Emerging Trends in the Information Security Landscape 2020

A whitepaper

bsi.

...making excellence a habit.™

Contents

Executive Summary

BSI's global centre of excellence for Cybersecurity and Information Resilience has forecast a range of emerging trends across the cybersecurity landscape for 2020.

This whitepaper highlights the next developments in cyber threats, cyber-related regulations, technological evolution and specific solutions.

Among the cyber threats, we analyze:

- Advanced techniques for verifying cyber defence capabilities

- Managing data breaches and third-party risk

- Ongoing compliance and regulations

- Cloud security risk

What becomes clear from the review is that industry regulations which include cyber elements and cyber-attacks continue to prevail in volume and sophistication. This means that security organizations are adapting to come up with new ways to manage these increased workloads. The term "shift-left" appears more often as cyber/regulatory efforts are addressed earlier on, as increasingly, organizations move to the cloud and reduce the burden on IT and security maintenance overheads.

Mature organizations are developing tailored and consolidated control frameworks to manage cyber, regulatory and legal needs through a single management system. This single view offers one set of controls against which privacy, cybersecurity, information security and supply chain can all be managed and monitored using formal KPIs and as regulations continue to mature and overlapping requirements become common, organizations would do well to understand where efficiencies can be leveraged to meet obligations, stay secure and increase the efficiency of security team workloads.

Attack defence preparation remains high on the agenda for 2020, with organizations who may have only considered table top cyber simulations up to now, opting for a deeper level of assurance through purple team attack simulation. These hands-on simulations derive some of the most tangible benefits in truly understanding the incident response capabilities across their people skills, process adequacy and system tuning.

Advanced hacking techniques

Purple is the new red

Author: Nick Hayes, Global Head of Technical Direction

Penetration testing is an activity which has been the foundation of offensive testing in the security industry for many decades and indeed continues to be an important part of many organizations security programs.

Although the concept has been around for quite some time, attack simulation testing has been gaining in popularity over the past few years, particularly the Red Team testing element of it. This was no-doubt aided by various schemes being introduced to the market which supported and mandated this type of work, such as the CREST STAR accreditation, the CBEST scheme from the Bank of England and others outside the UK such as TIBER-EU and iCAST. There was also the introduction of the GBEST scheme for government departments. Ultimately, what these schemes and accreditations achieved was to formalise the market requirement and mandated that organizations in certain industries had a duty to carry out such engagements.

During 2019 however, the industry did see a slight shift towards a preference to performing Purple Team engagements alongside, or in place of, the Red Team engagements. A Purple Team assessment simply means that the Red (offensive) and Blue (defensive) teams are working in unison to achieve mutually agreeable objectives, namely that of improving the organizations' response and detection capabilities. Purple Teaming as a concept and an approach can be a particularly powerful one, often with training of the Blue Team being a key objective, which in turn drives improvement throughout an organization and tightens its defences. Additionally, a Purple Team engagement does not necessarily need a high level of organizational maturity to be able to see actionable results due to the direct and collaborative approach which is not always the case with a Red Team. Purple Teaming is often seen as a sensible, pragmatic approach to proactive security and, along with Red Teaming, is the only testing type which truly gives a picture of the level of preparedness of an organization to resist a cyber-attack.

As more industries and sectors realise the benefits of performing attack simulation tests, BSI believe that the popularity of Purple Team testing will continue to rise as it did during 2019.

Advanced penetration testing

Author: Nick Hayes, Global Head of Technical Direction

As mentioned earlier in this whitepaper, penetration testing has been a cornerstone of many security programs over several decades. However, in the recent past there has been a shift in approach and requirements, driven by the buying market and the security challenges organizations are facing currently. As a result, the security industry has needed to evolve its approach and the way it provides assurances to organizations through security testing.

One of those key challenges is that of software development and the rising popularity of CI/CD (Continuous Integration/ Continuous Deployment) pipelines and alternative development methods such as Agile, Lean, Scrum and DevOps. Traditionally, penetration testing would have been performed as a point-in-time exercise at the end of a project lifecycle, however that was generally being performed at a stage in the project where remediating the errors was difficult and expensive.

