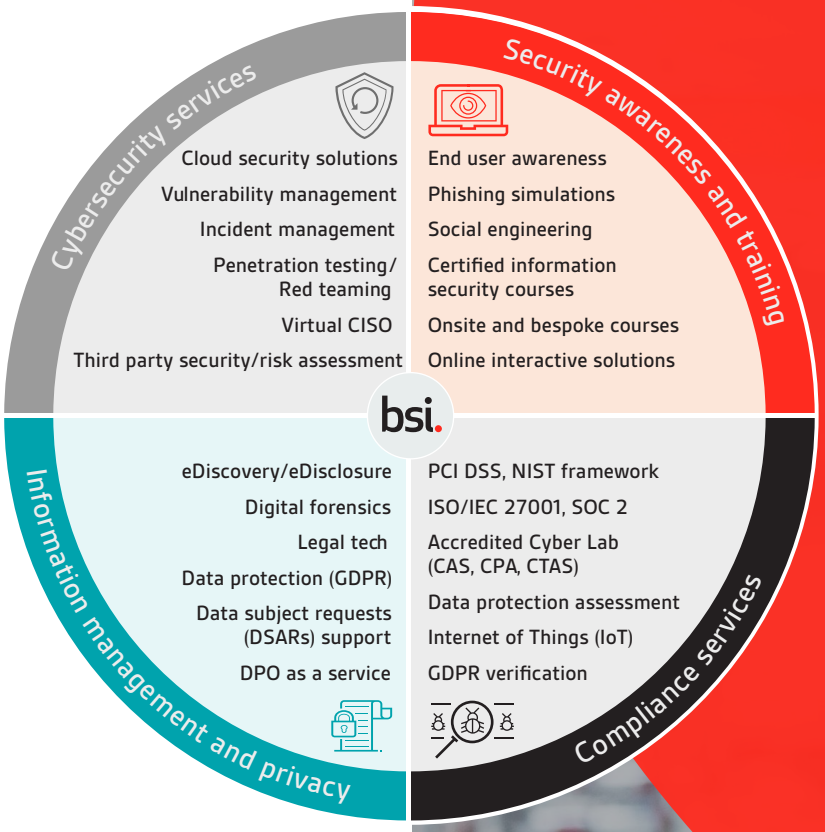
Certification and validation by trusted body

Robust, industry leading processes developed through expert engagement and training

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:

CREST · PCI Security Standards Council QUALIFIED SECURITY ASSESSOR · CYBER ESSENTIALS · CREST STAR · CHECK IT Health Check Service

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.