For any organisation to survive in an emerging information security ecosystem, standard security measures are no longer sufficient. The changing business landscape now requires an approach towards information resilience to enable an organisation to prevent, respond and recover from potential threats, and maximise the trustworthiness of its information.

To better understand why adopting a new approach is important, we discuss the characteristics of a business ecosystem and the common pitfalls of information security.

In this white paper, we also share the right approach to information resilience, supported by a relevant implementation framework.

Notis Iliopoulos  
Manager - Cyber Security  
WSP Middle East
Information resilience and its importance

Information resilience is the strategic and holistic approach towards protecting all types of sensitive information, in all phases of the information lifecycle. It demands continuous assurance, improvement and response.

To better understand why it is vital to adopt a new approach to protecting critical information, let’s have a look at the main characteristics of today’s business ecosystem which are driven by dynamic and constant change:

- **Shared services economy** - Organisations have moved towards collaboration and the development of shared services instead of building new services or products, which is driven by the need to bring new services to the market faster. Such a shared economy business model requires more collaboration and communication between stakeholders, and consequently greater information sharing.

- **Innovation & growth utilising technology** - Innovation is an essential part of the strategy of any sustainable business. This means producing something that is new to the market or changing the way existing products and services are being offered. In the next 3 to 5 years, innovation will take advantage of technological developments like never before.

- **Digitisation** - Innovation and competitive advantage has a key reliance on technology, and this goes as far as organisational growth being impacted by the adoption of new technologies. Digital strategies are utilised in order to reach clients through any digital pathway, as well as to enhance the efficiency of internal operational processes. Business models are changed because of the effects of digitisation.

- **Compliance goes regional and aims at critical infrastructure** - Regional compliance requirements, especially in information security, are becoming stronger than global requirements.

- **Threats target a wider spectrum** - Threats related to the protection of critical business information, go beyond typical ICT. Critical information often resides on resources not fully controlled or owned by the organisation. Interconnectivity between customers, suppliers and other stakeholders, and the use of smart devices, create a borderless business ecosystem.

The above characteristics are also components of a sustainable and resilient organisation which is able to absorb and adapt to change. Enterprise resilience goes beyond focussing on what could interrupt day-to-day business operations. It constantly questions what could prevent the organisation from achieving its goals and objectives.

Risks related to information protection are usually managed in an ad hoc manner, resulting in more risks. This is the most common scenario because most organisations lack a holistic approach to risk management. They tend to focus more on IT-related risks affecting the protection of critical business information. Information risks related to third parties, HR security, insider threats, privacy and, effectiveness of policies and procedures are often overlooked.

Quite a large number of organisations rely only on technical vulnerability assessments and penetration tests as a source to identify risks related to the protection of critical information. Risk evaluation, treatment and mitigation are often not aligned with the Enterprise Risk Management Framework which results in:

- a) downgrading the importance of information security risks, and
- b) not having these risks evaluated against business impact and how this risk might affect business objectives and strategy.

Most organisations do not focus on the root causes of information security risks. This ineffective approach and treatment is what consequently affects the resilience of the organisation. Furthermore, some organisations refuse to prioritise the treatment of information security risks in the same way they prioritise the treatment of financial and business-related risks.

The majority of organisations also loosen up their tolerance to risks related to the protection of critical information when the organisation is under stress. This is due to lack of readiness and proper planning.

The common pitfalls of information security

In such highly diverse and radically changing business environments, organisations often encounter some common pitfalls regarding information protection:

- Compliance goes regional and aims at critical infrastructure - Regional compliance requirements, especially in information security, are becoming stronger than global requirements.

- Threats target a wider spectrum - Threats related to the protection of critical business information, go beyond typical ICT. Critical information often resides on resources not fully controlled or owned by the organisation. Interconnectivity between customers, suppliers and other stakeholders, and the use of smart devices, create a borderless business ecosystem.

The above characteristics are also components of a sustainable and resilient organisation which is able to absorb and adapt to change. Enterprise resilience goes beyond focussing on what could interrupt day-to-day business operations. It constantly questions what could prevent the organisation from achieving its goals and objectives.

Risks related to information protection are usually managed in an ad hoc manner, resulting in more risks. This is the most common scenario because most organisations lack a holistic approach to risk management. They tend to focus more on IT-related risks affecting the protection of critical business information. Information risks related to third parties, HR security, insider threats, privacy and, effectiveness of policies and procedures are often overlooked.

Quite a large number of organisations rely only on technical vulnerability assessments and penetration tests as a source to identify risks related to the protection of critical information. Risk evaluation, treatment and mitigation are often not aligned with the Enterprise Risk Management Framework which results in:

- a) downgrading the importance of information security risks, and
- b) not having these risks evaluated against business impact and how this risk might affect business objectives and strategy.

Most organisations do not focus on the root causes of information security risks. This ineffective approach and treatment is what consequently affects the resilience of the organisation. Furthermore, some organisations refuse to prioritise the treatment of information security risks in the same way they prioritise the treatment of financial and business-related risks.

