


bsi.

Why your organization needs a Cloud security strategy and how to adopt one

An insights paper





“Adopting to Cloud brings significant advantages, however, organizations need to be mindful of the security issues that Cloud computing can potentially pose.”

How is migration to Cloud transforming global business?

The spread of the COVID-19 pandemic was matched by a significant change in the world of technology as organizations rapidly migrated from a position of Cloud aversion to overnight Cloud adoption. Whilst this mitigation was in many respects necessary to allow businesses to continue to operate in an uncertain period of remote working, many organizations will have migrated their IT needs to the Cloud without a strategic view of the impacts of cybersecurity and compliance.

As the spread of the pandemic is now slowed by the rapid deployment of scientific achievement through vaccination, organizations are now preparing themselves for a return to a new operating normal. But what will this mean for those organizations who raced to the Cloud, and what risks do they now have to resolve?

In this insights paper we will explore the security requirement for effective operation in Cloud computing and highlight the key actions organizations can take before it is too late to resolve past oversights.

When selecting a Cloud service provider, organizations need to both review the security options available and then assess whether they are aligned to the organizational needs to mitigate cybersecurity and compliance risk management burdens. As an example, a business may consider Cloud computing to offer them higher resilience and business continuity, and whilst in the main this may be an accurate assertion, a business may find that during an incident they have little control over how long critical business systems may be offline, and how well a breach is managed, unless those components of risk considerations have been researched and considered during due diligence conducted during the selection process.

For organizations now embarking on their journey to the Cloud, the situation requires a new strategic approach to governance structure, policies, and processes to work with the provider's technology. For those organizations who have already made the transition, the points in this insights paper should serve as a reminder and pose questions that require confirmatory response before business interruption occurs or risk compliance errors are highlighted with damaging consequence to brand reputation.

Author:

Mark Brown

**Global Managing Director,
BSI Cybersecurity and Information
Resilience, Consulting Services**



Mark joined BSI in February 2021 and is responsible for 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 over 20 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

Addressing Cloud security challenges

While the Cloud may offer vital benefits, organizations should be aware of the security challenges when devising a Cloud-first strategy. Here are three key challenges for you to consider:

- 1. Data breaches:** Since there are public and private Cloud offerings, resolving problems is in the third-party provider's hands. Consequently, the business may have little control over how long critical business systems may face downtime
- 2. Compliance complexity:** Achieving complete compliance while using Cloud offerings can be very complicated. Many companies attempt to gain compliance by using a Cloud vendor that is deemed fully compliant. However, in many circumstances a organization may find itself facing non-compliance and have little control over it
- 3. Insecure interfaces and APIs:** Unfortunately, not every API is fully secure. Ensuring an API's security throughout, especially at later stages, is a challenge when building an application layer on top of these APIs.

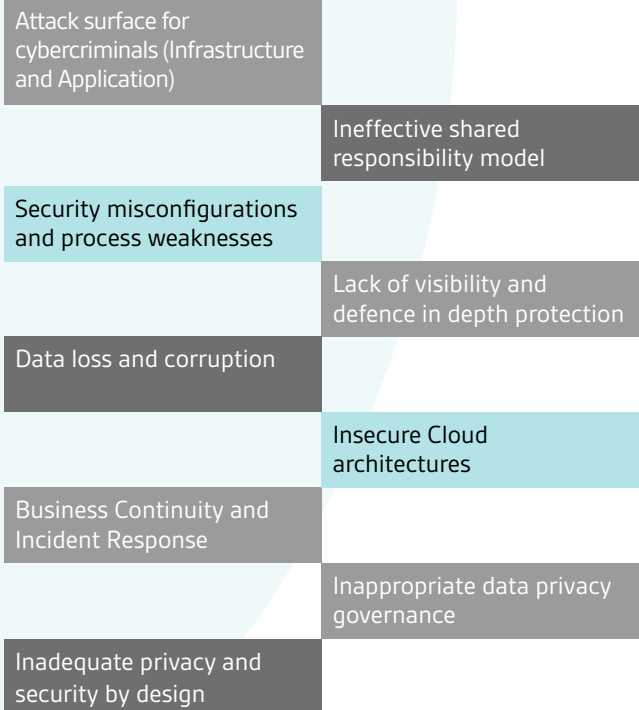
Other potential threats

Account or service traffic hijacking	Man in the middle	Distributed Denial of Service (DDoS)
--------------------------------------	-------------------	--------------------------------------

What could go wrong?

