Protecting our critical infrastructure

Understanding new cyber security laws

Author
Dr Richard Piggin
Principal Operational Technology Cyber Security Consultant, Atkins

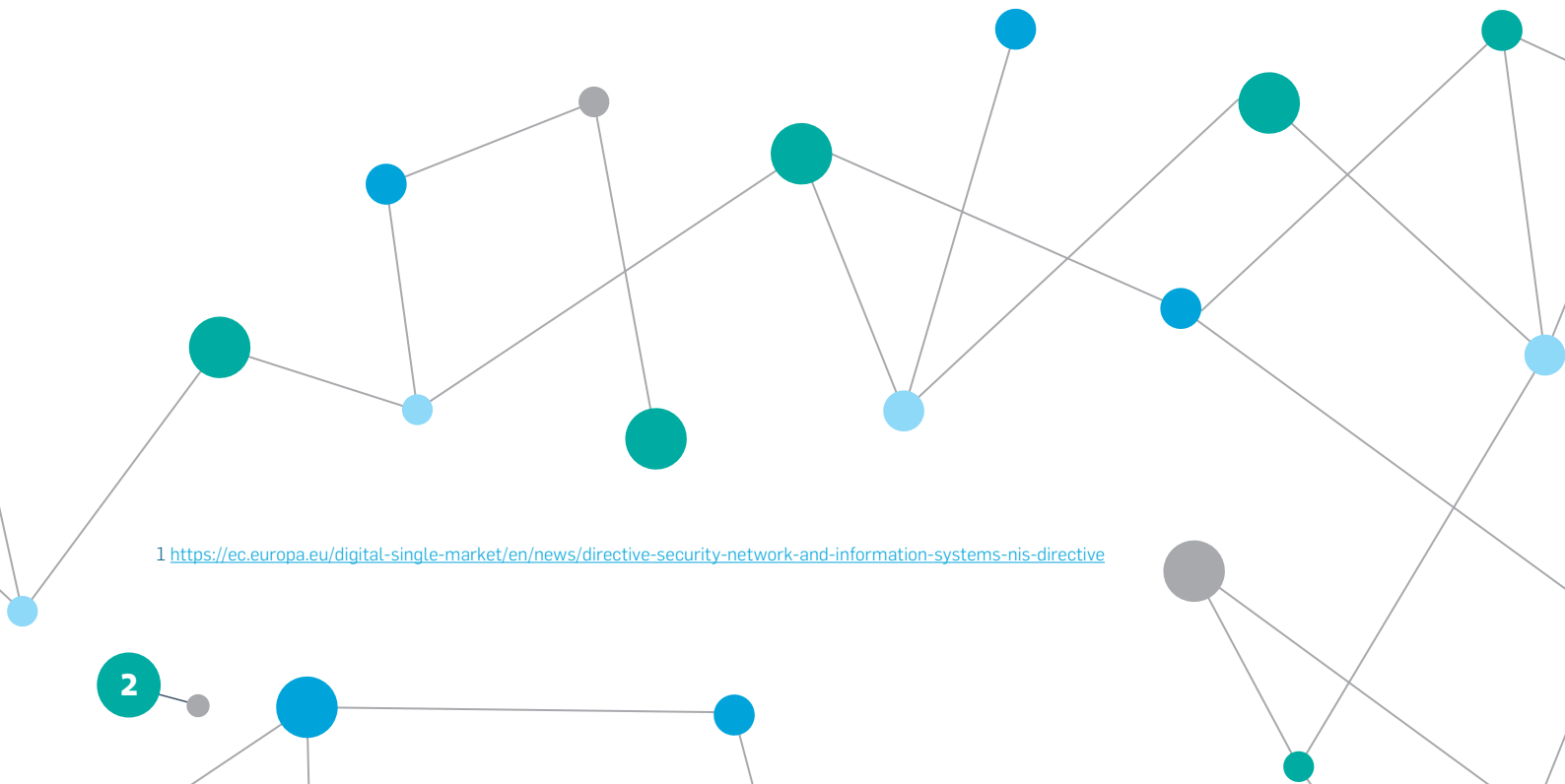
www.atkinsglobal.com/NISD

Introduction

Operators of the UK's essential services face fines of up to £17 million if they fail to comply with strict, new cyber security laws.

