Cloud computing

Understanding cloud security

A whitepaper

bsi.

...making excellence a habit.™

Introduction

Cloud computing provides the speed and agility that digital businesses require along with potentially significant cost savings and generating new sources of revenue. Gartner projects cloud computing to be a $300 billion business by 2021. Although, Gartner's emerging risk report results clearly show that organizations continue to struggle with cloud security.

Cloud security is a major component of cybersecurity. Cloud resources can help cybersecurity engineers and organizations predict and defeat attacks in real time, use big data and analytics over a large pool of end users to proactively address and predict threats.

Gartner suggests, "Organizations must invest in security skills and governance tools that build the necessary knowledge base to keep up with the rapid pace of cloud development and innovation."

It is essential for organizations to understand the security concerns in cloud computing in order to effectively adopt and use cloud solutions.

This whitepaper provides a general overview of cloud computing, its risks, ownership of risks, best practices and solutions for any organization or individual who wants to learn and understand cloud computing and its security. It also discusses cloud security standards and the General Data Protection Regulation (GDPR) on cloud computing, its impact and ways to remain compliant with the regulation.

Call: +44 345 222 1711 /+353 1 210 1711 Email: cyber@bsigroup.com Visit: bsigroup.com

What is cloud computing?

The National Institute of Standards and Technology (NIST) defines cloud computing as a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models.

Essential characteristics

1. **On-demand self-service:** Cloud computing consumers can independently provision their computing resources such as network storage and server time automatically without requiring human interaction with each Cloud Service Provider (CSP)
2. **Broad network access:** Cloud computing resources are accessible over the network through regular mechanisms, supporting heterogeneous thin or thick client platforms such as mobile devices, workstations, laptops and tablets
3. **Resource pooling:** CSPs computing resources are integrated to serve multiple customers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to the customer demand
4. **Rapid elasticity or expansion:** Cloud computing resources can be elastically provisioned and released automatically or on-demand based on certain criteria or triggers. These characteristics allow your applications to have the ability it needs at any point in time
5. **Measured service:** Cloud resource usage can be monitored, controlled, measured, and reported (billed), providing transparency for both the consumer and provider of the used service. In short, it can be described as pay for what you use

Service models

1. **Software as a Service (SaaS):** SaaS is a cloud offering that allows consumers to use the provider's applications or software running on a cloud infrastructure. The customers do not control or manage the underlying cloud infrastructure, do not need to install the application or software on their local devices, accessible through a client interface such as web browser
    a. **Examples:** Google Apps, Dropbox, Salesforce, Cisco WebEx, Netflix, Gmail, Microsoft Office 365, etc
2. **Platform as a Service (PaaS):** PaaS is a cloud offering that provides consumers with a cloud environment in which the cloud consumers can develop, manage and deliver applications created using programming languages, libraries, services and tools supported by the CSP
    b. **Examples:** Amazon Web Services (Elastic Beanstalk, etc.), Microsoft Azure, Heroku, Force.com, Google App Engine and OpenShift
3. **Infrastructure as a Service (IaaS):** IaaS is a cloud offering in which a CSP provides customers access to cloud computing resources such as servers, storage and networking. Organizations use their own applications and platforms within a CSPs infrastructure
    c. **Examples:** Amazon Web Services (AWS) (EC2, etc.), Microsoft Azure, Google Compute Engine (GCE) and Rackspace

Deployment models

1. **Public cloud:** As the name suggests, the cloud infrastructure is provisioned for open use by the public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on prem organizations of CSP
2. **Private cloud:** The infrastructure of the private cloud is provisioned for private use by a single organization comprising multiple consumers (e.g.business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises
3. **Hybrid cloud:** The infrastructure of the Hybrid cloud is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g. cloud bursting for load balancing between clouds)
4. **Community cloud:** The infrastructure of the community cloud is provisioned for private use by a specific community of consumers from organizations that have shared concerns (e.g. mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises

What is cloud security?

Cloud security can be defined as the protection of cloud based systems, applications, data and infrastructure through procedures, technologies, controls and policies designed to adhere to regulatory compliance rules.

