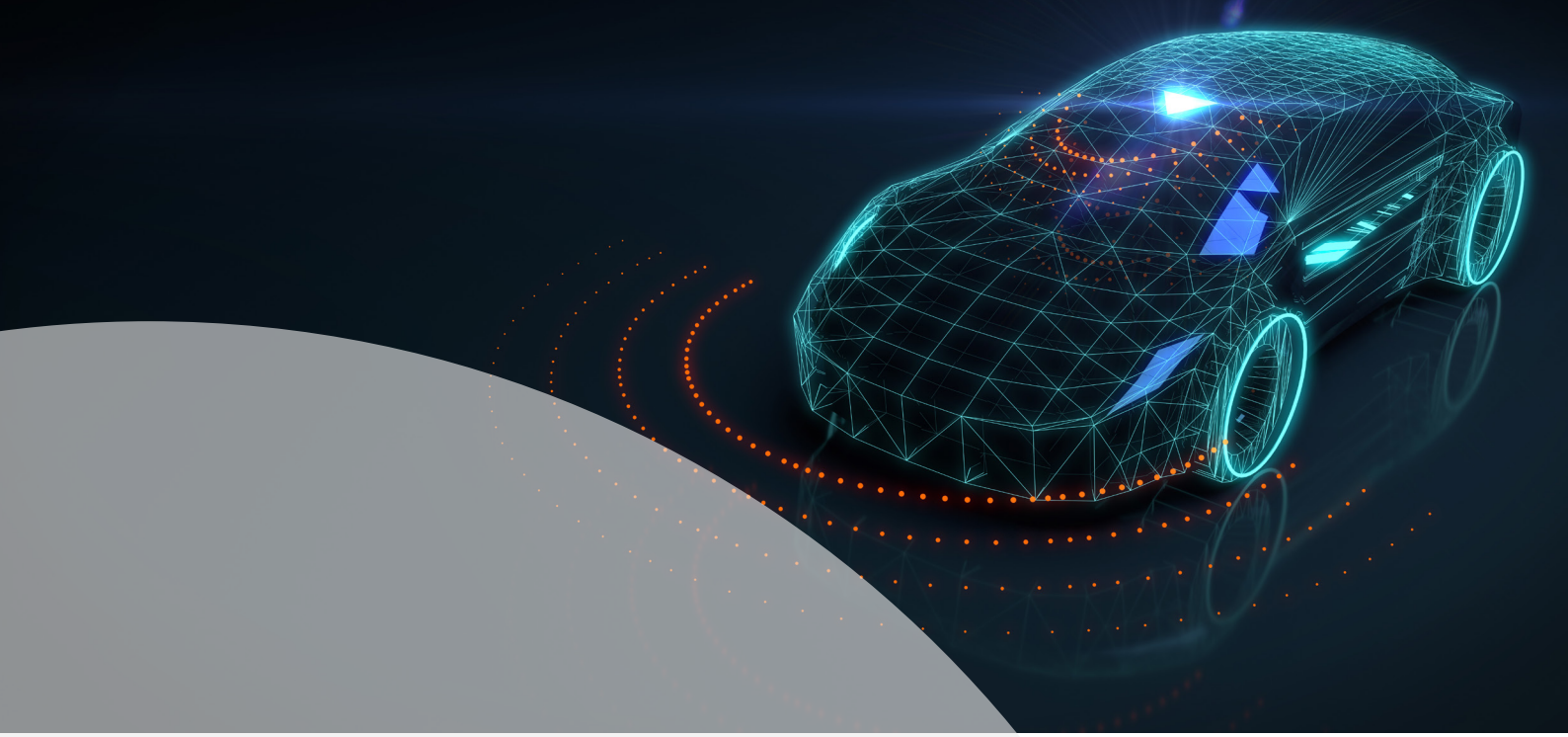
bsi.

