# Digital trust

## Achieving a state of Information Resilience

Whitepaper

bsi.

Inspiring trust for a more resilient world.

# Introduction

"A resilient organization is not one that merely survives over the long term but flourishes – passing the test of time"

**Howard Kerr, Chief Executive, BSI Group**

'Achieving a state of enhanced and sustainable information resilience', what does this mean? Firstly, in this information age, the cyberthreat landscape is constantly proliferating, becoming more sophisticated and growing exponentially. With the emergence of new wave cyber threats with examples of malware impacting Linux and Mac operating systems (OS), UEFI malware and Crypto Mining malware, not to mention end user security issues and phishing attacks, the need for resilience has never been so profound. Subsequently, companies must learn to adapt, be agile, anticipate the omnipresent threats and incorporate a culture of sustainability. These are the tenets of an organization integrating a protocol for information resilience.

In many organizations, across multiple sectors, varying industries and differentiating landscapes, it is the senior leadership whom are tasked with the ultimate responsibility of ensuring their information systems and services foster this state of information resilience. This is a challenge, of course, especially when the spectrum of potential issues is so vast. Information accessibility, security, protection, back up, integrity, assurance and more are only some of the dilemmas leadership need to concern themselves with. However, satisfying these information conundrums with the ability to access this secure information at exactly the precise moment it is needed, regardless of the threats, is the true hallmark of a company who has achieved or is on the pathway to achieving information resilience.

Moreover, leadership who have achieved this desired state, with confidence, can truly trust that their organization is able to proactively anticipate, identify, manage and mitigate the potential threats and associated risks. In addition, and more importantly, they are also able to deal with threats before they degrade the core functions of the business.

Conclusively, delivering a state of information resilience is achievable by any company that realizes the criticality of its information assets they have under their control. It is a reasonable question for any leadership group to ask of itself, how resilient are we? Do we have the ability to not merely survive but flourish over the long term? And if not, how do we get to this point?

# Evolving to a position of ongoing information resilience

**The evolutionary path an organization will take to adopting a stance of ongoing information resilience does not necessarily need to be complicated, however it does need to involve the business.**

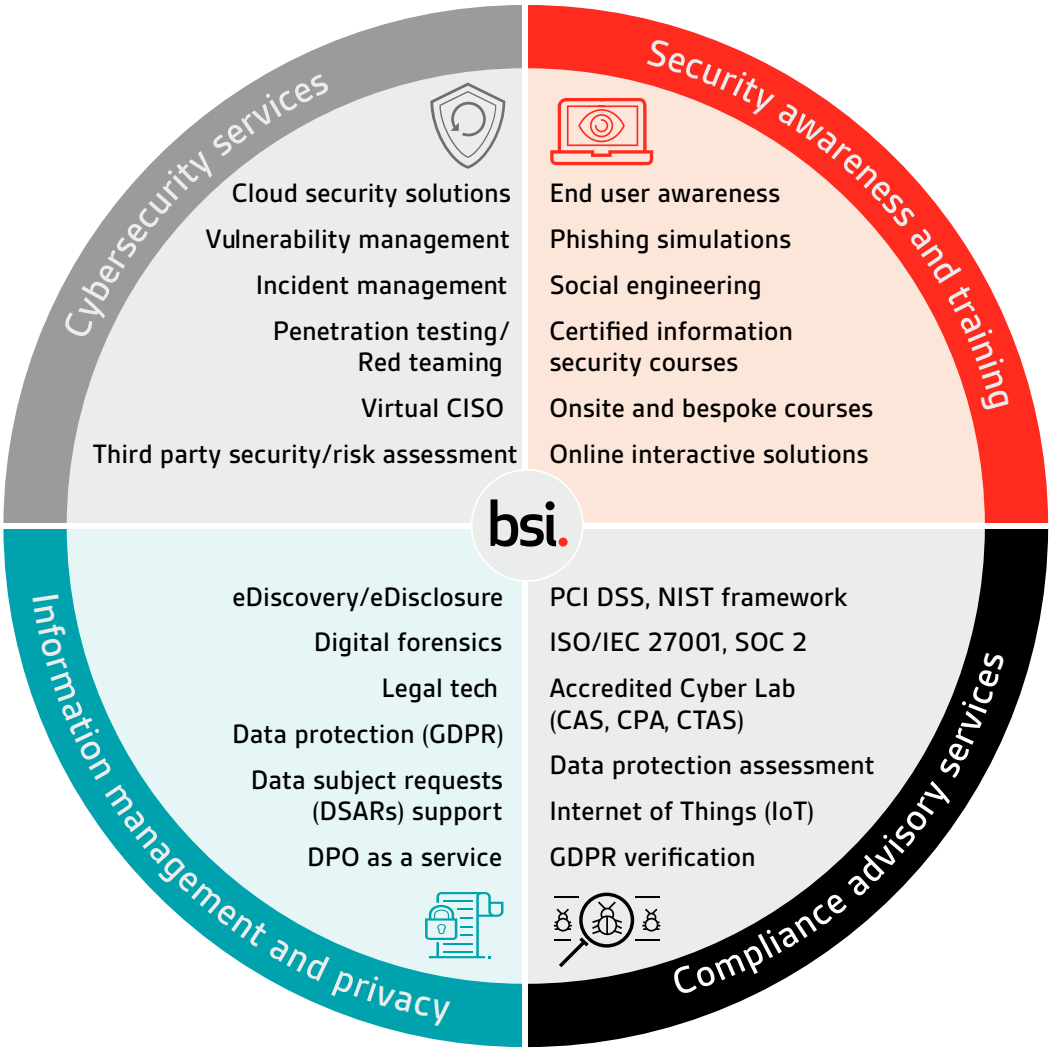
Everyone in the company from entry level positions right up to senior leadership levels will play a part in bringing about information resilience. Getting to this point will require an understanding of where your organization is currently placed against industry best practices for achieving information resilience, in terms of both prevention and preparedness for the realization of residual risk. Organizations should consider four key areas in their strategy for achieving information resilience.

