

Enabling Industry 4.0 and Digital Transformation by bridging IoT Security gaps

Presented by:

Mark Brown, Global Managing Director, CSIR, BSI

David Mudd, IoT Product Certification Director, BSI

Isabel Forkin, Head of Cyberlab Services, CSIR, BSI



By Royal Charter

bsi.



Mark Brown

Global Managing Director
Cybersecurity & Information Resilience

E: mark.brown@bsigroup.com



David Mudd

IoT Certification Director
Assurance Services

E: david.mudd@bsigroup.com

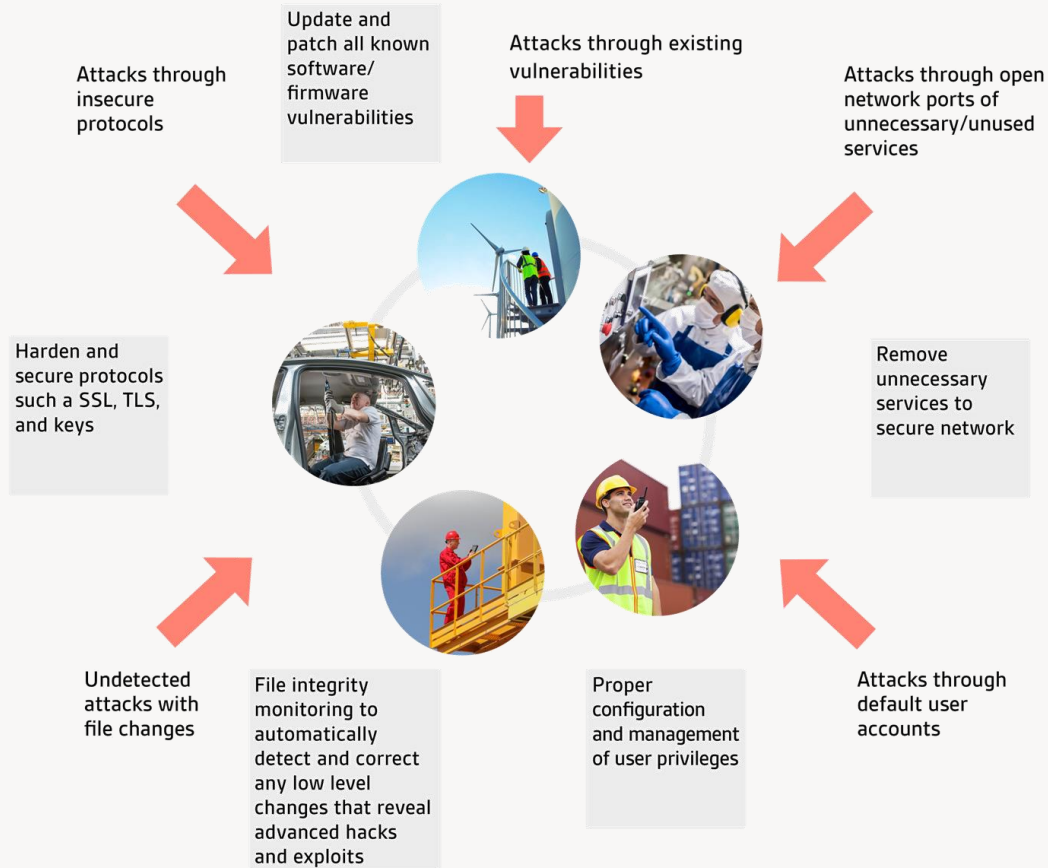


Isabel Forkin

Head of Cyberlab Services
Cyber Security & Information Resilience

E: isabel.forkin@bsigroup.com

The cybersecurity challenge for Industry 4.0



Common IoT Security exposures and the solutions recommend to resolve

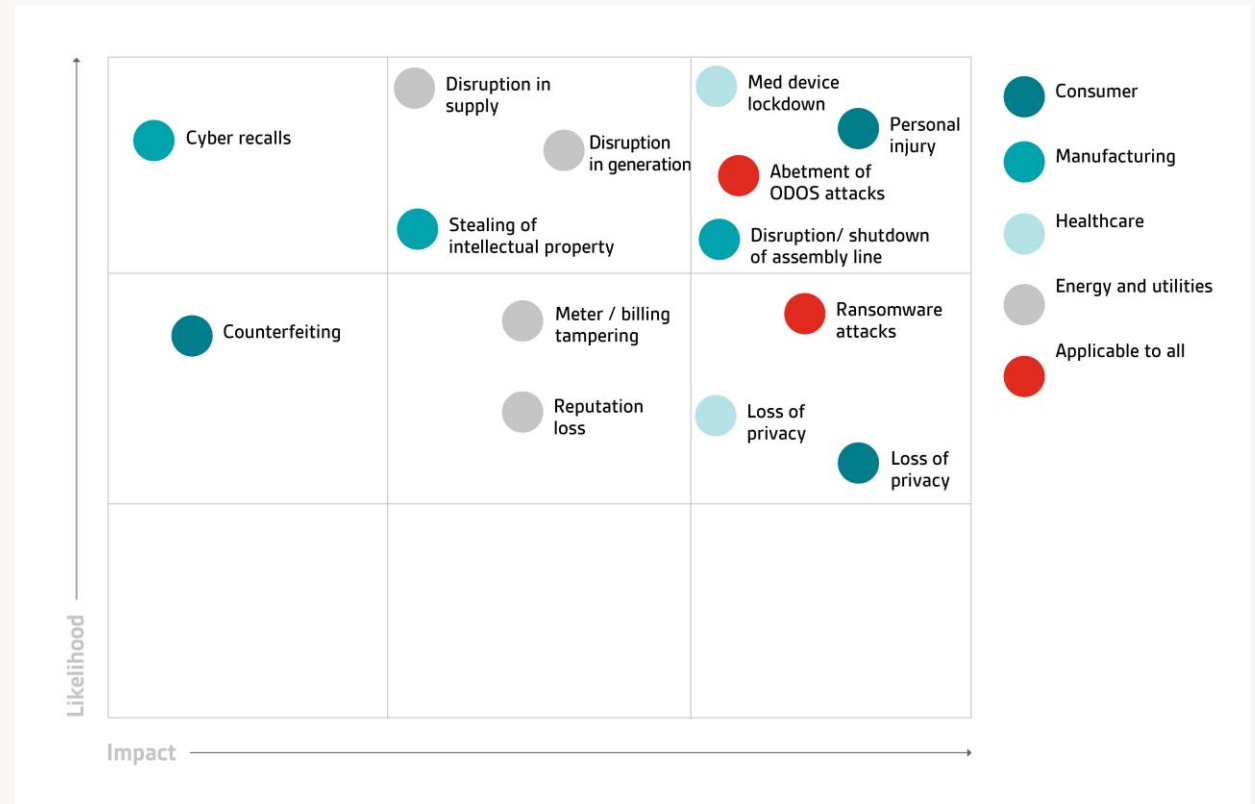
IoT has already made its way into many aspects of the way people live and work today and it's only set to grow, with experts **predicting as many as 75 billion by 2025**. As the number of connected devices continue to grow, so too will the volume and **variety of vulnerabilities** many of which have existed for years, lying dormant, and are only now being discovered.

Vulnerabilities in IoT devices are becoming more wide-ranging, and with **greater potential impact** if exploited. Securing IoT isn't easy for manufacturers to get right, but security should be viewed as an **enabler of the IoT's growth**, rather than a barrier, and baked in from the start.

IoT is not restricted to consumer devices. The rise in automation in the **manufacturing/engineering sectors** has seen the advent of the **Industrial Internet of Things (IIoT)**, which itself has led to something of a shift in mind-set as the technology brings the operational world and the **IT world closer together**.

Why society and industry needs to address Industry 4.0 Cybersecurity risks?

- Static credential and lack of encrypted communications are resulting in a **mass insecurity** impacting consumers and enterprise alike
- Many of the IoT devices have issues with **outdated firmware** of weak default passwords which make them perpetually **vulnerable** and **easy to compromise**
- The value of IoT is in the data and data **needs to be protected**. A failure to ensure that the data is secured can result in the risks illustrated as they apply to key sectors.



How can BSI help?