Organizations are therefore beginning to consider security much earlier in the lifecycle, often referred to as a "shift-left" culture. Simply put, "shifting-left" moves the security implementation to earlier stages of the lifecycle, thus enabling security-by-design and allowing for substantial cost and time savings over a project lifecycle.

For a client "shifting-left" ,a penetration test that only happens at the end of the lifecycle which would be out of sync with their existing security commitments. As a result, there has been a trend towards more continuous and integrated penetration testing. A continuous penetration test can mean a few things, such as external vulnerability scans (running 24/7),

testing of new code as it is deployed in an agile development environment, through to the introduction of additional automation of security efforts at various parts of the pipeline, such as integrating into DAST (Dynamic Application Security Testing), SAST (Static Application Security Testing) and IAST (Interactive Application Security Testing) techniques. Testing in this way does represent some significant changes in approach for the security industry, however, implemented well it can often provide organizations with a boost to the value they derive from testing.

Whilst the trend towards continuous and integrated testing activities continue, there is an additional requirement on the industry to rethink how reports are delivered. Testing in a development pipeline is fine, however, it would be counterproductive to then wait 5-10 days for a PDF report, which can be difficult to ingest into existing workflows and tooling. At BSI we are evolving too, and introducing a new client portal solution for our testing clients in 2020 which will allow for quicker and more seamless interaction with CI/CD pipelines and agile development teams, amongst other features such as allowing for quick estimations and booking of testing activities.

Advanced hacking techniques

Multi-factor attacks

Author: Conor Gavin, Technical Team Lead – eDiscovery and Digital Forensics

A positive development throughout 2019 has been the roll out of Multi-Factor Authentication (MFA). Reports from LastPass suggest that 57% of business globally are using MFA, an increase of 12% from 2018. Microsoft also estimates that 99.9% of attacks on your account can be prevented with MFA. However, as the number of organizations protected by MFA continues to rise, attackers will increasingly attempt to bypass MFA.

BSI's Incident Response and Forensics consultants have seen successful attacks using what we've termed a "9am Attack". In this attack, an end user has been successfully phished and their password compromised, but the account is protected by MFA. Through simple research it is usually possible to find out what country, and therefore time-zone, the compromised end user is based in. Armed with these details, the attacker attempts the following:

1. The attacker attempts a login at around 9am of the local time of the user

2. The end user, just arrived in the office and now logging in, gets a prompt on their authenticator app to approve

3. If the attacker has timed it correctly, the user associates their login with the prompt and approves it, granting the attacker access

As well as timing attacks, other possible attacks include sophisticated phishing tools like Evilginx which utilise genuine sign-in pages to perform man-in-the-middle attacks to capture authentication tokens sent as cookies after MFA has been completed by the user. If successful, the attacker can copy this captured cookie to their own machine and enjoy full access to the compromised user's account. SIM Swapping attacks are also popular for high value targets using SMS-based authentication. This involves the attacker socially engineering the mobile phone carrier. The attacker gathers enough personal information about the target, to convince the carrier that they are the legitimate owner of the account, and subsequently requests a replacement SIM. Once received, the attacker can then use the SIM to receive MFA authentication codes

MFA will continue to be an essential defence against attackers but as its adoption increases attacks against it will invariably increase too. 2020 might well be the year MFA attacks go mainstream.

IoT and Embedded Systems: the risks keep growing

Author: Adam Caudill, Director – Application Security Testing

As more devices are connected to the internet, from refrigerators to coffee makers the risk these devices present to their environment is going to continue to grow. While hacking a "smart" appliance may seem like a trivial risk, it's the access they can provide to other devices on the same network that presents the greatest threat.

By targeting IoT devices, attackers can gain a foothold in a network, allowing them to use the device as an entry point to attack systems that are far more critical. When targeting a network, attackers will seek out the weakest link first, and IoT devices are far too often not living up to the same security standards of the other systems that they share a network with. By installing devices that may have entirely unknown security properties on a network, it's easy to create new weak points on a network, just the thing attackers look for.