**1 Cybersecurity postures**

**2 Information management and privacy practices**

**3 Security awareness and training processes**

**4 Compliance to requirements and regulations**



# Cybersecurity

## Vulnerability management

**Knowing where potential vulnerabilities lie is critical to ensuring information resilience.**

Proactively seeking out these vulnerabilities in both infrastructure and application ecosystems will afford teams the opportunity to discover weaknesses and resolve them before a malicious attacker gets the chance to exploit them.

Proactively finding these vulnerabilities comes as a result of using the correct methods for the scenario. For most implementing a vulnerability management program should suffice. For organizations involved in application development, penetration testing will also be an excellent addition to your program.

Depending on the nature of their business, certain companies will employ Red Team testing. This can take vulnerability management to another level, involving people and processes in assessments as well as technology estates.

## Leadership

**Whilst every company will have its core functions and will need to ensure its own information resilience position, it may not be able to have full time expertize inhouse.**

Reasons for this can be varied and all equally valid. This, however, should never be a barrier to ensuring information resilience.  Choosing a partner organization to provide expertize in areas such as Virtual CISO, Data Protection Officer as a Service can overcome these issues, as well as eliminating the lengthy process of training up existing staff members into the role or the risk of spreading an existing staff member too thin.

## Third party supplier management

**When ensuring the availability of your information assets you may realize that those information assets are derived from third party sources.**
The proliferation of interconnectivity and consumable APIs can leave a company in a position of dependency on third parties. To achieve information resilience, you should understand the risk posed to your own resilience from third party suppliers, using systematic and repeatable processes.

## Incident management planning

**In order to have an information resilient organization is important to plan for the unexpected.**

Incidents need to be managed in a systematic way with roles and responsibilities pre-allocated. By ensuring this is the case, the organization will have in place best practice methodologies such as those contained in the "NIST Special Publication 800-61 Revision 2" or "ISO/IEC 27035-2:2016 Information technology – security techniques – Information Security Incident Management".

Incident management exercises should also be implemented to ensure that the measures put in place are regularly practised outside of an actual event.

This service provision should open a door into understanding any knock-on effect from the incident such as advice on contacting a supervisory authority under the GDPR requirements, or reporting a payment card information breach to the relevant acquiring banks.


Call: +44 345 222 1711 /+353 1 210 1711 Email: digitaltrust.consulting@bsigroup.com Visit: bsigroup.com/digital-trust

# Information Management and Privacy

## Data Loss Prevention (DLP)

**Your information should stay within the boundaries set by the company.**

Data loss can occur as a result of malicious or negligent activity and can lead to exposure to regulatory fines, negative publicity, customer dissatisfaction, or even possible litigation.