The main differences between public cloud security and traditional IT security is shown in the following table:

Public Cloud Security	Traditional IT Security
Low upfront infrastructure investments	High upfront costs
Quickly scalable	Slow scaling
Efficient resource utilization	Lower efficiency
Reduced time to market	Longer time to market
Usage based cost	Higher cost
Third party data centers	In-house data centers

Why cloud security?

The revolutionary development of cloud computing is significantly changing the current way of how network services work.

Organizations have begun shifting their spending from traditional systems to cloud services that open doors to great opportunities along with a number of risks. Reinforcing this view, Gartner says that by 2022 the development in IT spending for cloud-based offerings will be more rapid than development in traditional non-cloud IT offerings, making cloud computing a standout amongst the most disruptive powers in the IT markets since the beginning of the digital age. Gartner also forecasts, "Through 2022, at least 95% of cloud security failures will be the customer's fault", thus the mitigation of the associated risks needs to be enforced.

Call: +44 345 222 1711 /+353 1 210 1711 Email: cyber@bsigroup.com Visit: bsigroup.com

Cloud security risks

The most common security risks of cloud-based services include, but are not limited to, the following:

Sensitive data

- **Data breaches:** A data breach is an event in which confidential, protected or sensitive information is viewed, released, stolen or used by an individual or an entity/group who is not authorized to do so
- **Weak identity, credential and access management:** Data breaches and enabling of attacks can occur because of a lack of scalable identity access management systems, failure to use multifactor authentication, weak password use, and a lack of ongoing automated rotation of cryptographic keys, passwords and certificates
- **Data loss:** Data stored in the cloud can be lost for several reasons other than malicious attacks. An incidental deletion by the CSP, or worse, a physical calamity such as an earthquake or fire, can lead to the permanent loss of consumer data unless the provider or cloud consumer takes sufficient measures to back up data, following best practices in business continuity and disaster recovery as well as daily data backup and possibly off-site storage

Governance

- **Loss of governance:** When decision makers create business strategies, cloud technologies and CSPs must be considered. Developing a good roadmap and checklist for due diligence when evaluating technologies and CSPs is essential to ensure success. An organization that rushes to adopt cloud technologies and choose CSPs without performing due diligence exposes itself to a myriad of commercial, financial, technical, legal and compliance risks that jeopardize its success
- **Insufficient due diligence:** Cloud technologies and CSPs must be considered by the executives of the organization while creating business strategies. To be successful, organizations must develop a good roadmap and checklist for due diligence when evaluating CSPs and technologies
- **Vendor lock-in:** A condition in which a consumer using a cloud service or product cannot transition to a cloud service product or service of a competitor. It is generally the consequence of proprietary technologies that are incompatible with those of competitors. It is recommended to check whether your CSPs have proper interoperability and portability features or solutions and negotiate the entry and exit strategy upfront with your vendor

Technology Vulnerabilities

- **Shared technology vulnerabilities:** CSPs use scalable infrastructure to support multiple tenants which share the underlying infrastructure. All layers of shared technology can be attacked to gain unlawful access to data, like CPU, RAM, hypervisors, applications, etc.
- **System vulnerabilities:** System vulnerabilities are exploitable bugs in programs that attackers can use to penetrate a computer system for the purpose of stealing data, taking control of the system or disrupting service operations

Accidental and malicious attacks

- **Denial-of-service (DoS):** DoS attacks are attacks meant to prevent users of a cloud service from being able to access their applications or their data
- **Insecure interfaces and APIs:** CSPs expose a set of software User Interfaces (UIs) or Application Programming Interfaces (APIs) that consumers use to manage and interact with cloud services. Provisioning, management, orchestration and monitoring are all performed with these interfaces. The security and availability of general cloud services are dependent on the security of these basic APIs. From authentication and access control to encryption and activity monitoring, these interfaces must be designed to protect against both accidental and malicious attempts to circumvent policy
- **Malicious insiders:** The European Organization for Nuclear Research (CERN), defines an insider threat as follows: "A malicious insider threat to an organization is a current or former employee, contractor, or other business partner who has or had authorized access to an organization's network, system, or data and intentionally exceeded or misused that access in a manner that negatively affected the confidentiality, integrity, or availability of the organization's information or information systems"
- **Account hijacking:** The hijacking of cloud accounts is a technique in which an individual or organization's cloud account is stolen or hijacked by an attacker
- **Advanced Persistent Threats (APTs):** APTs are an ingratiating form of cyber- attack that penetrates systems to establish a perch in cloud infrastructure of target companies from which they export data and intellectual property
- **Abuse and nefarious use of cloud services:** Badly secured cloud service deployments, fraudulent account sign-ups and free cloud service trials can expose cloud computing model such as IaaS, PaaS, and SaaS to malicious attacks. The malicious actors may leverage cloud computing resources to target organizations, users or cloud providers