Keeping these devices isolated from important systems by properly segregating the network and ensuring that the devices have been tested by a reputable penetration testing firm are key steps to protecting the environment in which they will live.

Blockchain and immutable ledgers: moving beyond hype

Author: Adam Caudill, Director – Application Security Testing

There's no question that there has been a huge amount of hype around blockchains and other forms of immutable ledgers in recent years.

While there is still a great deal of hype, these technologies are more and more being used in business-critical systems, making it vital to ensure that they are secure. While systems built around blockchains have some unique weaknesses that do not apply to most applications, in reality most issues that are found in these systems are common application security failures that could be prevented by following well established best practices; failing to learn from the past, failing to learn from the well documented and well understood best practices that have been established is a recipe for disaster – and there have certainly been some spectacular failures.

Immutable ledgers – the vital core of blockchains – provide substantial value to businesses, helping to address a variety of challenges, such as tracking a chain of custody, verifying that records haven't been altered after the fact, documenting critical details as components pass through the supply chain, and many others. A ledger that is append-only, immutable, and backed by strong cryptographic guarantees can be leveraged in numerous ways to provide assurances that are difficult otherwise.

As more business look to leverage the benefits of immutable ledgers in their business processes, using their ability to provide cryptographic assurances to allow their customers and business partners to authenticate data, there will also be increased interest in subverting these systems to allow attackers to manipulate data for their own purposes. Whether it be maliciously altering existing records, inserting new records, or attempting to deny access to the system altogether, there will be substantial focus on these systems and the monetary impact could be very significant.

Advanced hacking techniques

Rise of the machines: machine learning and artificial intelligence

Author: Adam Caudill, Director – Application Security Testing

As machine learning is being deployed in an ever-expanding number of roles, attacks against these systems (which may have a life or death impact) are also improving at a rapid pace. Machine learning is being applied to a truly massive number of problems; from self-driving cars, detecting medical issues such as cancer, advising doctors and insurance companies of the best medical care plans, predicting supply chain issues, to optimizing investments and portfolio management. Machine learning is becoming a defining technology in solving some of the most pressing challenges that business face. It also creates some unique security challenges.

There has been a great deal of academic research into how to attack and otherwise trick systems that rely on machine learning, from fooling facial recognition systems to making self-driving cars think that a stop sign is instead a speed limit sign. As this research begins to move out of academia and into the real world, the results will likely be substantial and hard to predict.

Due to the nature of machine learning systems, in that they are often not fully understood even by their developers, the results of an attack can be hard to detect, and unlike other cybersecurity issues, may be very subtle. Attacks against the data used to train a machine learning algorithm, be it a labeled dataset, or the data ultimately fed into a reinforcement learning system, can result in the most subtle results – changing the outcome of the algorithm in ways that could easily go undetected for years.

Machine learning, for all the good it can do, also opens up entirely new classes of security issues (without closing any of those faced by other software), and as a result presents a greater challenge to secure. We expect to see some particularly interesting attacks in 2020 and beyond, which could lead to rather expected results for those using systems that are reliant on machine learning.

This is an area that we see as being at the earliest stages of attack development and expect implementation of proper defenses to become extremely important.

Third party risk

Supplier risk management

Author: Herman Errico, Security Consultant – Cyber, Risk and Advisory

Supplier risk management is a practice that allows organizations to identify, assess, manage and treat supplier risk. This practice applies to information security risks that relates to both supplier for services and for products. From a process perspective, organizations are following ISO 27002 and 27036 to perform supplier risk management operations.

In 2019, supplier risk has registered a substantial increase in terms of visibility and regulatory recognition. On one hand, legislative requirements such as the General Data Protection Regulation (GDPR) and the Network and Information Security (NIS) directive have identified a requirement to manage supplier risk effectively. On the other hand, some of the major recent data breaches (e.g. Airbus [2019]; Marriot International [2018]) were due to the lack of security controls within a supplier's environment and this has increased overall visibility.

