procorre®

Cyber Interference Risk Score

Cyber Interference Risk Score

Using cyber interference with business processes to steal critical information is now the largest criminal enterprise globally. The threat to your business is financial, reputational, loss of customers and compliance with significant fines possible for breaches where negligence, late reporting and poor management can be proven. This Cyber Interference Risk Score report outlines where the particular risks for businesses are from the cyber world.

Risk Levels Defined

Hazards, Dangers, Extreme Risk:

- Likely loss of business revenue, profits or customers.
- Likely theft of critical data, financial, partner or customer information.
- Requires immediate action
- Requires Board And/ Or Senior management involvement
- May require immediate reporting.

Threats, Attacks, Business Risk:

- Potential loss of business revenue, profits of customers.
- Possible theft of critical data, financial, Partner or customer information.
- Requires Immediate investigation
- May require board or senior management engagement
- May require reporting

Warnings and Advisories:

- Potential business impact on revenue, profits or customers
- Indicates increased negative activities in the region or market that could lead to a threat
- Does not require immediate action
- Maintain and check cybersecurity, staff and partner awareness of risks.



Procorre, 24 International House, Holborn Viaduct, London, EC1A 2BN
+44 2034 320 480

Not All Changes Are Bad

There are three reasons that your score will change:

1. If you launched a marketing or advertising campaign, which includes advertising for staff, blog posts, LinkedIn, Instagram, Twitter, Facebook (or similar) articles, comments or likes; this will likely register a change in score.

2. If you are in the news which creates media, internet or social media interests, this will likely register a change in score. The broader the coverage, the greater the change in score will be.

3. However, if the score changes when you have not changed advertising or marketing, Or have not been in the news, i.e. for unknown reasons you have likely become an organisation of interest to the wrong people and should increase your diligence and prepare for a cyber attack.

Note: if your score is significantly higher than the regional or industry averages scores and you are not the market leader (or 1 or 2 of the above), you have become interesting to the wrong external parties.



Procorre, 24 International House, Holborn Viaduct, London, EC1A 2BN

+44 2034 320 480

Cyber Interference Risk Score Defined

Your Cyber Interference Risk Score (CIRS) is in three parts – Your CIRS score (Number), your Dark Web Risk Scale, (DRS) and also your Partner/Supplier Risk Scale (PRS)

CIRS – The CIRS is the total of indicated risks from an external interest in your activity by region, market and industry sector. The score is assessed over up to one year through monitoring external interest in your organisation and your activities from the internet, news and social media, and the dark web. Dark scope's CIRS uses a scale from 1-100 for businesses with local presence only and a score from 101- 1000 for businesses which are trading globally.

DRS - The DRS is the activity level in the dark web related to your organisation. The DRS contributes to your CIRS but is shown as a stand-alone scale as the dark web hosts market place for stolen data, hacking for hire, ransomware and other tools that are used to breach a target. If your profile is high in the dark web, your risk of an attack or hack is significantly higher.

PRS - The PRS is risk based on the activity and behaviour of your named partners and suppliers 'Key Counterparty Networks Of Trust', Such as partners and supplier that have direct access to your systems, have become a growing cyber risk. Knowing what risk your partners represent is vital to your cybersecurity. Each partner is CIRS rated, and the average of their scores provides the PRS result. Where a partner presents a high or extreme risk, this is included in the identified risk section of this report.



What The Bad Guys Are Interested In

The Internet:

News articles

Financial reports

Key staff activities

Staff Changes

Advertising & marketing

Third party engagement

Customer & Supplier Listings

The Dark Web:

Previous Compromises

Customer Information

Hacks, Emails & Passwords

Exploitable Staff Behaviour

IP, Trade Secrets & Know – How

Credit Card & Bank Card For Sale

Ransomware, APT's & Other Tools

The Deep Web:

SaaS Usage

Cloud Storage Use

Poor Access Control

Poor Staff Passwords and Behaviour

Weak BYOD Management & Usage

Weak Privileged Access Management (PAM)

Social Media

Key Staff, Their Families & Close Friends

Weak Password And Access Management

Disclosure Of Sensitive Information

Outlier & Disgruntled Staff

Exploitable Staff Behaviour

Disgruntled Customers.