Cloud security solutions

The most common cloud security solutions for a secure cloud environment before and after adopting a cloud first strategy are discussed below:

Due diligence and business continuity

- **Organizations need to perform deep dive due diligence** when choosing CSPs – review Service Level Agreements (SLA's), vendor lock-in, interoperability and portability, discuss and agree on entry and exit capabilities
- **Develop a disaster recovery and business continuity plan** The planning of business continuity and disaster recovery are critical aspects of businesses but are often ignored. Businesses or organizations must make a well-structured plan and document for disaster recovery and business continuity

Identity and access data

- **Encryption of sensitive data -** Make sure your cloud providers have capabilities to perform the encryption of sensitive data in transit, or data in motion and data at rest. Use SSL transmission (TLS 1.2/1.3) to ensure the highest level of security for data in transit and encrypt cloud storage – data at rest using Advanced Encryption Standard (AES-256), and encryption keys should also be encrypted with a regularly rotated set of master keys
- **Setup an identity and access management solution** - This solution can be used to capture, manage, initiate, record user identities and access permissions. All users are authorized, evaluated and authenticated according to roles and policies
- **Apply the Principle Of Least Privilege (POLP)** - NIST Special Publication 800-160 states that each component should be allocated sufficient privileges to accomplish its specified functions, but no more
- **Use intrusion detection and prevention technology** - This technology has helped businesses to identify when an attack has occurred and prevent to stop attacks in progress
- **Educate your employees** - Train your staff by setting up a dedicated portal with videos explaining phishing activities (do not click unknown links), creating and maintaining a strong password, not sharing or saving passwords on paper or public places, use a strong password manager, should not use unknown USB drives on work laptops

Security and data management

- **Establish and enforce cloud security policies** - Business organizations should have their own guidelines to determine who can use cloud services, which data can be stored in cloud and how can they use them
- **Make sure you are compliant with all the legal, regulatory and other requirements** such as GDPR, NIS Directive, ENISA and Health Insurance Portability and Accountability Act (HIPPA)
- **Use a third party partner like Cloud Access Security Brokers (CASBs)** – Gartner says, a CASB is an on-premise or cloud-based security policy enforcement point that is placed between cloud service consumers and CSP to combine and interject enterprise security policies as cloud-based resources are accessed
- **Invest in or utilize log management and continuous monitoring** features from your CSP. Monitoring and log management is a vital element of cloud security and management
- **Set up alerts and reporting on your cloud environments** – Alerting is an important feature found in a cloud environment or as a service provided by the CSPs. It helps you to know about any unusual activities happening in your cloud environments. The reporting feature of the cloud can be critical to the success of your business. The reports can help businesses make better decisions
- **Conduct periodic audits and penetration testing** - We suggest performing penetration testing to determine whether your cloud security architecture design is sufficient to protect your applications and data. Periodic audits of your cloud providers should be conducted. It should include scrutiny of your cloud vendor capabilities. They need to meet the requirements of the SLA
- **Understand your cloud security shared responsibility** model as described in the next section

Call: +44 345 222 1711 /+353 1 210 1711 Email: cyber@bsigroup.com Visit: bsigroup.com

Who owns cloud security?

Cloud responsibility is detailed in the shared responsibility model. The level of responsibility for each party in the cloud will be determined by the services that the customer chooses from their service provider with responsibility rising for the customer the lower down model they are moving from SaaS to IaaS.

