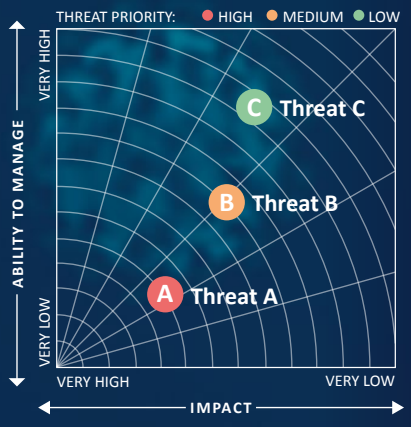
Top Tips to Prepare for Cyber Threats in the COVID-19 Era

The ISF ***Threat Radar*** is a visual aid created to accompany the Threat Horizon reports that can be leveraged by organisations to assess the impact of COVID-19 on the threat landscape.

These ISF tips can help you to make the best use of the ISF ***Threat Radar***.

For support creating a customised Threat Horizon scenario for your organisation, please get in touch.



ALIGN STRATEGY WITH THREAT FORECASTING

Carry out a review of your organisation's business continuity and crisis management plans, ensuring they account for the new and emerging threats introduced by COVID-19. The ISF ***Threat Radar*** can be used to develop a coherent and resilient approach to information security.

EVALUATE THREAT PREDICTIONS

In the COVID-19 era, some threats may take on added importance. Review your existing threat forecast and determine its continued applicability to your organisation. You may wish to revisit previous ISF ***Threat Horizon*** reports to assist during this process.

IDENTIFY ADDITIONAL THREATS

Use the ***Threat Horizon's PESTLE model*** to evaluate the new threat landscape in relation to political, economic, social, technological, legal and environmental factors that may be driven or influenced by the current COVID-19 pandemic.

RECORD RELEVANT THREATS

Use the ISF ***Threat Radar*** to plot the impact of threats related to COVID-19 and your organisation's ability to manage each threat appropriately. Create a continuous process for the evaluation of threats plotted on your Radar.

MANAGE AND PROTECT CROWN JEWELS

Identify and record mission critical information assets that are exposed to the threats presented on the ***Threat Radar***. Gain a clear understanding of the techniques and methods likely to be used by adversarial threats against these assets to determine their level of exposure and the appropriate security controls.

ENGAGE WITH STAKEHOLDERS

Use the ***Threat Radar*** as a visualiser to facilitate discussion with business leaders around threats introduced by COVID-19 and the potential risks they pose to your organisation's information security. Validate identified threats with relevant parties – this may involve developing, modifying or removing threats from the Radar. You may also need to rethink and adapt some of your security policies.

PREPARE TO ADDRESS EMERGING THREATS

Develop and implement remediation plans for each threat, identifying changes required to controls, infrastructure and architecture in your organisation. Assign responsibilities to named individuals, set target dates for specific actions and align these actions with your existing risk management structures and frameworks.

PRIORITISE PLANS FOR REMEDIATION

Assess and prioritise all threats leveraging your organisation's existing risk management tools and methodologies. Set the budget needed to remediate threats and gain business buy-in for information security investments

TEST BUSINESS CONTINUITY AND CRISIS MANAGEMENT PROCEDURES

Implement threat simulation exercises to gauge the preparedness of the workforce and security systems to handle new and emerging threats that stem from the COVID-19 pandemic. Adjust organisational strategies and remediation plans to improve threat resilience.

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. Find out more at **www.securityforum.org**

Information Security Forum
@SecurityForum
info@securityforum.org

FIND OUT MORE

Discover more useful resources at **www.securityforum.org/covid-19/**

REFERENCE: ISF 20 03 04