Cloud is more secure than ever today, but organizations are still experiencing a surge in the number of data breaches. This is primarily due to a lack of understanding of Cloud architecture and awareness of responsibility for securing data. Organizations need to understand that Cloud security is a shared responsibility model, to be fully aware of those responsibilities, and perform necessary actions depending on the type of Cloud computing service model they choose such as infrastructure, platform and software as a service (IaaS, PaaS, SaaS).

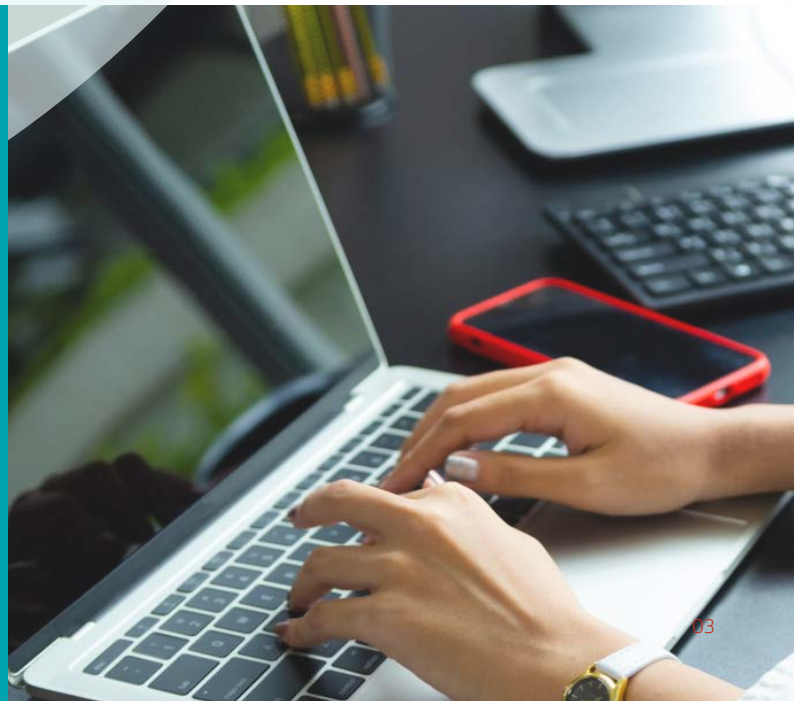
When you are adopting Cloud technologies and services there are some deceptions that can get your organization exposed to risks – such as:



“Cloud is more secure than ever today, but organizations are still experiencing a surge in the number of data breaches. This is primarily due to a lack of understanding of Cloud architecture and awareness of responsibility for securing data.”

Mark Brown, Global Managing Director, BSI CSIR

Why your organization needs a Cloud security strategy and how to adopt one
 Call: +1 800 862 4977 (US) / +44 345 222 1711 (UK) / +353 1 210 1711 (EMEA)
 Email: cyber@bsigroup.com



Adopting Cloud with a secure strategy

Some of the challenges involved in adopting to Cloud not only cover protection and compliance, but also operational considerations.

So, while you migrate to Cloud, it is best to adopt security strategies, such as:

01

Having the ability to integrate security solutions and maintain control over the dynamic infrastructure

An integration of a complete security platform can support IT and security teams, save time, and speed up identifying signs of a data breach accurately

04

Striking a balance between protection and compliance

Allowing hackers to spend more time, energy, and resources than they initially estimated into breaching the organization, strengthens the security. Making attackers go through several layers of defences would make them trigger an alert before reaching the organization's most sensitive information

02

Deploying consistent security policies across the hybrid Cloud

Newly generated virtual servers should immediately adhere to group-specific guidelines and newly generated VDI's., as contrarily, the consequences could be unfavourable. There may be a case that they are left unprotected against threats for as long as they are operational

03

Automating virtual machine (VM) discovery

To ensure visibility and to have control over the dynamic infrastructure without sacrificing performance, usability, or security, it is essential that the security solution embraces the same elasticity and enables organizations to maintain an "any moment in time" view of their environment

"Making attackers go through several layers of defences would make them trigger an alert before reaching the organization's most sensitive information."

Mark Brown, Global Managing Director, BSI CSIR



What are the key watch-outs?