Gartner defines Cloud Services Brokerage (CSB) as an IT role and business model in which a company or other entity adds value to one or more (public or private) cloud services on behalf of one or more consumers of that service via three primary roles including aggregation, integration and customization brokerage.

The following figure describes the shared responsibility model across different cloud service models:

Shared Responsibility Model for Security in the cloud			
On-Premises (for reference)	**IaaS** (Infrastructure-as-a-service)	**PaaS** (Platform-as-a-sevice)	**Saas** (Software-as-a-sevice)
User Access	User Access	User Access	User Access
Data	Data	Data	Data
Applications	Applications	Applications	Applications
Operating System	Operating System	Operating System	Operating System
Network Traffic	Network Traffic	Network Traffic	Network Traffic
Hypervisor	Hypervisor	Hypervisor	Hypervisor
Infrastructure	Infrastructure	Infrastructure	Infrastructure
Physical	Physical	Physical	Physical

Customer responsibility

Cloud service provider responsibility

The Cloud Security Alliance provides two recommendations on the shared responsibility model,

1. **Cloud providers** should clearly document their internal security controls and customer security features so the cloud user can make an informed decision. They should adopt a Security by Design approach and implement those security controls
2. **Cloud users** should, for any given cloud project, build a responsibilities matrix to document who is implementing which controls and how. This should also align with any necessary compliance standards

Cloud security standards

Best practices and solutions

Gartner says Security Control Frameworks are outlines of best practices — the set of processes and controls that would typically be applied to securely provision and run a digital service under defined circumstances. The risk assessments of the CSP can be assessed by the following most important control frameworks and best practices documents:

Security techniques

- **ISO/IEC 27001:2013: Information technology – Security techniques – Information security management systems – Requirements:** It is the most commonly used control framework globally, not intended specifically for cloud assessment, but it is commonly and successfully used in conjunction with the more detailed control framework, ISO 27002 in the cloud service context. It specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organization. It also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organization
- **ISO/IEC 27002:2013 Information technology – Security techniques – Code of practice for information security controls:** It gives guidelines for organizational information security standards and information security management practices including the selection, implementation and management of controls taking into consideration the organization's information security risk environment(s)
- **ISO/IEC 27017:2015: Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud services:** This control framework was published in 2015, supplements 27002 with additional security controls and practices for the security of public cloud services
- **ISO/IEC 27018:2019: Information technology – Security techniques – Code of practice for protection of Personally Identifiable Information (PII) in public clouds acting as PII processors:** This control framework was published in 2019, supplements 27002 by identifying appropriate controls for the protection of PII in a public cloud service

Cloud Security Alliance (CSA) and Governance, Risk and Compliance (GRC) stack

This is a set of disciplines ensuring than an organization acts ethically correct and in accordance with its risk appetite, internal policies and external regulations can also be useful in CSP's security evaluation

- **CSA Security Trust, Assurance and Risk (STAR™)** is the industry's most influential programme for security assurance in the cloud. STAR™ delineates key principles of transparency, rigorous auditing, and harmonization of standards. The STAR™program provides multiple benefits, including indications of best practices and validation of the security posture of cloud offerings. It comprises of the following tools:
  - A standard template for cloud providers to document their security and compliance controls called **Consensus Assessment Initiative Questionnaire (CAIQ)**
  - The other tool is called the **Cloud Control Matrix** (CCM), which lists cloud security controls and maps them to multiple security and compliance standards. The CCM can also be used to document security responsibilities. These documents will need tuning for specific organizational and project requirements, but it can act as a comprehensive starting template and can be especially useful for ensuring compliance requirements are met
  - The **CSA Code of Conduct for GDPR Compliance** is a tool developed in association with industry specialists and representatives from EU national data protection authorities to help organizations in complying to the European GDPR. The CSA's code contains all the essential requirements a CSP has to satisfy in order to comply with the EU GDPR

Call: +44 345 222 1711 /+353 1 210 1711 Email: cyber@bsigroup.com Visit: bsigroup.com

