ABOUT DARKSCOPE

Darkscope is focused on delivering superior cyber intelligence to clients about nefarious activities being planned against them in the deepweb and darknet. Today's cyberattacks are sophisticated, well researched and planned. They are more complex, better delivered and are more attuned to the market than ever. They will continue to develop at a faster rate and be delivered more professionally than ever before. Being unaware of these risk puts an organisation at heightened risk. Not knowing, or not caring, is not a valid option anymore.

Darkscope delivers new tools that help our clients to be prepared for any attack before it is delivered, by looking in the places the attacks are created. Darkscope has a range of solutions that deliver improved cybersecurity for our clients. These include Cyber Interference Risk Score ™, Cyber Risk Assessment™, Cyber Watchtower™, Impersonate Protection.

PARTNER & SUPPLYCHAIN PROTECTION

For many enterprise businesses, partner & suppliers are their biggest risk of being attacked through. Darkscope measures the Cyber Risk for each partner or supplier and identifies 'weak' links and provides data to determine and recommendations to minimise the cyber risk.

CYBER WATCHTOWER

Using our networks in the deepweb and darknet and our state of the art artificial deep neural networks, Cyber Watchtower provides strategic threat intelligence ahead of any attack, phishing or hacking attempt to an organisation.

CYBER INTERFERENCE RISK SCORE

Instead of assessing your capability to protect against risk, the Darkscope Cyber Interference Risk Score looks for the risks you need to defend against.

IMPERSONATE PROTECTION

In any business, key personnel are most vulnerable for targeted attacks. Darkscope's Watchtower uses its DANN (Darkscope Artificial Neural Network) to detect and identify content in the Dark web, Internet, and social media which relates to your key personnel.

DARKSCOPE
THE CYBER WATCHTOWER

CIQ360
THE CYBER RISK RATING SERVICE™

DARKSCOPE INTERNATIONAL LTD.
WWW.DARKSCOPE.COM

WHAT IT DELIVERS

Combing the three elements, the 360R, P2P and DWRS, delivers a snapshot of the external cyber risk your client is exposed to. With this information you can determine how to handle this client for cyber risk insurance.

HOW THIS IS DELIVERED

Combing the three elements, the 360R, P2P and DWRS, delivers a snapshot of the external cyber risk your client is exposed to. With this information you can determine how to handle this client for cyber risk insurance.


CIQ360

CIQ360 Report

Report Summary

Results at a Glance

THE RESULT

The CIQ360 Report is a five-page report delivering the outcome of the CIQ360 investigation of your client's potential risk in cyberspace.
At a glance you can see the three metrics in graphic form that summarise your client's cyber risk profile. The other pages of report explain how to interpret these results and the factors that may affect the result for a client based on their market standing, marketing, sales, news and media activity.

FACTORS AFFECTING RESULTS

To fully understand the result, you must also understand your client. Their result is affected by three key factors:
1. Market standing. If they are a market leader, their higher profile will result in a higher score
2. Marketing activity. If they have launched an advertising or sales campaign or are very active in social media.
3. News. If they are in news which creates media, internet or social media interest, this will create higher scores.

WHY YOU NEED THIS REPORT

The global cybersecurity insurance market is forecast to grow at over 25% annually from 2018 to 2023 when it is forecast to reach US$17.55 billion.
Most tools offered to insurers that measure cyber risk, do so by assessing the clients network defensive capability. While such assessments are useful for the client, they do not help the insurer to assess whether the client is at risk from a cyberattack.
Here's why...
75% of the root cause of a data breach is either malicious or criminal attack (48%) or human error (27%) meaning that a tool that assesses their network security is only looking at a minor part of their cyber risk exposure.
More importantly 70% of the cyber risk that a client faces is external and outside of their control. Of the 30% internal risk, 90% of this is staff behaviour. So, measuring network resilience will tell you very little about your client's cyber risk profile.

Informed Decision

The CIQ360 report gives you the information about the risk profile of your client from outside their business where their real cyber risk is. This information lets you make an informed decision based

Understanding the exposure of providing cyber risk insurance to a business makes good sense.
Now you can know what your risk is before you sign them as a client.

PURPOSE

CIQ360™ is the cyber risk insurance rating service designed for insurers assessing a potential client for cyber risk insurance.
Better than any actuarial calculation or guess, CIQ360 calculates risk by scanning the same external domains that "the bad guys" use to assess whether the business is a worthwhile target.
CIQ360 rates your client's cyber risk in cyberspace. Cyberspace is three domains: the internet, social media and the darkweb. By scanning a full circle (360°) around them, CIQ360 can measure activity that shows if there is external malicious interest in your client that would make them a greater risk to you when you provide cyber risk insurance.
The result is reported in three parts which shows you the current external cyber risk for your client. You can now know if they represent a high, medium or low risk, and therefore whether they are likely to cost or make you money if you sell them cyber risk insurance.
"No touch"
ethical engagement
CIQ360 works in cyberspace, a world outside of the control of your clients. It does not need access to the client's offices, network or data. As the information being used is in the public domain, and is not owned or managed by the client, CIQ360 does not need their permission to create this report. CIQ360 uses ethical processes and techniques to generate a rating and does not breach any laws to deliver this service.

HOW IT WORKS

CIQ360 works in three parts.

1. It scans cyberspace – the internet, social media and the darkweb – for activity focused on your client. It then rates the scan results using trained Artificial Intelligence. By using AI, CIQ360 can distinguish between normal business activity and malevolent interest in your client from the wrong people. Where this type of interest exists, your client is at higher risk from a cyber-attack, hack, phishing attack, ransomware, crypo-jacking or other form of breach; or may have already been compromised. This step delivers the CIQ360 rating for your client (360R).

2. By using the same process to rate 1000's of similar businesses, CIQ360 has already created a baseline result that your client can be compared against. Peer-to-peer comparison within the same industrial sector and region is more useful than comparing your client against all industries and regions globally. This peer comparison accounts for the specific market that your client is engaged in. This step delivers a Peer-to-Peer comparison rate (P2P).

3. A special AI search of the darkweb focused on your client is run. Most businesses do not engage or work in the darkweb, so heightened activity in this domain is an indicator that your client is at risk from the wrong sort of interest from the wrong people. This step delivers the Darkweb Risk Scale (DWRS).