Companies are starting to improve their ability to manage those risks by adopting third party services for outsourced monitoring (e.g. Security rating – BitSight) or by implementing cloud-based management systems for supplier risk management. Therefore, in 2020, risk related to supplier relationships will continue to be considered an emerging trend. However, we do see some differentiators for 2020 compared to 2019. Companies will require the ability to further customize their solutions to better identify security controls baselines that are necessary to reduce suppliers' risks. This approach will contribute to the effective reduction of risks to offsite processing of information, outsourced system development, integrations, configurations or hardware product provenance to name a few.

By having a dedicated security baseline to manage supplier risk, companies will be better positioned to achieve their compliance requirements and their business' objectives.

Ongoing compliance and regulations

Ongoing GDPR privacy assurance

Author: Conor Hogan, Senior Manager – Cyber, Risk and Advisory

Ever-new and maturing privacy regulations mean that organizations need to evolve their approach to privacy compliance. Adopting a rights-focused privacy programme will enable organizations to embrace compliance as an enabling "BAU" process.

Globalization and the relentless advance in technology means that privacy safeguards are necessary to ensure the fundamental rights of citizens are protected. Legislatures all around the world are alert to the increasing imbalance of power between citizens and corporations and governments. The rise of big data and artificial intelligence continues to threaten privacy. Strong, robust, and rights-based protections are needed to insulate from unnecessary intrusions, for example tracking a person's location and every movement via fitness trackers or "smart" watches.

EU regulators continue to grapple with the weight of public and industry expectations of GDPR enforcement. But organizations routinely struggle to meet the accountability requirements of the GDPR. Individuals are more aware than ever of their rights, but also heavily fatigued by privacy related scandals.

Privacy is in vogue, limited credit due in part to the GDPR, but we continue to see a steady increase in evolving or new legislation like the GDPR. Japan's Act on Protection of Personal Information (APPI) and Brazil's Lei Geral de Proteção de Dados (LGPD) are closely aligned with the GPDR. US developments like California's Consumer Protection Act (CCPA), and a proposed federal privacy bill ("Consumer Online Privacy Rights Act") mean that the corporate challenge of privacy compliance will not simply disappear. Organizations must consider their global

requirements with a properly resourced and scoped privacy program to help plan, manage and demonstrate compliance.

Adopting a principles-based privacy program to establish a rights-centred approach to controls is a pathway forward. Documentation is critical to evidence compliance – whether in response to a regulatory demand or to satisfy a customer or certification audit. Embedding a culture of privacy takes time and investment - especially when compliance is traditionally viewed as a barrier to innovation. Privacy must be considered at the earliest possible stages of projects to help organizations improve data protection maturity. The simple idea of "shifting privacy compliance left" means that that a culture of privacy-by-design can be nurtured, and the challenges of ongoing privacy assurance can be more easily met.

Organizations traditionally engage third party auditors or an internal function to provide varying degrees of assurance over internal controls. Indeed, assurance frameworks are a dime-a-dozen (e.g. ISO27001, ISO27701, SOC2; PCI DSS; BS10012; HIPAA; FISMA, etc.). But demonstrating privacy compliance is not an easy task and cannot be considered a point in time requirement. Ongoing assurance over the privacy programme will help improve privacy maturity, enable innovation, build trust with customers and investors, and help meet mounting regulatory expectations with a robust and defensible position.

Weaponized DSARs and the automation to come

Author: Ciaran Mahon, Consultant – eDiscovery & Digital Forensics

Increasing use of Data Subject Access Requests (DSARs) by individuals, activists and cybercriminals will accelerate the move towards improvements in standardized processes and automation for handling DSARs.

The General Data Protection Regulation (GDPR) and other global privacy regulations have put organizations on a positive path to privacy management. It has encouraged more responsible data handling, greater transparency of how personal information is processed, controlled and governed.

However, complying with Data Subject Access Requests (DSARs) continues to be a challenging area for most organizations. Many departments from Human Resources to Legal to Compliance are continuing to feel the impact as consumers become more aware of their right to obtain a copy of their personal data in the form of a DSAR.