Other guidelines and recommendations

- **NIST Special Pub 800-144 guidelines on security and privacy in public cloud computing:** This U.S. federal government publication provides an outline of the security and privacy challenges relevant to public cloud computing
- **European Banking Authority's (EBA's) recommendations on outsourcing to CSPs:** These recommendations intend to clarify the EU-wide supervisory expectations if institutions intend to adopt cloud computing, so as to allow them to leverage the benefits of using cloud services while ensuring that any related risks are adequately identified and managed
- **European data protection supervisor – Guidelines on the use of cloud computing services:** The Guidelines provide recommendations and indicate best practices to implement accountability for personal data protection by helping to assess and manage the risks for data protection, privacy and other fundamental rights of individuals whose personal data are processed by cloud-based services
- **European Network and Information Security (ENISA's) Cloud Computing Security Risk Assessment:** This publication provides an overview, benefits, risks and recommendations of the Information or cloud security risks when adopting a cloud first strategy.
- **Financial Conduct Authority (FCA's) FG 16/5 Guidance for firms outsourcing to the 'cloud' and other third-party IT services:** The publication clarifies the requirements on firms when outsourcing to the 'cloud' and other third-party IT services
- **The U.S. Federal Risk and Authorization Management Program (FedRAMP):** The FedRAMP provides a standard methodology to security assessment, authorization, and continuous monitoring of cloud products and services. All federal organizations that use or plan to use cloud services are required to implement the FedRAMP program

Cloud computing and GDPR

The EU General Data Protection Regulation (GDPR), one of the most rigid data privacy laws came into effect on May 25, 2018. It applies to any organization who collects, stores or processes personal information of EU citizens or EU residents in any part of the world.

The basic rights given to data subjects under the GDPR are the right to access, the right to be forgotten, the right to data portability, the right to be informed, the right to have information corrected (the right to rectification), the right to restrict processing, the right to object and the right to be notified.

If a data breach occurs, the regulators and users must be notified within 72 hours without delay. If an organization violates the regulation, they can be penalized a maximum of 4 percent of their annual turnover or €20 million, whichever is a greater amount.

Impacts of the GDPR on cloud computing

How to manage compliance?

Under the GDPR regulation the data should not be stored longer in the cloud or on premise than needed for its prescribed purpose. This duration depends on the type of the data and region where it resides.

The deletion of data

Once the duration is passed, data must be permanently deleted from the cloud. The deletion of data will impose a challenge as it may be stored in various locations and jurisdictions which requires identification and management of multi-jurisdictional retention requirements.

The primary method of deleting data in the cloud is crypto-shredding whereby the data is encrypted and the primary keys are destroyed. Backup deletion of data will also be a challenge. Accordingly, it is essential for every organization to understand how backups are secured and retention is handled by your CSPs.

Breach notification

- The responsibilities of the breach notification and protocols must be clearly included in the SLAs with your CSPs. It should clearly define that if any breach occurs, you should be informed in a definite amount of time complaint with GDPR (72 hours) or even quicker depending on your contract with your service provider
- The ownership of data must be clearly stated in the contract. If your data is stored in another country, you must make sure that you have the ownership right of data and consider the local legislation as it pertains to that jurisdiction
- One of the most important challenges is risk management. Data Protection Impact Assessments (DPIAs) and security assessments can be performed on CSPs. The right to audit CSPs must be included in your agreements
- Follow the **Cloud Security Alliance – Code of Conduct for GDPR Compliance** which includes all the essential requirements a CSP must satisfy in order to comply with the EU GDPR

These are the common impacts and tips to achieve compliance. There might be other impacts that organizations might face depending on their businesses, and they should always have a plan or solution to remain compliant with the GDPR. The information provided above is for informational purposes only and not for the purpose of providing legal advice. You should seek advice and guidance from your own legal counsel with respect to any interpretation of the GDPR or a specific law.

Conclusion

Gartner suggests "Different cloud models have different risks and control amplifications. Make sure your strategy reflects this reality". A high-impact transformation to the cloud comes with the need to ensure that organizations are ready to support it.