Lack of visibility and transparency

A lack of visibility to security vulnerabilities can lead to a business failing to identify potential risks

Vendor lock-in

If crucial business applications are locked into a single provider, it can be challenging to make tactical decisions such as migrating to a new vendor

Insufficient due diligence

For businesses that lack the internal resources to evaluate Cloud adoption implications, the risk of deploying an insecure platform is real

Having little control

Responsibility for distinct issues of data security necessitates being fully defined by both parties before any deployment of services. Neglecting to do so could point to a situation where there is no clearly defined way to deal with possible risks and solve current security vulnerabilities

Shared technology vulnerabilities

The accountability is upon the Cloud vendor to see that this does not happen, however, no vendor is perfect. Security vulnerability caused by another user in the same Cloud is always likely to affect every other user

17%

Sectors such as Media have only 17% Cloud adoption due to lack of visibility and control¹

80%

80% of decision makers blame the fear of vendor lock-in for their Cloud aversion²

75%

75% of IT managers lack confidence in ongoing data protection and privacy in the Cloud³

Establishing best practices for Cloud adoption

The first factor is to make sure your requirements and vision as a CIO, CISO or technical leader match with the organizational vision and goals in the short and long term. Perform a current state assessment of all your Cloud capabilities with respect to people, processes, and technology. It is recommended to understand the size of your organization, budget, data requirements and whether you have regional and global footprints.

The onus is on the organization to develop a plan for ensuring everyone has the required knowledge to make the transition successful. **Don't blame your employees.** You need to invest in employee training to make cybersecurity awareness a priority. It demands a mindset shift that does not view a person who opens the wrong attachment as the point of failure, rather instead acknowledging that it is the security and training structure around that individual which has failed and reviewing it.

It is essential to have a clear awareness of how much of a threat data breaches have on the organization and employees need to be made clearly aware of this also. Building clear cybersecurity guidelines for employees can be a significant asset because it supplies them with a resource to look at when they need help. Committing to an all-inclusive variety of approaches to direct your team ahead of any recurring issues as well as evolving problems highlighting the best solutions is advantageous.

Some of the most potent cyberattacks that are out there today rely on human error and are done through email. Many attackers cast wide to see what they can get, but an advanced attacker with the correct information can create a highly targeted scheme to work their way into a system or network.

At BSI, we would advise investing in a 'live fire' simulation to test awareness levels so that employees can learn to identify risks. This will provide data on where improvements can be made and support planning for future training sessions.

Don't blame your employees. You need to invest in employee training to make cybersecurity awareness a priority.⁴

"Building clear cybersecurity guidelines for employees can be a significant asset because it supplies them with a resource to look at when they need help."

Mark Brown, Global Managing Director, BSI CSIR



How to establish best practices?

Training is the key here. Constant reminders about the threats that are out there and a "live fire" exercise demonstrates how easily you can fall prey to an attack. Cybersecurity is a team effort, and there is a need to put employees in an active position to succeed. It is therefore vital to ensure that your employees are well trained, educated or certified to use Cloud services and technology securely and efficiently.

Organizations need to develop Cloud strategy by performing a current state assessment, determining the desired state, performing a gap analysis, and developing initiatives.

Your business needs to take steps to ensure you do not find it in the news headlines.

BSI's Cloud solutions approach – an end to end service model

01

Cloud risk assessment:

Designed to assist you to evaluate the suitability of migrating services to Cloud environments and assess existing risks in hybrid or full Cloud deployments. Meaning you are prepared with a 'sword and armour' before the attackers even consider sneaking into your system

02

Secure Cloud design:

To detect potential exposure points for sensitive information, we design, build, and deliver secure Cloud environments based on your specific security and compliance considerations

03

Intelligent Cloud migration:

A holistic assessment of your security layers across Network, Applications, People and Processes, helping you save money, improve security, and increase awareness

04

Cloud testing and audit: As a partner of the Cloud Security Alliance (CSA), we utilize many of its industry leading tools to ensure that you are safe in your choice of Cloud deployment and understand the associated risks

05

Cloud incident response: From identifying risks to finding measures to mitigate them, record outcomes, and minimise their future possibility by advising you on the best practices when dealing with Cloud service providers and other related third parties

Why BSI?