A systematic methodology should be in place to minimize the threat posed to its information resilience by data loss. Classification schemes as well as user awareness can contribute to the success of a data loss program as well as DLP systems which can help automate the process of policy enforcement.

## Forensic services

**Business should also have in place a resource or partner organization to utilize in the event of an incident which is regarded as a major or sophisticated breach.**

Service organizations in this space will typically provide you with the ability to triage an incident, provide forensic information aiding in root cause identification as well as offer a path to remediation.

## Privacy

**All organizations should examine their obligations under relevant privacy legislation.**

European organizations will of course be subject to the EU General Data Protection Regulation, where their operations require the processing of personal data.

Resilience in this regard is learning how your information assets should be managed with respect to the legislation. Particularly around areas such as understanding the need for data protection impact assessments, handling data subject access requests, the right to be forgotten and other key components of the legislation. Undertaking a review or gap analysis can ensure there are no issues which could be prevented by a proper understanding of their current position and the development of a roadmap to achieving alignment.

Legislation in this space may also mandate companies to have full time roles appointed to ensure that regulation is implemented, and the rights of the data subject are safeguarded. Not every business carries the ability to hire the right personnel and whilst they may be mandated to do so, may not actually have a full-time role for them.

Consideration at this stage in an organization's journey to information resilience should be given to employing a Data Protection Officer (DPO) – as a service offering. Doing so will allow businesses to remove the 'key person dependency risk' associated with an internal DPO, reduce the overhead costs related with employing an internal DPO, plus being able to quickly access specialized, skilled and experienced advise in the event of a personal data breach.

# Security Awareness and Training

## Threat awareness

**It's arguable to say that an organization's greatest asset is its people. When it comes to information resilience, all organizations striving to achieve this state are heavily reliant on the combined effort of the wider team. Leadership needs to ensure that those they are relying on are adequately and regularly trained to firstly identify and secondly respond to issues happening.**

Training such as information security awareness can help identify common attack methods such as phishing, vishing, ransomware and web content hosting malware. Training partners should be able to deliver to your team online or in formalized offsite courses as well as bespoke on-site courses to suit needs of an organization.


# Compliance

## Information Security Management Systems (ISMS)

**Having an information security management system in place will make significant inroads into achieving an ongoing state of information resilience.**

The good news on this front is that these programs are a well-established path with standards like ISO / IEC 27001, NIST and Common Criteria for Information Technology Security Evaluation being in place for many years and are very mature. Frameworks will typically cover areas such as risk management, systems development and acquisition, Identity and Access Management (IAM), and asset management.

There is no need to reinvent the wheel in this regard. A detailed gap analysis can reveal an organization's current posture against the best practice guidance contained within the standards. Certification to an internationally recognized standard such as ISO/IEC 27001 will not only enhance your position regarding information resilience but may also be a value position for your clients.

## Business continuity and disaster recovery planning

**This is defined as the process of creating systems of prevention and recovery to deal with potential threats to a company.**

This should be considered as a critical component to achieving the desired outcome of information resilience for any organization. You should understand the business impact of not having your information assets available to you during an incident. This impact should be assessed systematically, and in a repeatable manner in order to allow your organization to identify key assets which support critical business processes. Businesses should have in place a solid business impact assessment methodology. This assessment will identify critical business processes and ensure prioritization in the event of disaster recovery or business continuity plan invocation.

Plans and the associated actions should be revisited on a regular basis to ensure that they are still relevant and consider any change which may have occurred since its creation. Business continuity planning should be implemented throughout the organization and tested at regular intervals to ensure the business is able to continue to run when an event outside of the norm occurs e.g. severe weather events, unavailability of key buildings, mass transit unavailability.