From 10 May 2018 organisations must be able to demonstrate that they understand the threat to their network and systems and have wide-reaching measures in place to detect and manage a security breach.

The Network and Information Systems Directive (NIS Directive), proposed by the European Union, seeks to protect our vital infrastructure from increasingly sophisticated attacks[1]. In this paper, we offer our insight into the regulations and ask what they mean for the UK. We consider how the structure, processes, policies and systems within companies may change to meet the requirements, and we highlight the resources and expertise needed to comply. Finally, we discuss the impact of the new rules on the supply chain, and consider the action operators should take to avoid a hefty penalty.



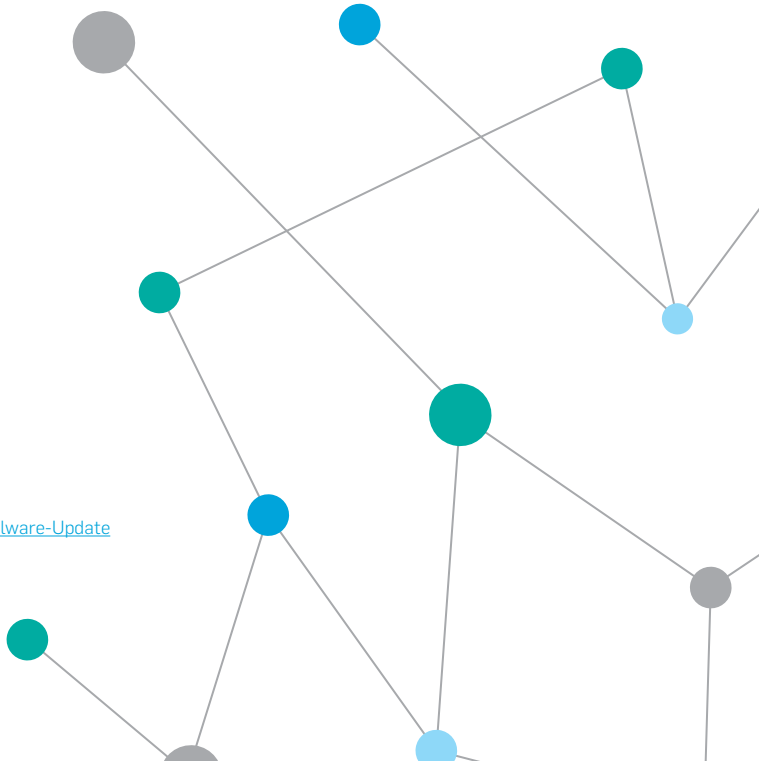
1 https://ec.europa.eu/digital-single-market/en/news/directive-security-network-and-information-systems-nis-directive

Protecting critical services safeguards the economy, society, and people's wellbeing

The resilience of critical services highlights the requirement to secure not only information systems, but the technologies that are relied upon to operate essential services; known as cyber physical systems, industrial control systems (ICS) or operational technology (OT)[2]. Their disruption or failure can impact many people and cost millions, with potentially severe consequences.

The recent watershed attack (HatMan) late last year targeted a Schneider Electric Triconex safety shutdown system in the Middle East (widely reported to be the Saudi Arabian oil and gas sector), stopping critical infrastructure plant operations. This incident illustrates the increasing capability and intent to attack specific critical infrastructure, and the motivation to compromise safety systems.*

Recent destructive attacks include NotPetya, which masqueraded as ransomware. Reckitt Benckiser, the consumer products manufacturer (brands include Dettol, Nurofen and Durex) predicted £100 million losses. The transport and logistics company Maersk declared losses exceeding $300 million. Fedex estimated losses to be more than $500 million. The pharmaceutical company Merck anticipated losses to exceed $600 million and needed to borrow paediatric vaccine from US Government contingency stocks to meet demand, following manufacturing disruption. Black Energy and Industroyer/ CrashOverride attacks both targeted the Ukrainian power grid. The WannaCry ransomware afected the NHS, manufacturing plants, telecoms, transport and energy organisations globally. These highlight the necessity for proportionate risk-based cyber security and more importantly, operational resilience.



2 https://www.ncsc.gov.uk/topics/operational-technology

* https://ics-cert.us-cert.gov/MAR-17-352-01-HatMan-Safety-System-Targeted-Malware-Update

The Network and Information Systems (NIS) Directive

The new legislation aims to protect the networks and information systems that underpin society and facilitate economic growth - that is, our energy, transport, water, and digital infrastructure and our healthcare services.