At BSI, we have a large team of highly experienced, industry-leading consultants that help ensure that you and your business have all the Cloud security requirements you need. The team has years of industry-relevant experience and expansive multiple sector experience. We provide you with cutting edge and leading insights to ensure your Cloud infrastructure and connected assets are secure and have information resilience.

Added Services

- Secure Web Gateway as a Service
- Cloud Access Security Broker and Cloud DLP
- Identity and Access Management
- Security Information and Event Management
- Software Asset Management
- User and Entity Behavioural Analytics / Security Orchestration, Automation and Response
- Email security and Security Awareness Training

Disclaimer

BSI is an accredited Certification Body for Management System Certification and Product certification. No BSI Group company may provide management system consultancy or product consultancy that could be in breach of accreditation requirements. Clients who have received any form of management system consultancy or product consultancy from any BSI Group company are unable to have BSI certification services within a 2 year period following completion of consultancy.



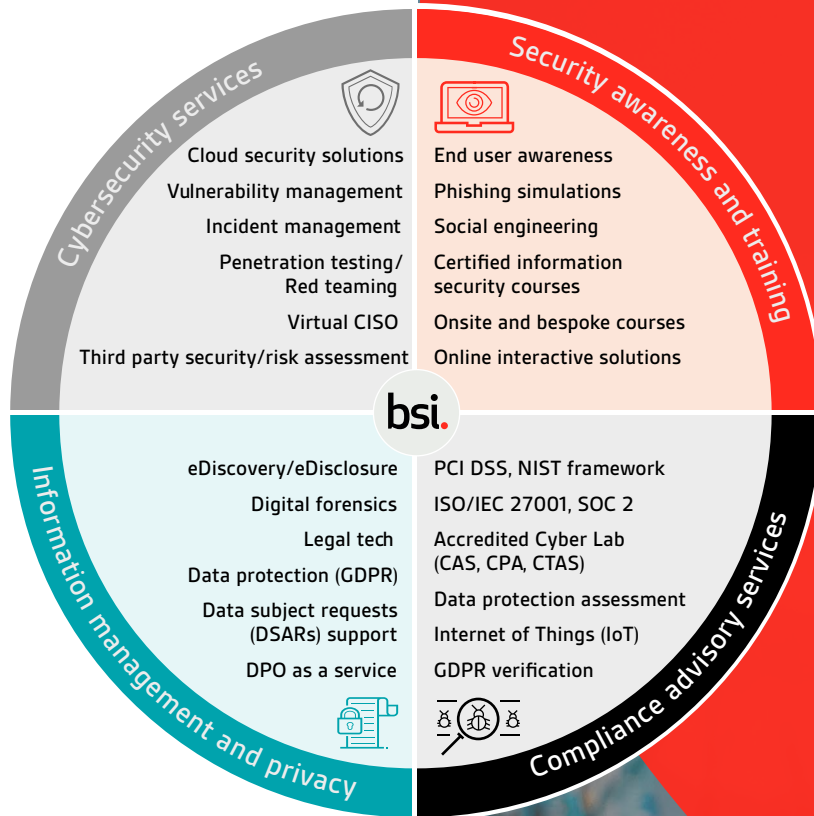
References

- Jones, M., 2021. Best Practices for How to Train Employees for Cyber Security. [online] Coxblue.com. Available at: <https://www.coxblue.com/8-tips-and-best-practices-on-how-to-train-employees-for-cyber-security>
- Arsene, L., 2021. Five Steps to Address Cloud Security Challenges. [online] Network Computing. Available at: <https://www.networkcomputing.com/network-security/five-steps-address-cloud-security-challenges>
- Databrilliancesoftware.com. 2021. Five Steps to Address Cloud Security Challenges. [online] Available at: <https://www.databrilliancesoftware.com/article.cfm?ArticleNumber=15>
- IDG. 2021. Maximizing productivity in remote work. [online] Available at: <https://www.cio.com/native-link/boundless-agility/collection/working-remotely-with-full-productivity/article/maximizing-productivity-in-remote-work>
- Deshmukh, S., 2021. Cloud Computing Security Challenges and Considerations - DZone Cloud. [online] dzone.com. Available at: <https://dzone.com/articles/cloud-computing-security-challenges-and-considerat>

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, or consultancy services or training and qualifying your people, we'll help you achieve your security goals.

Our Cybersecurity and Information Resilience 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