The majority of organisations also loosen up their tolerance to risks related to the protection of critical information when the organisation is under stress. This is due to lack of readiness and proper planning.
Proposed approach to information resilience

For information security to be able to support current and future business needs, as well as to support enterprise resilience, it is necessary to evolve and provide an effective way for organisations to protect their information in an extremely dynamic and risky environment.

Information resilience, considered a better approach to information security, is characterised by:

- **Business & information centric approach** – Organisations must follow the information lifecycle and protect information wherever it resides.

- **Holistic approach to risk management** – Integrate information security risks and risk management methodologies with enterprise risk management & business impact approaches.

- **Protect information outside the organisation** – Define controls for information that exist in resources that cannot be controlled by the organisation.

- **Response & effective protection** – Even when the organisation is under stress, critical information assets need to be adequately protected.

- **Establish continuous assurance, improvement & response** – This means effective implementation of the required controls based on each organisation’s risk profile and compliance requirements; integrate compliance requirements with governance & risk management processes; establish a process for continuous risk monitoring & effectiveness control. The readiness to respond to any kind of incident that can affect an organisation’s resilience is very important.

- **Maximise the sustainability & trustworthiness of information** – The primary objective is to support business growth and sustainability and all information protection decisions should be based on business needs.

The WSP approach

WSP has established its own approach to information resilience, supported by a relevant implementation framework. We follow a holistic approach towards protecting all types of sensitive information, in all phases of the information lifecycle throughout all business verticals, regardless of the underlying business and technology ecosystem.

Our aim is to maximise the resilience of critical business information and keep information trustworthy even when the organisation is under stress.

Information Resilience is all about continued Assurance, Improvement and Response.

- **Assurance** – Build and implement the Information Security Strategy based on the risk profile and the compliance requirements of each organisation. Information protection risks should be identified holistically and take into consideration the different types of risk assessment exercises. Assurance also requires the integration of the information security processes with the relevant operational processes and wider enterprise management systems and frameworks (e.g. risk management, change management, incident response, compliance). Adoption of the management & technical controls focusing on effectiveness, transparency and accountability is also critical.

- **Response** – Response to any kind of event might affect the resilience of information, resulting in less than required protection of the information assets. This is not only about responding to incidents related to hacking attempts, but also about responding to organisational and technological changes, changes in business models and strategies, as well as responding to changes in the threat landscape, social and cultural changes, all of which can affect the resilience of business information.

- **Improvement** – The required level of information protection can only be maintained and maximised if we continuously improve the efficiency, effectiveness and the level of adoption of management & technical controls. This encompasses having a continued improvement process in place in order to prove compliance with standards and regulations. It is about approaching improvement holistically, i.e. improving all aspects of incident response, all aspects of user access control, all aspects of risk management. It is about improving anything related to the protection of critical information regardless of the underlying technology, interested parties and organisational structures.
WSP’s services and implementation approach are built around the following guiding principles:

- Adoption of the required processes and controls to establish continuous assurance, improvement, and readiness to respond.
- The objective of any implementation, framework and service we build is to maximise the trustworthiness of information.
- Information needs to remain trustworthy, even when the organisation is under stress.
- Information needs to be protected anywhere it resides, and adequate controls shall be applied throughout the information lifecycle and throughout the flow of information within and outside the organisation.

Following this approach, we assist our clients to achieve information resilience by establishing two continuous processes for Governance & Assurance and Resilience & Response:

Via our Governance & Assurance offering, we aim to assist our clients to build a continuous process to:

- Assess the risks & vulnerabilities for all information assets, taking into consideration their true business impact.
- Define and review information security governance in accordance with strategy and compliance requirements for information security, taking into consideration our guiding principles regarding information resilience.
- Effectively implement, communicate and adopt the required management and technical controls. Adoption of controls differs from the implementation of controls because we focus on the effective operation of controls rather than proving that controls are implemented for the sake of compliance.

Via our Resilience & Response offering, we aim to assist our clients in building a continuous process to:

- Respond to any kind of event related to information resilience and build-enhance the controls which affect information resilience.
- Monitor the effectiveness of management and technical controls, and the treatment of risks and vulnerabilities.
- Continuously improve the whole information assurance and resilience process. The level of information resilience will be increased when we elevate the level of effectiveness of the implemented controls, and when the maturity of processes is enhanced.

Our implementation approach to information resilience is based on effectiveness and applied innovation, utilising our worldwide expertise through WSP’s Information Assurance & Resilience Innovation Hub, and driven by our Middle East practice.
WSP is one of the world’s leading engineering professional services consulting firms. We are dedicated to our local communities and propelled by international brainpower. We are technical experts and strategic advisors including engineers, technicians, scientists, architects, planners, surveyors and environmental specialists, as well as other design, program and construction management professionals. We design lasting solutions in the Property & Buildings, Transportation & Infrastructure, Environment, Industry, Resources (including Mining and Oil & Gas) and Power & Energy sectors as well as project delivery and strategic consulting services. With 1,700 talented people in 11 offices across the Middle East, we engineer projects that will help societies grow for lifetimes to come.

www.wsp.com