The digital revolution continues apace, with organisations and individuals immersed in the “Information Age”. Today, valuable information is used to compete and succeed in a global market; information assets can represent more than 80%¹ of an organisation’s total value.

Mission-critical information assets – an organisation’s “crown jewels” – are information assets of greatest value and would cause major business impact if compromised. These assets attract the attention of highly motivated, capable and well-funded adversarial threats, such as unscrupulous competitors, nation states and organised criminal groups, all of whom are intent on exploiting this valuable information.

Businesses must prioritise the protection of mission-critical information assets. All too often leaders consider the value of mission-critical information assets but fail to recognise the extent to which these assets are exposed to threats.

Organisations that recognise both the value of, and the risks to, mission-critical information assets will be best positioned to take advantage of the ISF Protection Process to deliver comprehensive, balanced and end-to-end protection.
PROTECTING THE CROWN JEWELS – HOW TO SECURE MISSION-CRITICAL INFORMATION ASSETS

Conventional approaches to deploying security controls seldom provide appropriate or sufficient protection for mission-critical information assets. The ISF Protection Process is a structured and systematic five-phase process for determining the approaches required to deliver comprehensive, balanced and end-to-end protection.

**THE ISF PROTECTION PROCESS**

A **IDENTIFY MISSION-CRITICAL INFORMATION ASSETS**
- Define what constitutes a mission-critical information asset
- Identify potential mission-critical information assets based on their value to the organisation and the potential business impact if compromised
- Maintain a record of approved mission-critical information assets

B **ASSESS THE MAIN ADVERSARIAL THREATS**
- Investigate the main adversarial threats to mission-critical information assets
- Identify threat events likely to be used to target mission-critical information assets
- Evaluate the level of exposure to each mission-critical information asset

C **DETERMINE THE REQUIRED PROTECTION APPROACHES**
- Understand possible approaches for protecting mission-critical information assets
- Define objectives for protecting mission-critical information assets
- Select the required approaches to protect mission-critical information assets
- Identify the security controls and solutions required to support chosen protection approaches

D **COUNTER THE MAIN ADVERSARIAL THREATS**
- Deliver the appropriate extra layers of preventative and detective security controls across the five stages of the cyber attack chain

E **PROTECT THE INFORMATION LIFE CYCLE**
- Apply fundamental, enhanced and specialised controls throughout the information life cycle

**PROTECTION CAPABILITY**

The ISF Protection Process can be used in isolation or embedded into the broader protection capability of an organisation. This capability consists of a range of different supporting elements, typically comprising: governance, risk management and compliance (GRC); people; technology; and security assurance.

GRC
Set direction for security, promote ownership, collaborate with stakeholders.

People
Invest in skilled and experienced IT practitioners, security specialists and risk experts.

Technology
Automate protection of mission-critical information assets using security architecture, specialised technical security controls and advanced security solutions.

Security Assurance
Provide assurance for the protection of mission-critical information assets.

Threat-based protection provides an early warning system to inform of emerging or imminent threat events, enabling a balanced set of end-to-end controls to counter the main adversarial threats.
WHERE NEXT?

The ISF series for Protecting the Crown Jewels enables organisations to protect their mission-critical information assets against highly motivated, capable and well-funded adversarial threats. The series incorporates:

– a main report targeted primarily at CISOs and business leaders, introducing mission-critical information assets, outlining the main adversarial threats and presenting the ISF Protection Process

– an Implementation Guide and other supporting materials targeted at information risk specialists and information security professionals, providing practical steps to implement and embed the ISF Protection Process.

Organisations should give careful consideration to the ISF resources in this series including The Standard of Good Practice for Information Security, Benchmark and IRAM2: The next generation of assessing information risk.

The ISF encourages collaboration on its research and tools. Members are invited to join the vibrant Protecting the Crown Jewels community on ISF Live (https://www.isflive.org/community/risk/protecting-the-crown-jewels) to share their experience and discuss the findings and recommendations presented in this ISF series.

Consultancy services from the ISF provide Members and Non-Members with the opportunity to purchase short-term, professional support activities to supplement the implementation of ISF products including the ISF Protection Process and other resources in this ISF series.

Protecting the Crown Jewels is available free of charge to Members, and can be downloaded from the Member website www.isflive.org. Non-Members interested in purchasing the series should contact Steve Durbin.

CONTACT

For further information contact:

Steve Durbin, Managing Director
US Tel: +1 (347) 767 6772
UK Tel: +44 (0)20 3289 5884
UK Mobile: +44 (0)7785 953 800
Email: steve.durbin@securityforum.org
Web: www.securityforum.org

ABOUT THE ISF

Founded in 1989, the Information Security Forum (ISF) 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 cyber, information security and risk management by 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 programme. The ISF provides a confidential forum and framework, which ensures that Members adopt leading-edge information security strategies and solutions. And by working together, Members avoid the major expenditure required to reach the same goals on their own.

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.