It is relevant to all European Union (EU) member states but its introduction has been overshadowed by high-profile changes to personal data protection laws (General Data Protection Regulation or GDPR), which are also effective from May 2018.

The Directive (implemented under the Network and Information Systems Regulations 2018 domestic legislation[3]) requires operators to secure information systems and the technologies they rely on to operate essential services; known as cyber physical systems, industrial control systems or operational technology.

High-profile cyber attacks

HatMan, Triton or Trisis (2017)
TARGET: Safety systems in the oil and gas sector, Middle East
Article link: Safety System Targeted Malware

NotPetya (2017)
TARGET: Corporate and government systems in Ukraine and then large, multinational companies elsewhere
Article link: Russian Military Almost Certainly Responsible Destructive 2017 Cyber Attack

WannaCry (2017)
TARGET: The NHS, manufacturing plants, telecoms, transport and energy organisations globally
Article link: Combating the menace of ransomware in critical infrastructure

Mirai botnet (2016)
TARGET: US domain name system infrastructure
Article link: www.us-cert.gov/ncas/alerts/TA16-288A

Crash Override or Industroyer (2016)
TARGET: Ukrainian power grid
Article link: Responding to another ukrainian power attack

BlackEnergy 3 (2015)
TARGET: Ukrainian power grid
Article link: Learning from ukraines power grid malware

Massive damage to steelworks (2014)
TARGET: German Steel Plant
Article link: Targeting industrial plant

Havex/DragonFly (2014)
TARGET: European energy systems
Article link: Industrial control systems and SCADA cyber security

Stuxnet (2010)
TARGET: Nuclear enrichment plant in Natanz, Iran
Article link: Control network security lessons from stuxnet

3 http://www.legislation.gov.uk/uksi/2018/506/contents/made

> These systems can be an attractive target for malicious actors, and they can also be susceptible to disruption through single points of failure. Incidents affecting any of these systems could cause significant damage to the UK's infrastructure, economy, or result in substantial financial losses.[4]
>
> UK Government

NIS Directive

KEY DATES

2013

March
Negotiation by the Council of Member States and the European Parliament commences

2015

May
NIS Directive approved by the Council

July
NIS Directive approved by the European Parliament Published in the Official Journal of the European Union

December
European Parliament and Council Agreement

2016

NIS Directive transposition into national legalisation commences

2017

August
DCMS Industry consultation – the Government published its proposals for improving the security of the UK's essential services, with the implementation of the NIS Directive