In 2020, new privacy laws will come into force around the world such as the CCPA in California, the LGPD in Brazil and PDPA in Thailand. With similar bills pending in New York (New York Privacy Act s.5642), Pennsylvania (House Bill 1049) Massachusetts (Consumer Privacy Bill SD 341) among others, the coming year is going to be another busy year from a DSAR standpoint, organizations are likely to see the continued use of DSARs by:

• **Individuals** curious to see what personal information a company may be processing on them

• **Activists** attempting to cause disruption to an organization

• **Cyber-criminals** looking to steal personal information

In 2019, the Blizzard Entertainment protest demonstrated how Article 15 of the GDPR can be used by activists to flood a company with simultaneous DSARs. As these requests can place a significant administrative burden on organizations, we may see more of these protests in future.

There is also the potential for DSARs to be used by cybercriminals as a mechanism to steal personal information. A University of Oxford-based researcher demonstrated in his 'GDPArrrrr: Using Privacy Laws to Steal Identities' paper, how organizations lacking a clear and robust method for verifying Data Subjects can be manipulated into sending personal information to the wrong individual.

Given these challenges and the increasingly changing regulatory landscape, in 2020 organizations are likely to adopt more robust mechanisms for verifying Data Subjects, make smarter use of data retention strategies, and make further moves towards automation to reduce the resource intensive burden that falls on organizations.

Ongoing compliance and regulations

PCI (Payment Card Industry) trends

Author: Leo Boike, Senior Consultant – Cyber, Risk and Advisory

With much anticipated excitement, v4.0 of the Payment Card Industry Data Security Standards (PCI DSS) is tentatively scheduled for late 2020.

Goals for v4.0 include:

1. Meet the security needs of the payments industry
2. Add flexibility and support of additional methodologies to achieve security
3. Promote security as a continuous process
4. Enhance validation methods and procedures

The twelve core requirements of PCI DSS will not change but will introduce a new validation methodology. Instead of the traditional method, organizations may opt to show that their controls meet the intent of PCI DSS and address risk. Having a flexible method of validation will allow organizations to better align their compliance efforts with risk and to allow for alternative solutions in order to meet the intent of PCI DSS. For organizations wishing to avail of this more flexible option, it is likely that significantly more time will have to be added on to their audit in order for justification to be verified.

Businesses continue to move their networks to cloud solutions for ease of configuration and network management. Also, for security, flexibility, and rapid deployment of changes needed in today's competitive business world.

Solutions that remove the storage, processing, and transmitting of cardholder data from the network and business environment reduce not only the risks to the organization but also reduce the reporting efforts needed to validate compliance to PCI DSS. These solutions include, but are not limited to payment channels for:

- Mail order/telephone order (MOTO) – including PBX, call recordings, and call centers
- E-commerce
- Card present (face-to-face)

The trend for PCI compliance is to implement solutions that not only decrease risk, but also the efforts needed to meet and validate the PCI DSS compliance, allowing businesses to improve their processes. The business goals are to maintain a culture of change and agility, without being overly incumbered by resource intensive and financially impactful compliance requirements.

As businesses move forward, they must maintain engagements with the PCI DSS advisors in order to stay abreast of changes coming in v4.0, ensuring that they are de-risking their card processing environment and where card data must be stored and processed, are maintaining PCI DSS in an effective and efficient manner.

Cloud security risk management

Zero trust networks in an O365 world

Author: Vincenzo Rea, Senior Consultant – Cyber, Risk and Advisory

How do you define your company's network boundaries when using cloud services? How do you feel when username and password are the only obstacles between a web page and your data? The Zero Trust Networks model utilises new security measures for protecting organisations and their perimeter when it is truly distributed.

If you are wondering how a single data breach can extract data in a single cyber-attack, the answer is probably through the castle-and-moat model weaknesses.

While many people may not be familiar with this terminology, the castle-and-moat model is widely used every day by many companies around the world.

In a castle-and-moat model, everyone inside the network has access to certain resources and more importantly, everyone's identity is trusted by all the others inside that network. The flaw with this model is that once attackers gain access to the network, they are trusted and considered as legitimate users.