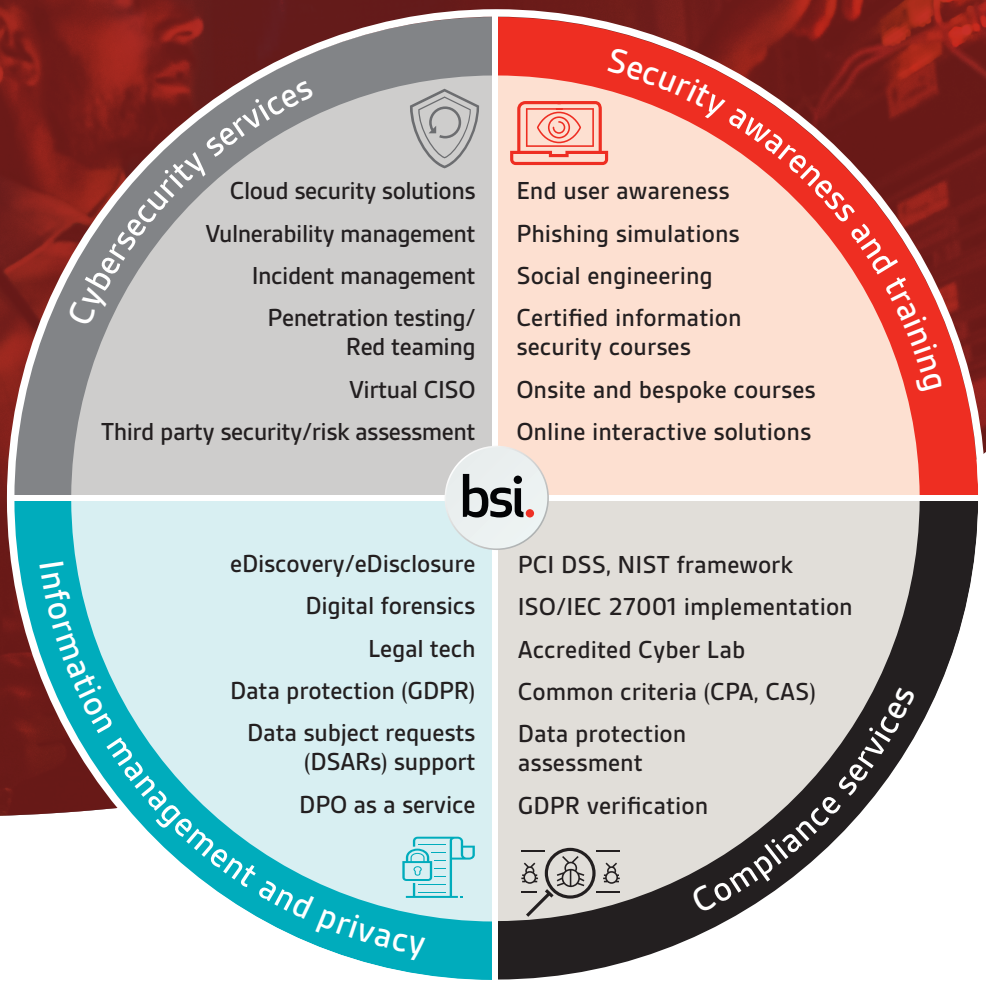
All the users whether an individual or organization should be aware of the security concerns existing in the cloud. It's important to understand these security concerns and effectively implement cloud security solutions.

Securing your cloud computing posture can be achieved through a layered approach combining "secure by design" principles, referencing cloud security standards, employing cloud technology solutions, adhering to best practices, utilizing cloud security professionals and staff with the skills required to achieve your organizational strategy.

BSI Cybersecurity and Information Resilience

Protecting your information, people and reputation

BSI Cybersecurity and Information Resilience helps you address your information challenges. We enable organizations to secure information, data and critical infrastructure from the changing threats that affect your people, processes and systems; strengthening your information governance and assuring resilience. Our cyber, information security and data management professionals are experts in:



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

bsi.

UK

Call: +44 345 222 1711
Email: cyber@bsigroup.com
Visit: bsigroup.com

IE/International

+353 1 210 1711
cyber.ie@bsigroup.com
bsigroup.com