2018

April
NIS Regulations laid before Parliament

9 May
Implementation deadline for the NIS Directive implementation by Member States

10 May
Entry into force

4 https://www.ncsc.gov.uk/guidance/introduction-nis-directive

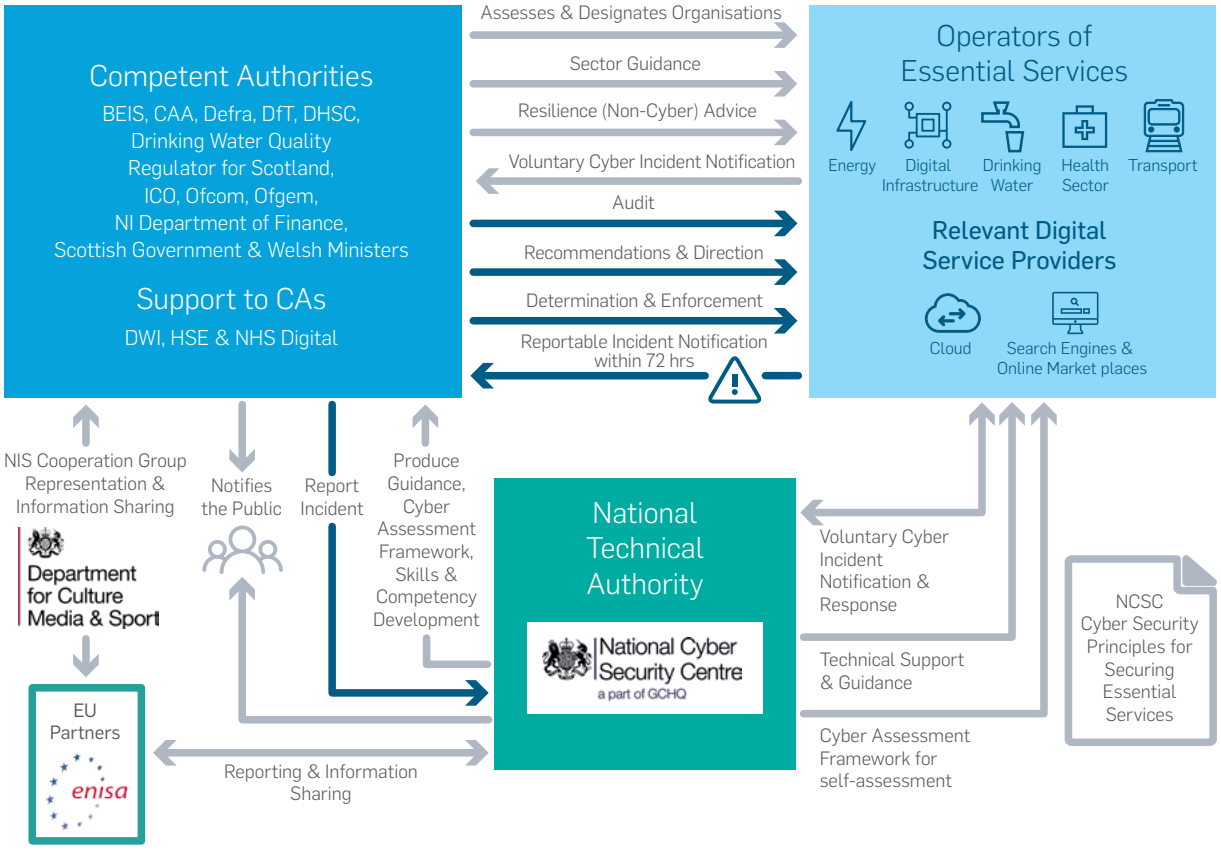
* The Government has stated its intention that the policy will continue to apply following the UK's exit from the EU.

Improving security and resilience

The NIS Directive[5] is part of the EU Digital Market Strategy, which helps to ensure member states benefit from the opportunities presented by the digital economy and seeks to position Europe at the forefront of developments.

Technology has already transformed entire sectors and the latest advances will enable us to drive greater efficiency and productivity, and improve safety within our industries. But increasingly sophisticated technology has a downside too. In recent years, cyber security incidents have become more frequent and disruptive. They threaten the supply of critical services, and undermine trust in digital systems and products.

The new legislation recognises what is at stake and aims to improve overall security and resilience against a cyber attack. In the UK, it applies to essential services, including key digital infrastructure. Digital service providers with 50 or more staff and/or a turnover of more than £8.5 million (€10 million) will have similar, but less onerous requirements. The implementation excludes the nuclear, banking and financial sectors.



5 https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive

Who is responsible for protecting our infrastructure?

Operators of essential services must manage their risks by implementing 'appropriate and proportionate security measures'. They are also required to notify the relevant national authority of serious incidents.

Member states
Set national strategy and foster collaboration

Competent authorities (lead govt depts, devolved administrations, existing regulators)
Monitoring and oversight of NIS implementation in their sector

Operators of essential services (as defined by the Government)
Put appropriate security measures in place and notify authorities in the event of an incident

National technical authority (National Cyber Security Centre)
Provide technical support/guidance to affected organisations. Point of contact for EU partners. (It is not a regulatory role.)

European Union Agency for Network and Information Security (ENISA)
Supports member states in the implementation of the Directive

The public
To be notified in the event of a serious incident

The Directive has been shaped around four high-level objectives:

1. Appropriate organisational structures, policies, and processes to understand, assess and manage security risks;
2. Proportionate security measures to protect essential services and systems;
3. Capabilities to ensure defences remain effective and detect cyber security events;
4. Capabilities to minimise the impacts of a cyber security incident on the delivery of essential services including the restoration of those services where necessary.

The UK has expanded on the objectives to form a number of security principles, which describe the outcomes that must be achieved. Organisations should review the requirements and the guidance available from the National Cyber Security Centre (NCSC)[6]. The NCSC has referenced a broad range of existing guidance and good practice (individual examples do not necessarily provide adequate coverage), which align with established cyber security frameworks[7]. Other guidance and its application will be less familiar, including operational technology[8] cyber security.