In 2010, the researcher John Kindervag formalized the concept of a Zero Trust Network model, based on the principle that no one is trusted by default from inside or outside the network, and identity validation is required from everyone before access is granted to any resource.

There is no single technology associated with this security concept; it is rather a different approach to network security that embeds several different principles and technologies.

One clear example of Zero Trust Network model can be seen when using Office365.

To most of us, it would appear that the correct username and password take us directly to our mailbox or to the spreadsheet we were working on earlier in the day. Behind the scenes, multiple controls have been validated prior to
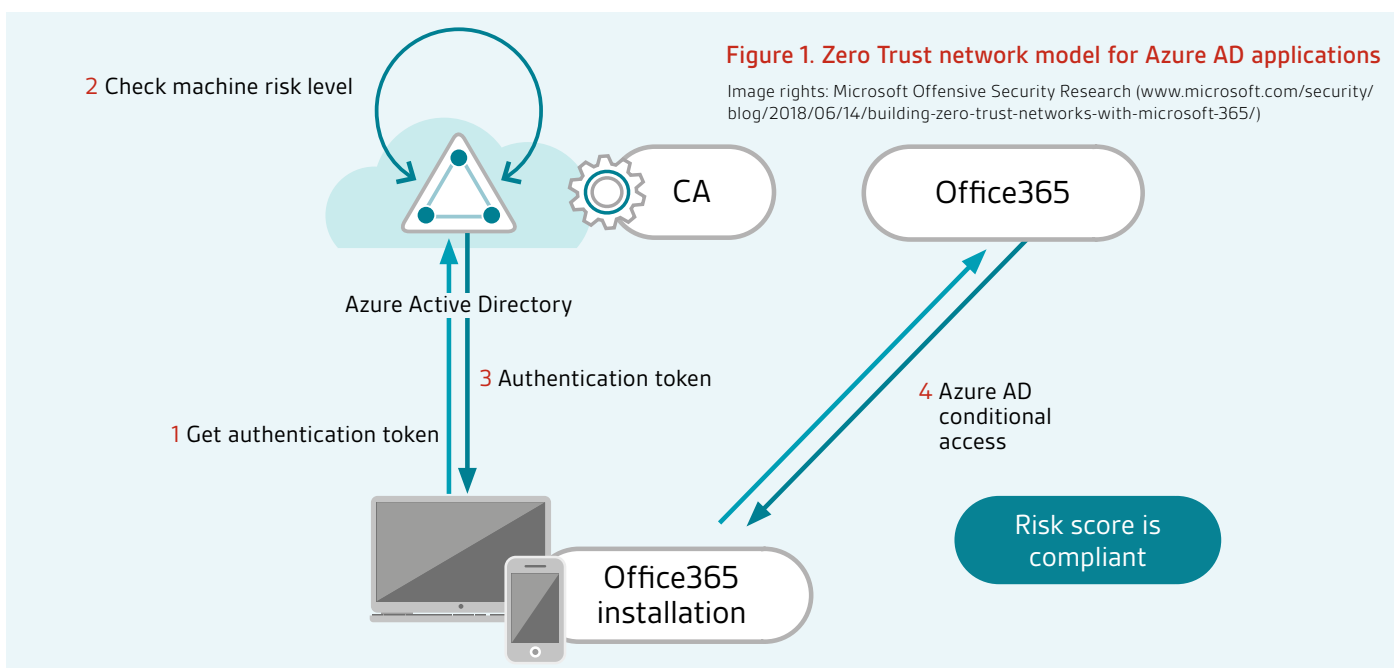
granting access to ensure our identity is legitimate and has the necessary rights to proceed. Along with the credentials, additional controls include the network and the device where the request originated, geolocation, previously initiated sessions including those with different applications within the organisation, proxy services, multi-factor authentication, access control lists, encryption and scoring mechanisms.

While the Office365 user may not realize it, he or she is already part of the Zero Trust Network security model.