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

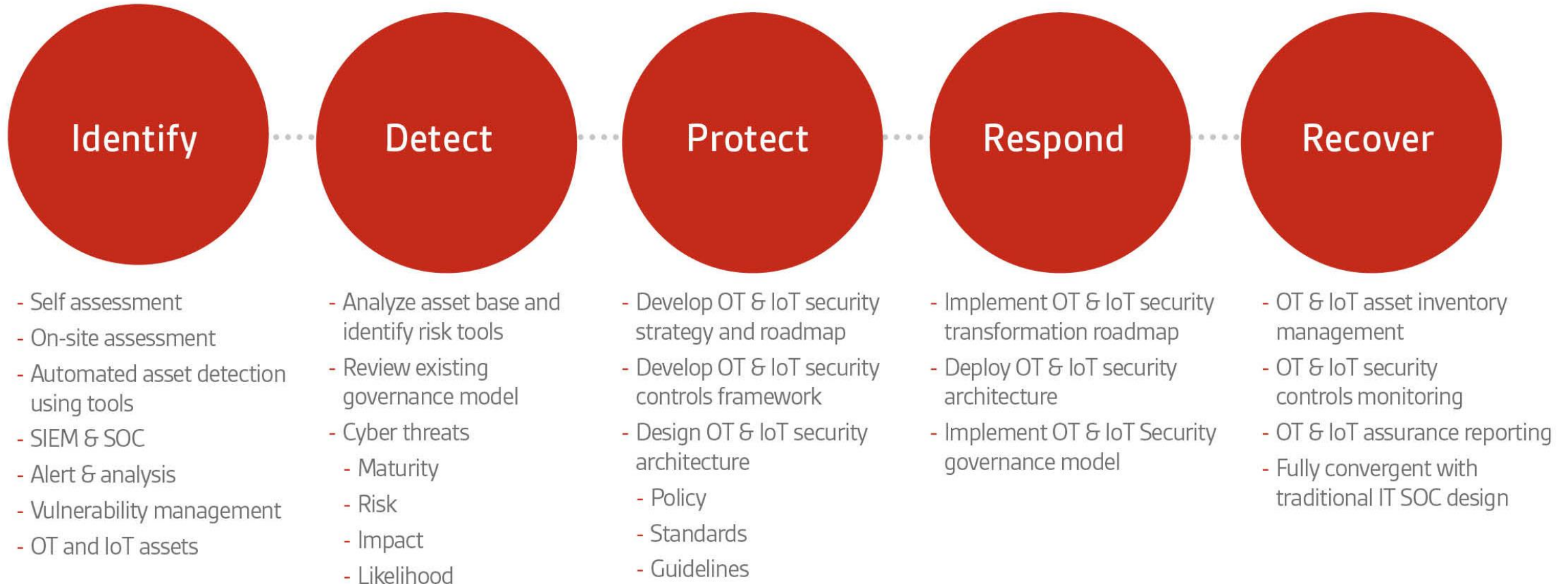
- IoT security strategy
- IoT security roadmap
- IoT security architecture design
- IoT security governance and controls framework

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

IoT cybersecurity technology

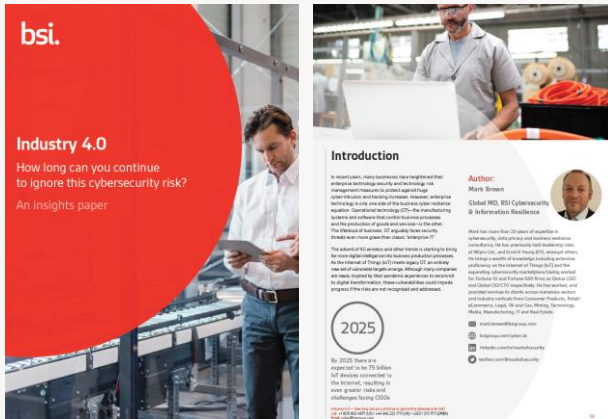
..... End to end integrated cybersecurity approach (IT, OT, & IoT)

A multiphased approach to OT and IoT cybersecurity



Connect with us

- Download the insights paper: **Industry 4.0 – How long can you continue to ignore cybersecurity risk?**




[Click here to download](#)

Get in contact:

 bsigroup.com/cyber-uk

 mark.brown@bsigroup.com

 linkedin.com/in/markofsecurity

 twitter.com/@markofsecurity