Automotive cybersecurity

Addressing the challenges of a sector in transformation and preparing to meet new cyber compliance burdens (ISO/SAE 21434)

An insights paper



The cybersecurity paradigm of connected automotive

Connected, autonomous vehicles and self-driving cars, as a concept are nothing new. Experiments were conducted on automated driving systems (ADS) back in the 1920s[1] and trials began as early as the 1950s. In 1977, Japan's Tsukuba Mechanical Engineering Laboratory developed the first self-driving car which required specially marked streets that were interpreted by two cameras on the vehicle via an analogue computer. Miraculously, the vehicle reached speeds up to 30 kilometers per hour (19 mph) with the support of an elevated rail.[2]

Nearly 50 years later, the landscape looks very different through a series of disruptive and sustained innovative technologies, the automotive industry has advanced beyond all expectations. In line with Industry 4.0, cyber physical systems and the acceleration of digitization, the industry is gearing up to an enormous change in 2021. For example, AI-based autonomous vehicles are the frontrunners in the automotive industry whilst Artificial Intelligence is already enabling smart travel methods through self-driving cars which do not require drivers and rely on sensors and software for navigation and control. Moreover, according to Research and Markets (2020)[3], connectivity is increasingly no longer an optional feature for vehicles but embedded by design. The automotive industry is in the midst of a massive transformation, where automakers are no longer hardware makers but are evolving into tech companies, and represents the largest change to the automotive sector since the invention of the combustion engine.

Author:

Mark Brown

Global MD, BSI Cybersecurity & Information Resilience

Mark joined BSI in February 2021 and is responsible for overall driving the growth of the Consulting Services business stream – Cybersecurity and Information Resilience – at a global level, harnessing a key focus on the Internet of Things (IoT) strategy and how BSI can help clients bridge their cybersecurity and data governance challenges.

Mark has more than 25 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

1 'Phantom Auto' will tour city". The Milwaukee Sentinel. 8 December 1926. Retrieved 23 July 2013.
2 Vanderblit, Tom (6 February 2012). "Autonomous Cars Through The Ages". Wired. Retrieved 26 July 2018.
3 Global Connected Car Market Outlook, 2020 Source

The cybersecurity paradigm

Like anything connected to the internet, there are risks, vulnerabilities, and threats everywhere. As Brian Krebs, American Journalist, and Investigative Reporter attests4, "everything gets hacked" and 'businesses and IT professionals need to start accepting the "depressing reality"'. The connected automotive industry is no exception.

The list of examples is endless. Notable data breaches extend from Honda in 2017 with WannaCry, the notorious and well publicized ransomware crippled their computer systems globally, in 2018, thousands of files of factory records from Tesla Inc., Toyota Motor Corp. and Volkswagen, along with Fiat Chrysler Automobiles, Ford Motor Co. and General Motors, were found in a data leak this month that exposed several of the companies' trade secrets. More recently, in 2020, Tesla filed a lawsuit against a former employee after it emerged the employee made changes to company source code and exported gigabytes of proprietary data to unknown third parties, launching an insider attack with mass ramifications.

Other key trends in the automotive and connected marketspace are equally conspicuous.

- Car-as-a-marketplace or "car commerce" is fueling veritable demand in the automotive retail and vehicle payment systems through enabling the end user to reserve, order, and buy everything within an on-route journey
- Features on demand which is a subscription-based service being offered by the original equipment manufacturers (OEMs) for the likes of lighting on demand, night vision assistant and navigations maps
- Intelligent transport systems where there is a large focus on tracking demographic, movements and designing systems like Cedric/E Palette which shared mobility as a theme
- Neutral server platforms where legislation is currently being planned to protect the interest of the automotive aftermarket players

The estimated number of connected vehicles in the global automotive market by 2025[5]

Of business may rely on data-enabled services and shared mobility by 2030[5]