6 https://www.ncsc.gov.uk/guidance/nis-directive-top-level-objectives
7 https://www.ncsc.gov.uk/guidance/table-view-principles-and-related-guidance
8 https://www.ncsc.gov.uk/topics/operational-technology

Knowing what action to take

The NCSC has not set out to produce an all-encompassing compliance check list. Instead, it requires organisations to be capable of taking informed, balanced decisions about how they achieve the outcomes specified within the principles.

The NCSC's expectation[9] is for the operators of essential services to:

Understand the principles and why they are important. Interpret the principles for the organisation.

Compare the outcomes described in the principles to the organisation's current practices. Use the guidance to inform the comparison.

Identify shortcomings and understand how serious they are by using organisational context and priorities.

Implement prioritised remediation. Use the guidance to inform remediation activities.

The NCSC guidance has deliberate similarities with the US National Institute of Standards and Technology (NIST) Cyber Security Framework, including referring to good practice or standards. Both contain recognised industry cyber security frameworks such as the ISO/IEC 27001/27002 standard series and for operational technology, the IEC 62443 series.

The NCSC has also developed the cyber assessment framework (CAF) in support of the regulations[10]. It enables organisations to perform their own assessments against the objectives and principles, and identify ways to improve their cyber security. It also fulfils an omission from the Directive - the absence of a cyber maturity framework.

The CAF is intentionally less complex than other cyber security maturity models. It utilises a red, amber, green (RAG) methodology and highlights good practice. However, its simplicity could also create challenges for operators. It will emphasise the interpretation of results, which could be difficult early on. Organisations may also struggle to show tangible or continuous improvement to help them justify investment.

9 https://www.ncsc.gov.uk/guidance/introduction-nis-directive

10 https://www.ncsc.gov.uk/guidance/nis-directive-cyber-assessment-framework

Training and education requirements

Operational technology requires different skills to IT systems. Critical infrastructure security practitioners appreciate the scarcity of specific skills and suitable experience.

The proposed EU Cybersecurity Act (Article 4) sets the European Union Agency for Network and Information Security (ENISA) objectives for skills and competency development and certification, and for becoming a centre of expertise on cyber security.

Organisations affected by the new legislation may not have the resources or the expertise to act quickly to upgrade their cyber security, or to fully integrate cyber security governance and operations with their engineering functions. Therefore, technical training, education and senior- leadership awareness programmes will be vital to maintaining compliance. Competent authorities (CAs) will also need to develop or acquire cyber security capability and auditing expertise.

Demonstrating compliance

Companies may need to seek the support of engineering and operational technology specialists to help them go beyond an approach that is relevant to traditional information systems and instead appropriately protect operational technology.

Operators are advised to carry out an assessment of their internal processes against the Directive, NCSC guidance and emerging CA requirements. They will need to identify and address areas that need improvement and demonstrate how their cyber security programmes meet all of the requirements.

They will be supported by the relevant CAs. The Authorities' initial focus will be on developing a detailed understanding of security within their sector, and working with operators to assess areas in need of further development[11]. CAs are encouraged to take a cautious approach to enforcement during the first year. However, the Government has emphasised they do have the power to issue penalties if significant compliance issues arise, and if organisations have not made an effort to remedy them[12].

Combining an outcome focus with risk management and cyber maturity assessment will provide greater business resilience and benefits over chasing compliance.

11 https://www.gov.uk/government/publications/nis-regulations-guidance-for-competent-authorities
12 https://www.gov.uk/government/consultations/consultation-on-the-security-of-network-and-information-systems-directive

