Where next?

The full report Cyber Security Strategies: Achieving cyber resilience is available from the ISF website. It helps business leaders and information security professionals understand the serious threat presented by cyberspace, and it provides practical guidance on the organisational response needed to address this threat.

It does this by:

- explaining cyberspace, cyber security, the nature of the cyber threat and the concept of cyber resilience;
- describing the similarities and connections between cyber security and information security;
- introducing the ISF Cyber Resilience Framework, a vision of organisational cyber resilience;
- outlining practical steps organisations can take to customise and implement the framework;
- providing clarity that can be used to communicate the issue, challenges and plan to stakeholders.

Input for the report was gathered from workshops and online meetings with ISF Members around the world, interviews with ISF Member experts and other experts, Member case studies, previous ISF research and reports including Information Security Governance and Risk Management, and thought leadership provided by the ISF Global Team.

The ISF Cyber Security Strategies report is available free of charge to Members of the ISF. Non-Members are able to purchase a copy of the report by contacting Steve Durbin at steve.durbin@securityforum.org.

About the ISF

Founded in 1989, the Information Security Forum is an independent, not-for-profit association of leading organisations from around the world. It is dedicated to investigating, clarifying and resolving key issues in information security and developing best practice methodologies, processes and solutions that meet the business needs of its Members.

ISF Members benefit from harnessing and sharing in-depth knowledge and practical experience drawn from within their organisations and developed through an extensive research and work program. The ISF provides a confidential forum and framework, which ensures that Members adopt leading-edge information security strategies and solutions. By working together, Members avoid the major expenditure required to reach the same goals on their own.

Contacts

For more information on the ISF’s Cyber Security Strategies report, please contact:

Michael de Crespiigny
Tel: +44 (0)20 7213 1745
Fax: +44(0)20 7213 4813
Email: michael.de.crespiigny@securityforum.org
Web: www.securityforum.org

Disclaimer

This document has been published to provide general information only. It is not intended to provide advice of any kind. Neither the Information Security Forum nor the Information Security Forum Limited accept any responsibility for the consequences of any use you make of the information contained in this document.

Cyber Security Strategies

Achieving cyber resilience

“2010 was the year the Internet got scary. Get used to it.” — Arik Hesseldahl, technology writer

Business leaders recognise the enormous benefits of cyberspace and know that cyberspace increases innovation, collaboration, productivity, competitiveness and engagement with customers. Yet they are having difficulty determining the risk versus the reward.

The benefits of cyberspace come with significant risks, and the threat of cyber attack is firmly at the top of the board agenda. While organisations are exploiting the business benefits of cyberspace they may not realise that cyberspace confers the same benefits to those who attack our organisations. Hacker groups, criminal organisations and espionage units worldwide have access to powerful, evolving capabilities, which they use to identify, target, and attack. They even have well-developed marketplaces for buying and selling the tools and expertise used to target and execute attacks.

We call this Malspace.

It is critical that organisations understand Malspace and the increased threat it poses. Organisations should develop a business plan to exploit cyberspace that identifies threats, considers the limitations of IT and information security, and develops cyber resilience.

Based on insights from the Information Security Forum’s global Membership and ISF Global Team, the ISF Cyber Resilience Framework identifies the key capabilities that organisations should possess to increase their resilience to the threats from cyberspace.

Cyberspace is critical to most organisations today; disconnecting is not an option. By implementing the ISF Cyber Resilience Framework — supported by the wide range of ISF tools and materials — organisations can develop cyber resilience and be better able to withstand impacts from evolving cyber threats. Only then can organisations safely realise the benefits of cyberspace.
Developing cyber resilience is the only way to survive in cyberspace

Malspace is a complex, highly-functional and developing industry. It includes sectors for all aspects of modern crime, including the development and sale of sophisticated attack tools, services to help plan and coordinate attacks, and large scale laundering of stolen assets. It operates at the scale and with the sophistication of other global industries.

New threats will appear overnight that can’t be predicted or easily prevented. Traditional risk management is insufficiently agile to deal with the potential impacts from activity in cyberspace. Enterprise risk management must be extended to organisational risk and cyber resilience.

The ISF Cyber Resilience Framework is a vision of organisational resilience that can be established to deal with cyberspace threats head-on – building on current information security arrangements.

**KEY FINDINGS**

1. The benefits from cyberspace are immense, as are the risks
2. Organisations must embrace uncertainty and develop cyber risk resilience
3. Malspace is a global industry that has evolved to deliver cyber attacks
4. Impacts from cyber threats can have a very long and disproportionate risk tail
5. Hacktivism presents significant threats to the organisation, not just information security
6. Cyber security is more than information security
7. Cyberspace vastly increases information security risk
8. Information security is fundamental and more important for security in cyberspace
9. The complexity of cyberspace enables threats to combine quickly in unpredictable and dangerous ways
10. It is essential to collaborate – to share intelligence and influence good practice across cyberspace

**ACTIONS**

1. Use the Cyber Security Strategies report to assess and determine the issues with senior management and cyber stakeholders
2. Obtain support from senior management to consider the opportunities and address the threats of cyberspace
3. Create a Cyber Resilience Group to lead, drive and coordinate all cyber resilience activities
4. Adapt the ISF Cyber Resilience Framework to your organisation and use it to create your vision of cyber resilience; use the diagnostic tool to assess your current resilience, identify gaps, and prioritise your plan
5. Implement your cyber resilience plan, using other ISF deliverables to assist
6. Partner and collaborate with others, including your supply chain and customers, to share intelligence and influence adoption of good practice across cyberspace
Business leaders recognise the enormous benefits of cyberspace and know that cyberspace increases innovation, collaboration, productivity, competitiveness and engagement with customers. Yet they are having difficulty determining the risk versus the reward.

The benefits of cyberspace come with significant risks, and the threat of cyber attack is firmly at the top of the board agenda. While organisations are exploiting the business benefits of cyberspace they may not realise that cyberspace confers the same benefits to those who attack our organisations. Hacker groups, criminal organisations and espionage units worldwide have access to powerful, evolving capabilities, which they use to identify, target, and attack. They even have well-developed marketplaces for buying and selling the tools and expertise used to target and execute attacks.

We call this Malspace.

It is critical that organisations understand Malspace and the increased threat it poses. Organisations should develop a business plan to exploit cyberspace that identifies threats, considers the limitations of IT and information security, and develops cyber resilience.

Based on insights from the Information Security Forum's global Membership and ISF Global Team, the ISF Cyber Resilience Framework identifies the key capabilities that organisations should possess to increase their resilience to the threats from cyberspace.

Cyberspace is critical to most organisations today; disconnecting is not an option. By implementing the ISF Cyber Resilience Framework – supported by the wide range of ISF tools and materials – organisations can develop cyber resilience and be better able to withstand impacts from evolving cyber threats. Only then can organisations safely realise the benefits of cyberspace.