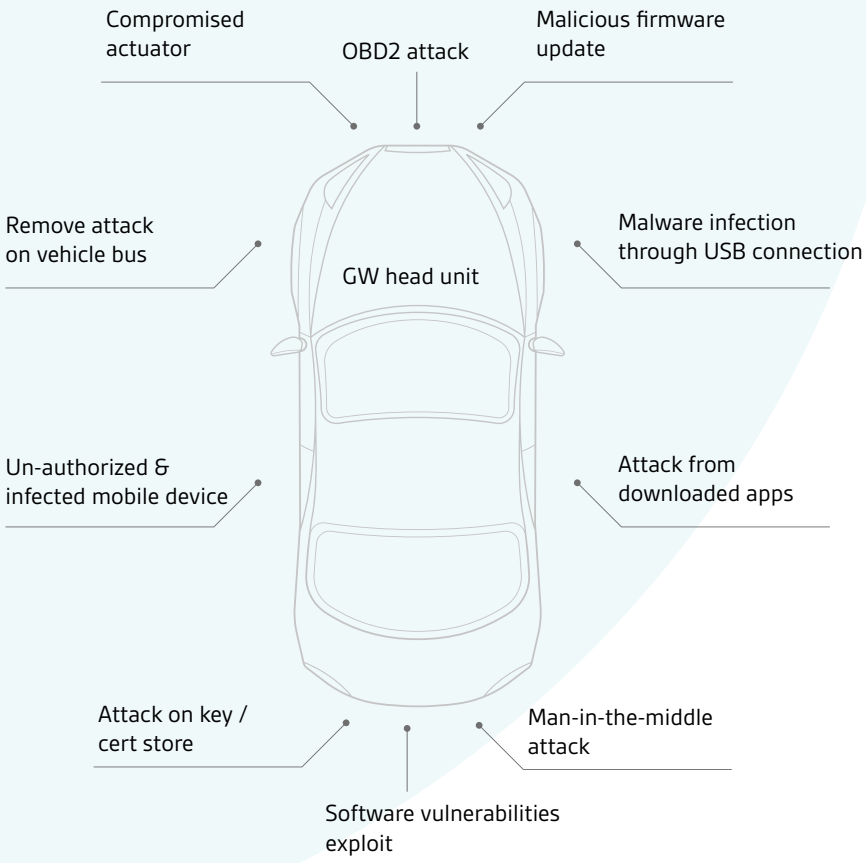
Automotive cybersecurity
Call: +1 800 862 4977 (US) / +44 345 222 1711 (UK) / +353 1 210 1711 (EMEA)
Email cyber@bsigroup.com

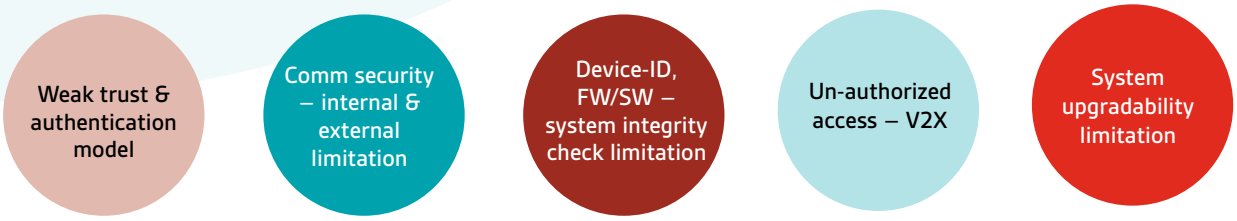
4 Brian Krebs BSI's International Cyber Resilience Exchange 2019 source
5. Upstream Security: Global Automotive Cybersecurity Report 2021

Connected automotive threat vectors

The biggest challenge our clients see is how to stay protected against the ubiquitous threat with the threat vectors that circle a car are omnipresent and malicious in nature. Take malware infection through a USB Connection. We all know the ramifications of plugging an unprotected and unknown USB into any device is dangerous and a car USB port is no different. There is also the threat of attacks from downloaded apps that the end user might have on their can dashboard and CPU. Like any application, cloud based or on prem, they need to be validated and security checked before downloaded. These applications in a car should follow the same rigor and vigilance before downloading. Man-in-the-middle (MATM) attacks are also prevalent, where the attacker covertly relays and possibly alters the communications between two parties who believe that they are directly communicating with each other, like eavesdropping. These can be remediated in numerous ways by authentication, like key-agreement protocols, tamper detection where a normal process might take a bit longer than normally and digital forensics. The latter is obviously advanced means, but a suspected attack can be checked and monitored using incident forensics and details if the data was comprised, where this happened and provide threat intelligence to remediate the situation.