Security doesn't stop there though, and users still have to play their part. As emphasized by the NCSC UK in a recently published article, cloud services, including Office365, are now at the top of the list of targets for cyber-attacks. Password spray attacks and credential stuffing are only two of the many new ways for remote attackers to gain access to company's information, without even breaking into organization's infrastructure.

Companies should implement a robust Identify and Access Management (IAM) when using cloud-based services and be security-oriented more than ever: relying solely on username and password is no longer fit for purpose.

Together with the Microsoft published best practices, companies using Office365 should ensure that only the necessary required services are exposed, implementation of MFA, device enumeration, leveraging automation to alert or prevent "risky sign-on" are all in place.

Figure 1. Zero Trust network model for Azure AD applications

Image rights: Microsoft Offensive Security Research (www.microsoft.com/security/blog/2018/06/14/building-zero-trust-networks-with-microsoft-365/)

2 Check machine risk level

CA

Office365

Azure Active Directory

3 Authentication token

4 Azure AD conditional access

1 Get authentication token

Office365 installation

Risk score is compliant

Cloud security risk management

Cloud security

Author: Harshad Ravichand, Senior Cloud Security Consultant

Whether you are migrating existing workloads to the cloud or are a new organization with a cloud native strategy, the utilization of the benefits of the cloud must be balanced by an awareness of the unique risks and differences between traditional infrastructure and the new paradigm.

A recurring cloud security issue that continues to arise is misconfiguration and inadequate change control. According to Cloud Security Alliance's (CSA) report "Top Threats to Cloud Computing: The Egregious 11", misconfiguration occurs when computing assets are set up incorrectly, often leaving them vulnerable to malicious activity.

The examples include unsecured data storage elements or containers, excessive permissions, default credentials and configuration settings left unchanged and standard security controls disabled. Visibility into such misconfigurations is in most cases via API access. The organization can determine policy and alter based on ongoing monitoring and visibility into these infrastructure aspects. Software-defined/event-driven security could then be utilized for automatic remediation (utilizing serverless functions). The organization is then enabled to embrace a modern continuous workflow, in addition to the requirements of their traditional point-in-time audits.

The lack of effective change control is a common cause of misconfiguration in a cloud environment. It is recommended that organizations should embrace automation and employ technologies that scan continuously for misconfigured resources and remediate problems in real-time when designing their cloud strategy.

Migration to the cloud always comes with distinctive challenges in data protection and management. Cloud Access Security Brokers (CASB) technology has surfaced for the unique purpose of securing corporate data while embracing cloud applications and cloud services.

CASB technology addresses a variety of new use cases that define some of the most difficult security problems in cloud computing. These include visibility where CASB helps provide insight into sanctioned cloud services, unsanctioned cloud services (otherwise known as shadow IT) and custom applications that are deployed on public cloud platforms such as Amazon Web Services, Microsoft Azure, Google Cloud and other services that are being used across the entire organization.

A second use case is Data Protection where CASB helps implementing Data Loss Prevention (DLP) policies that regulate the protection of data when uploaded to the cloud, prevent unauthorized sharing of sensitive data to the wrong people, provide notification, block synchronization and download of corporate data to personal devices and many more.

Threat Protection is another situation where CASB helps to protect your cloud from malicious insiders, advanced persistent threats (APTs), ransomware, compromised accounts, attacks on application program interfaces (APIs) and malware. In addition, it allows you to encrypt cloud data with keys that only you can access.