Call: +44 345 222 1711 /+353 1 210 1711 Email: digitaltrust.consulting@bsigroup.com Visit: bsigroup.com/digital-trust

# Conclusion

**Achieving a state of enhanced and sustainable information resilience can be achieved by any organization. Information resilience empowers organizations to safeguard its information – physical, digital and intellectual property – throughout its lifecycle from source to destruction. This requires the adoption of information security-minded practices enabling stakeholders to gather, store, access and use information securely and effectively.**

Achieving this state requires four interconnecting sub-domains to be addressed with strategies, plans and actions:

1. **Cybersecurity**
2. **Information management and privacy**
3. **Security awareness and training**
4. **Compliance to requirements**

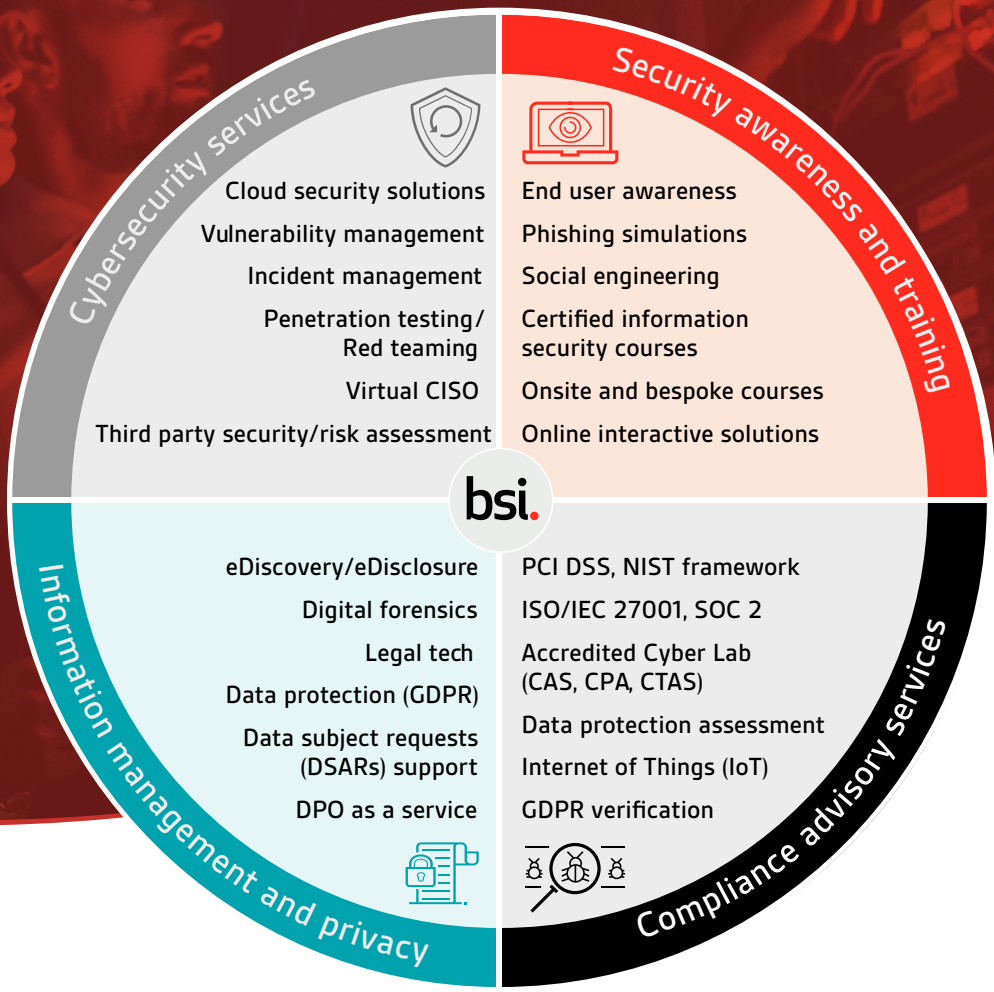
When addressing these perennial and growing challenges across the cyber-domain, organizations need to employ operational best practises and good governance. They must be implemented in areas such as information security management, privacy management, third party supplier management, threat awareness, leadership, vulnerability management, Data Loss Prevention (DLP), change management and review processes.

Organizations with high levels of information resilience will plan for the unexpected. Critical components of this will be understanding the importance of its business processes derived from its business impact analysis. They should also be able to carry on business operations in the face of significant events as a result of its business continuity plan, and finally its ability to recover from a serious issue as a result of its disaster recovery planning. Effective implementation of all these concepts as well as buy into the concepts will not only allow you to survive a serious incident but anticipate this, ensuring longevity and sustainability flourishing over the long term, passing the test of time.

# Digital trust

## Protecting your information, people and reputation

Digital trust 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: digitaltrust.consulting@bsigroup.com
Visit: bsigroup.com/digital-trust

**IE/International**

+353 1 210 1711
digitaltrust.consulting.IE@bsigroup.com
bsigroup.com/digital-trust