Automotive cybersecurity – addressing the challenges of a sector in transformation





Connected automotive threat vectors

Another challenge facing this sector has been the lack of technical cybersecurity compliance standards resulting in a lack of standardization in the industry. Until the advent of ISO/SAE 21434, no connected automotive cybersecurity standard existed in the marketplace.

The ISO standard establishes "cybersecurity by design" throughout the entire lifecycle of the vehicle. ISO/ SAE 21434 provides the model for developing a risk assessment system and specifies details on processes and work products.

The overall process for ISO/SAE 21434 compliance can be broken down into three phases:

- Assessment, which includes scoping and the evaluation of status. The result should be a compatible framework
- Implementation, which covers the cybersecurity organization (based on ISO/SAE 21434), definition of the risks, people, and tools, and finalization of the organization orchestration
- Operations, which consists of monitoring, evaluation and continuous processes. It leads to the launch of the CSMS, which is followed by a type of approval.

Challenge: Compliance with existing Automobile Security Standards

ISO/IEC Standards	SAE* International standards
ISO/IEC 9797-1: Security techniques – Message Authentication Codes	J2945: Dedicated Short Range Communications (DSRC) Minimum Performance Requirements
ISO/IEC 11889: Trusted Platform Module	J3061: Cybersecurity Guidebook for Cyber-Physical Vehicle Systems
ISO 12207: Systems and software engineering – Software life cycle processes	J3101: Requirements for Hardware-Protected Security for Ground Vehicle Application Examples of other industry and government security initiatives include:
ISO 26262: Functional safety for road vehicles	• E-safety Vehicle Intrusion Commission Protection Applications (EVITA): Co-founded by the European Commission, it is an architecture for secure on-board automotive networks, with a focus on protecting components from compromise due to tampering other faults
ISO 27034: Application security techniques	• Secure Hardware Extensions (SHE): From the German OEM consortium Hersteller Initiative Software *HIS), these on-chip extensions provide a set of cryptographic services to the application layer and isolate the keys
ISO 29119: Software testing standard	
IEC 62443: Industrial Network and System Security	
Until ISO/SAE 21434 was formalized no CONNECTED AUTOMOTIVE security specific standards or regulations existed *	

*SAE – Society of Automotive Engineers

Another challenge facing business has been the lack of cybersecurity compliance and lack of standardization in the industry

Automotive cybersecurity
Call: +1 800 862 4977 (US) / +44 345 222 1711 (UK) / +353 1 210 1711 (EMEA)
Email: cyber@bsigroup.com

ISO/SAE 21434 overview

ISO/SAE 21434 covers all stages of a vehicle's lifecycle from design through to decommissioning by the application of cybersecurity engineering. The standard applies to all electronic systems, components, and software in the vehicle, plus any external connectivity. Moreover, the standard will provide developers with an overarching approach to implementing security safeguards that spans the entire supply chain, and protects the lifecycle of the vehicle.

The importance of the standard is unequivocal and a first for the industry. With the increase in connectivity in vehicles, such as Wi-Fi, Bluetooth and future 5G connectivity as well as the development of autonomous cars, the risks of cyberattack and the subsequent damage also increases. Current safety-critical standards are not sufficient to cover this type of risk and therefore new guidelines and standards needed to be established.