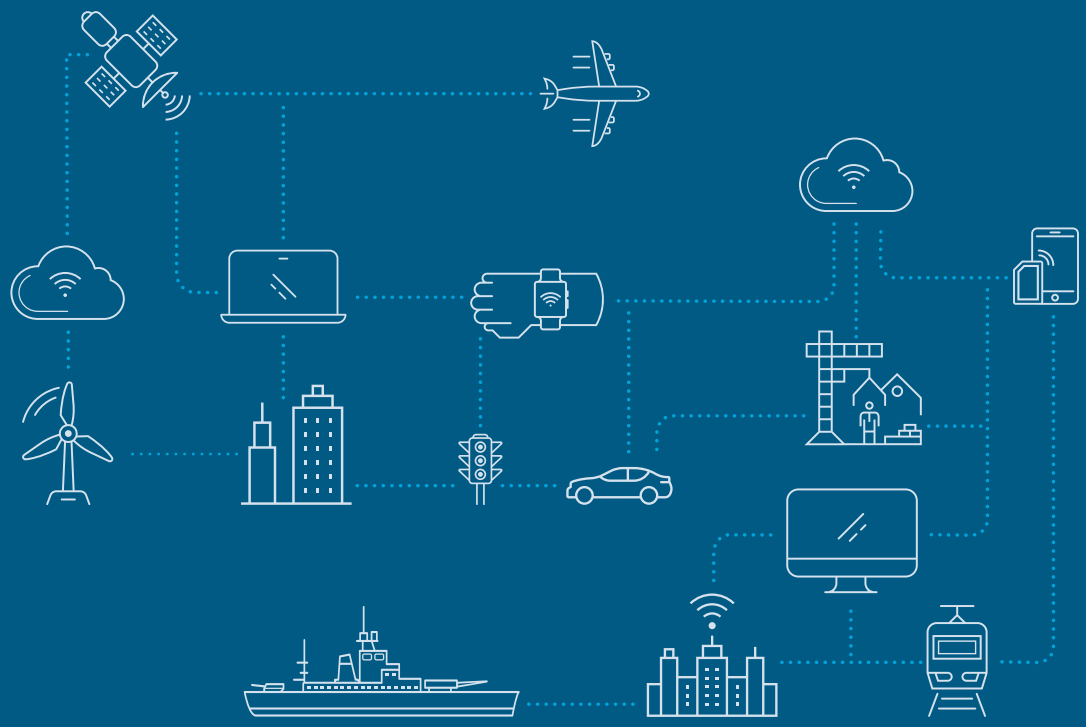
How do the changes affect suppliers?

Operators of essential services are responsible for compliance within their supply chain too, so consideration should be given to the way third party services, systems and components are procured.

Operators should assess their approach to security lifecycle management, including specifying (non-functional) cyber security requirements in their contracts, and subcontracts. Suppliers are not expected to have a direct obligation but they are likely to be contractually obliged to comply.

Operators and suppliers will benefit from working towards common goals. Using shared procurement language and guidelines to ensure objectives are integrated into systems and services will help.

Procurement specifications should cover all aspects of cyber security, including acceptance testing, verification, integration, maintenance guidance and any supporting references (guidelines, regulation or standards). Supply chain cyber security features in the NCSC guidance, and in recent operational technology standards, including the IEC 62443 series.



Recommendations

The NIS Directive, implemented under the UK regulations, will concentrate Board members' attention on cyber security and resilience, and highlight the requirement to exercise good judgment when critical services are reliant upon networks, information systems and operational technologies. To meet the requirements organisations should:

Review the requirements and the guidance available from the National Cyber Security Centre (NCSC)[13].

Assess their readiness and capability to meet the NIS Directive security objectives and NCSC principles.
This includes providing proportionate risk prevention measures, and mechanisms to detect and deal with breaches, report incidents and maintain service resilience.

Seek the support of engineering and operational technology specialists if additional resource or expertise is needed to appropriately protect services.

Develop a common set of security expectations to underpin relationships with suppliers.
For example, a shared procurement language and guidelines to ensure good practice.

Please note that evidence of cyber security capability and practices that protect essential services will be necessary to avoid potential non-compliance.

Combining an outcome focus with risk management and cyber maturity assessment will provide greater business resilience and benefits over chasing compliance.

13 https://www.ncsc.gov.uk/guidance/introduction-nis-directive

www.atkinsglobal.com/cyber

SNC·LAVALIN

ATKINS
Member of the SNC-Lavalin Gr

About the author

Dr Richard Piggin
Principal Operational Technology
Cyber Security Consultant

Richard is a security consultant at SNC-Lavalin's Atkins business. He has an Engineering Doctorate in industrial networking from the University of Warwick and has since focused on networking, technology evangelism, international standards, safety and security. He is a member of the IEC standards working group bridging safety and security. Richard also chairs the Institution of Engineering and Technology (IET) Cyber Security Technical Professional Network, a thriving community that enjoys membership from across all of the Institution's sectors. At Atkins, Richard is working with clients to make their Operational Technology resilient against current and emerging threats.

Linkedin

Atkins Angles articles

© Atkins Limited except where stated otherwise.