Finally, compliance, which is one of the biggest drivers of the CASB technology. CASB compliance modules allow an organization to audit and tighten the security settings of cloud services. Global compliance polices have made cloud deployment much more complicated and CASB is considered as the best solution to deal with it efficiently.
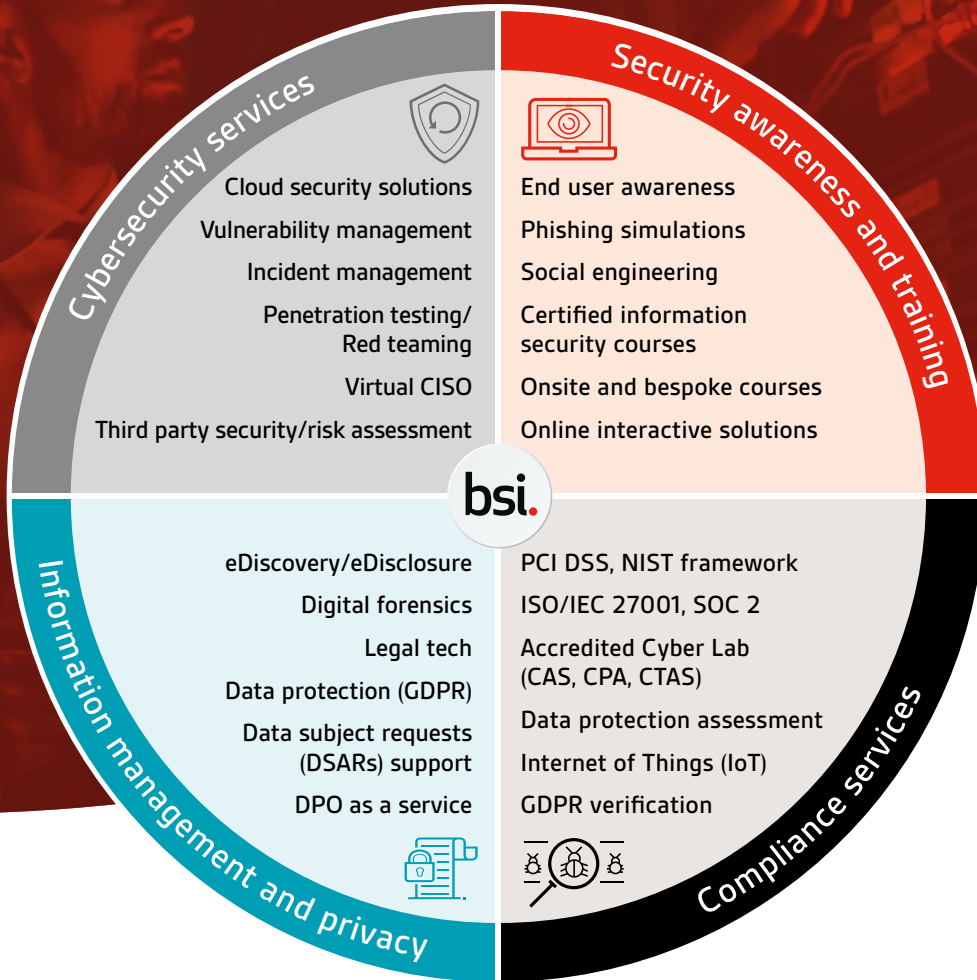
With the global movement of data, applications and services to public and private clouds it is more imperative than ever that organizations consider the use of appropriate technologies to assist making their organization as resilient as possible to the new threats that are posed.

BSI Cybersecurity and Information Resilience
Protecting your information, people and reputation

BSI 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:

Cybersecurity services

- Cloud security solutions
- Vulnerability management
- Incident management
- Penetration testing/ Red teaming
- Virtual CISO
- Third party security/risk assessment

Security awareness and training

- End user awareness
- Phishing simulations
- Social engineering
- Certified information security courses
- Onsite and bespoke courses
- Online interactive solutions

bsi.

Information management and privacy

- eDiscovery/eDisclosure
- Digital forensics
- Legal tech
- Data protection (GDPR)
- Data subject requests (DSARs) support
- DPO as a service

Compliance services

- PCI DSS, NIST framework
- ISO/IEC 27001, SOC 2
- Accredited Cyber Lab (CAS, CPA, CTAS)
- Data protection assessment
- Internet of Things (IoT)
- GDPR verification

Our expertise is accredited by:

CREST | PCi Security Standards Council QUALIFIED SECURITY ASSESSOR™ | CYBER ESSENTIALS | CREST STAR | CHECK IT Health Check Service

bsi.

Find out more

Call: +84 28 3820 0066
Email: info.vietnam@bsigroup.com or
Visit: bsigroup.com