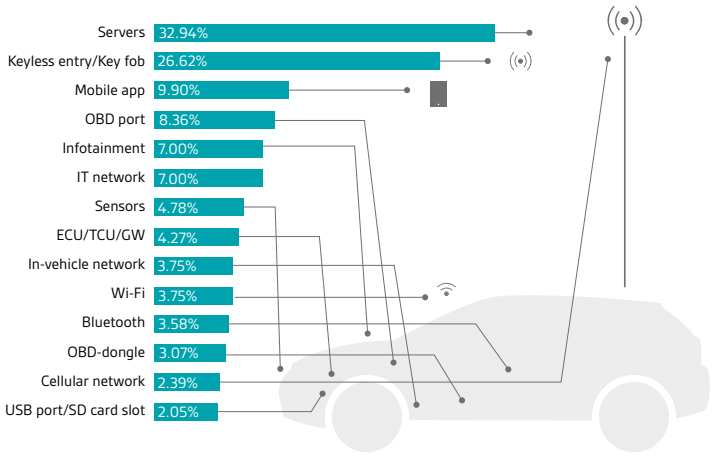
The intent behind the standard is to provide a structured process to ensure that cybersecurity considerations are incorporated into automotive products throughout their lifetime. Furthermore, the standard will require automotive OEMs and suppliers alike to demonstrate due diligence in the implementation of cybersecurity engineering and that cybersecurity management is applied throughout the supply chain to support it.

It is intended that organizations will encourage a cybersecurity culture so that everything is designed with security considerations from the start a la, security by design.

How BSI can 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 connected automotive 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 IoT infrastructure and connected assets are secure and has information resilience, backed by leading edge innovative alliances specializing in IoT, connected systems and automotive security.

Most common attack vectors[5]



Value Proposition: Our connected automotive cybersecurity responses

Unified trust model

- Enables trust for Smartphones applications and vehicle systems
- Eliminates unauthorized access issues

Security model for safety and data privacy

- Real-time device authenticity validation
- Coupled relationship between device identity and data
- Only trusted entities can participate in the interactions

Use access control & authorization

- Eliminates unauthorized access to vehicles
- Provide granular policy control for access privileges

Flexible platform

- Token based access control
- PKI management and automation
- Platform adaptable to business & customer needs
- High scalable and flexible platform-based solutions

Automation and support for enterprise security vendor ecosystem

- HSM integration and support
- Public certificate authority and private PKI options
- Future proof, flexible options

Ongoing near real-time connected car security

- Vehicle SOC

Automotive cybersecurity
Call: +1 800 862 4977 (US) / +44 345 222 1711 (UK) / +353 1 210 1711 (EMEA)
Email: cyber@bsigroup.com

5. Upstream Security: Global Automotive Cybersecurity Report 2021

BSI's Cybersecurity solutions approach – an end to end services model

BSI has constructed an E2E connected automotive cybersecurity model that is broken out across three pillars:

1. **Strategic consulting**: through a holistic consulting model, using the teams' experience, we firstly conduct a threat modeling framework with risk matrices and design. Then, we look at the security model and design the relevant roadmap and look at areas such as trust and identity, supply chain integration and controls and assurance through product certification. We can then create an ISO/SAE 21434 aligned and compliant security architecture, operation integration, third party risk and compliance on controls and checks.
2. **Security engineering and assurance**: we look at the lifecycle of the Security Bill of Materials (Sec BoM) and analyze, through a series of security testing, from build all the way through to a series of both purple and red teaming engagement. This includes adversary and attack simulations to defense and protection techniques, in the event of a data breach or vector attack, in the pathway to ensure that the cycle is robust and secure, ensuring information resilience.
3. **Compliance services**: lastly, on the E2E model we check the controls and methodologies against leading standards from IACS to CC-ITSE and also against regulations like the EU GDPR on data protection and privacy management and FIPS compliance. As a last check we then check these against best in class security test models such as OWASP's ASVS and embedded controls and MITRE 's ATT&CK framework among others. This iterative approach is proven to simplify achieving ISO/SAE 21434 compliance.

Value proposition: BSI's E2E connected automotive cybersecurity services model

Strategic consulting

Security requirements validation:

- Use-case analysis || Threat modeling & operational risk metrics design

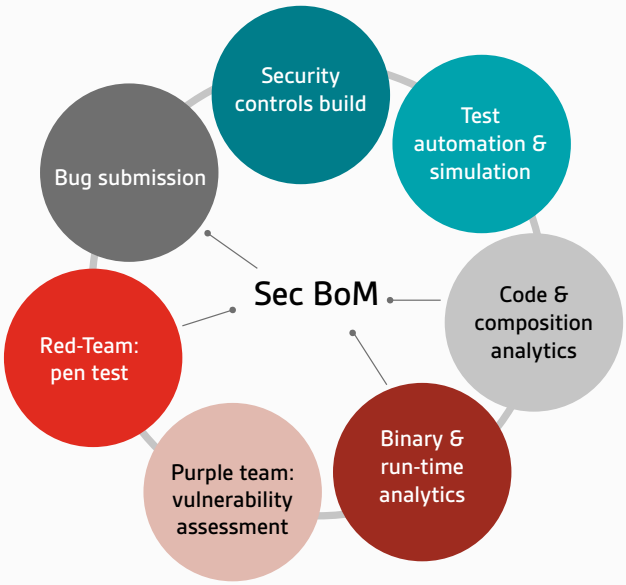
Security model & roadmap

- Trust & Identity model design
- Supply-chain integration controls
- Security assurance, product certification & compliance controls design

Product market-fit validation (prototype)

- Security architecture prototype
- Operational integration validation
- Certification & compliance controls check

Security engineering & assurance



Compliance

Standard and framework:

- ISA/IEC: 62443 (IACS)
- ISO/NEC: 15408 (CC-ITSE)
- NIST 800-82 | CSF 1.1
- TISAX compliance
- FIPS compliance | ISO 19790
- EU GDPR
- ISO/SAE 21434

Security test model: 3 level | 17 categories | 211 test cases

- OWASP: ASVS & embedded controls
- MITRE ATT&CK framework & STRIDE threat model
- ISO-29147 & 30111 (vulnerability disclose & handling)

Operate

Governance, risk & compliance roadmap

Asset monitoring & anomaly detection

Vulnerability assessment

***

Penetration testing

Threat monitoring & incident response

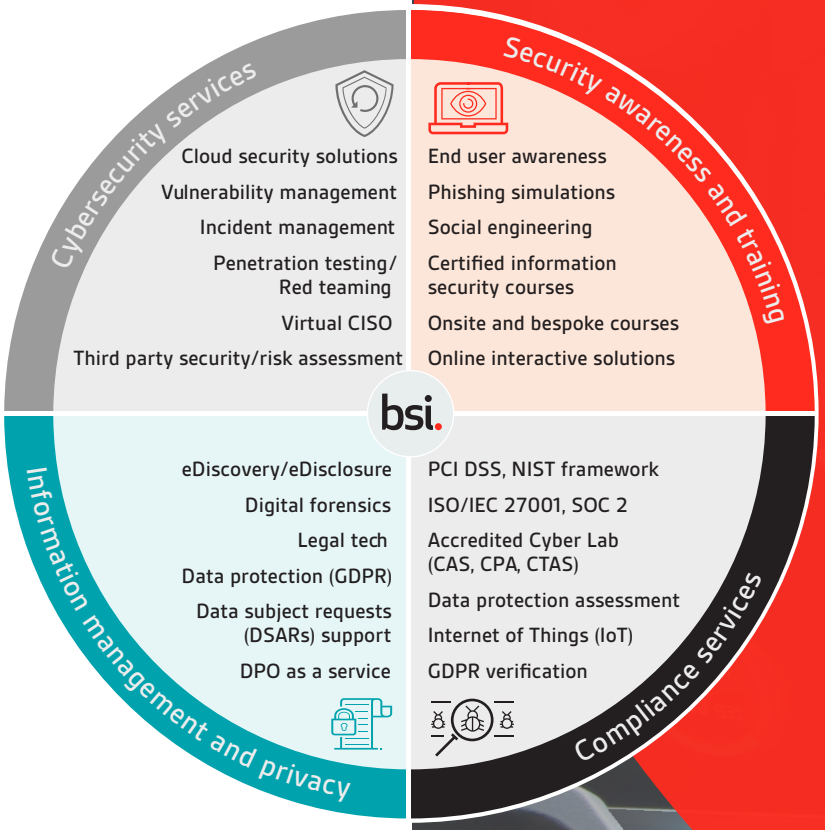
Security information & event management

Risk & compliance management

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.