The Importance Of Digital Risk Protection In Your Cybersecurity Strategy

Cyberint

Digital Risk Protection solutions ("DRP") make up a vital part of every organizations' cybersecurity strategy. DRP provides security leaders and security teams with the ability to implement powerful tools and integrate it into the organization's cybersecurity strategy. It allows every threat researcher and security analyst the ability to identify and address any existing cyber risk exposures as quickly as possible.

DRP solutions can provide valuable assessments that focus on the short-term outcomes of an organization, while also planning for the long term. For this reason, these new tools aid in developing accurate strategies that can be used to fight against attack surface activities and malicious entities while improving the cybersecurity of an organization.

WHAT IS DIGITAL RISK PROTECTION?

Digital Risk Protection is classified as a proactive defensive strategy used by organizations to pursue counter threats, improve efficiency, avoid unnecessary costs, and recover lost revenue. Digital Risk Protection is known to provide a significant return on investment. For this reason compliance and risk officers, IT security departments, marketing and brand leads and the C-suite will find DRP very useful.

Learn how Cyberint implements Digital Risk Protection here

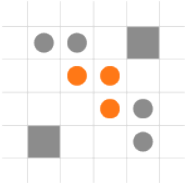
THE BASICS OF DIGITAL RISK PROTECTION

The right Digital Risk Protection tools are used to leverage and control every threat intelligence as a method of identifying stolen credentials, vulnerabilities and phishing attacks. Digital Risk Protection solutions have various strengths, including coverage of extensive Deep and Dark Web capabilities to potential threats from social media.

When taking a deep dive into the mechanisms of the right DRP tools, these are used to empower security analysts and threat researchers to conduct the following:

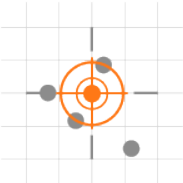
BRAND AND SOCIAL MEDIA PROTECTION

The right DRP solution is used to discover malicious entities that are impersonating the respective brand and targeting these executives of the company both on social media and across the web.



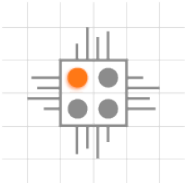
DIGITAL FOOTPRINTING

Every threat intelligence incorporated into the systems of DRP tools is used to determine which assets actually belong to the organization and which are impersonating the organization.



THREAT LANDSCAPING AND HUNTING

DRP tools help identify active campaigns that are against the respective organization or the industry that the organization operates in. remediation, and alerting workflows as a means of quickly and effectively mitigating attack surface threats.



CYBER EXPOSURE MITIGATION

DRP tools process threat intelligence items and embeds actionable data (and resources), remediation, and alerting workflows as a means of quickly and effectively mitigating attack surface threats.

FACILITATING THE DIGITAL TRANSFORMATION JOURNEY

There are a variety of reasons why a Digital Risk Protection solution can help an enterprise during it's digital transformation journey. The main benefit is that it will aid in improving the migration to the cloud and SaaS based applications by ongoing monitoring of all digital assets. It provides visibility and an essential layer of required security.

RISK MITIGATION

The investment in a solution needs to be seen within the specific context of unwanted costs that a security breach is going to generate. This is like the majority of other elements within a general cybersecurity strategy. These unwanted expenses are valuable but not THE most valuable feature of Digital Risk Protection (DRP) solution.

Instead, the most valuable feature of implementing good Digital Risk Protection services is the insights provided in the organization's digital footprint. This is an exceptionally vital component to establish the actions required to protect the business, as well as the business's reputation, from such risk.

BETTER COVERAGE AND MONITORING

Digital Risk Protection services offer the ability to automate several tasks that involve monitoring, identifying, as well as resolving digital threats that are organizations face. This is provided around the clock. DIY cybersecurity and on-premise off-the-shelf measures are known to only offer half-decent coverage of these monitoring, identifying, and resolving activities. When compared with purpose-built and continuously updating solutions, which are delivered as a fully-functioning service, they come up short.

The most effective Digital Risk Protection solutions are also equipped to cover Shadow IT. These are unauthorized devices, apps, and domains that are being developed or utilized without informing the respective IT department. Included in this coverage offered by the best digital risks protection services is Forgotten IT, which is archived content and old website landing pages.

This service is incredibly important with some instances of malicious activity resulting in businesses spending an average of $141,000 for damage and recovery. In fact, according to the FBI, malicious cyber activity accounts for more than $3.5 billion in losses.

INCREASED EFFICIENCY

The automation incorporated into the systems of Digital Risk Protection services aids in identifying vulnerabilities quicker and easier. Thus, increasing efficiency. The identification and elimination of Forgotten IT and Shadow IT also aids in streamlining the organization's digital footprint and saves on the resources and data needed to maintain and host these risks protection.

Reporting being easy to read, simple to digest and quick to act on increases efficiency significantly too, enabling fast and effective mitigation of threats.

RECOVERED REVENUE

Successful cyber attacks on a company have an immediate effect that negatively impacts organizational revenue. Successful cyber attacks, online websites seeking stolen or counterfeit goods, and phishing websites also have a strong negative impact on corporate revenue.

All of these threats have an adverse effect on the brand's reputation. As a result, this reputation can end up driving potential customers to alternative vendors that have a better reputation. However, effective Digital Risk Protection solutions are known to help mitigate these new risks to the revenue of a company by identifying and eliminating chances of a possible attack or surface activities. Thus, aiding in recovering revenue.

ONGOING DISCOVERY OF THE DIGITAL FOOTPRINT

The majority of enterprises are going to have an investment in the digital sphere, which brings many advantages such as profit, collaboration, speed and more..

However, these advantages can only be received when the new risks associated with such investments are effectively managed.

Each connection, technology, or application increases the complexity of such investments as the data and resources are stored in multiple places. Thus, the supply chain that's providing these services or accesses this information is far larger. As a result, the weaknesses in legacy technologies make this digital world incredibly difficult to protect. In addition to this, the relevance to the company imperatives like communicating with customers is negatively affected.

Moreover, these digital footprints incorporated into this digital network are exceptionally vast and forever growing. The reason for this is because of more technologies, along with third parties forming a complex ecosystem.

Due to this, it becomes increasingly challenging to comprehend the growing attack surface, measure the critical data's ephemeral loss, effectively manage the Shadow IT, as well as understanding the integrity associated with the organization's identity. When looking at all of these components, the chances of exposure to weaknesses in this organization's growing footprint are increased drastically.

HOW CAN DIGITAL RISK PROTECTION HELP GAIN ADDITIONAL CONTEXT AND VISIBILITY?

When implementing effective Digital Risk Protection solutions, the main objectives are to ensure that these tools aid in reducing exposure and driving mediation, along with focusing on strategic security attack surface preventatives. The goal of implementing such strategies is to provide short-term exposure mitigation data, resources, and insights, which also provides a proactive and long-term performance management context.

When these Digital Risk Protection solutions are specifically developed and customized to the exact needs of the organization, security teams and leaders get help in understanding the overall performance of the organization over time. They also gain the ability to effectively allocate limited resources (and data) and make risk-based program decisions that are entirely based on the accurate security ratings developed from such strategies. These security ratings can be classified as an objective and verifiable measurement of the organization's security performance.

Here are some of the very crucial ways that proper implementation of Digital Risk Protection solutions can offer additional context and visibility to organizations as a method of making more informed and strategic security decisions:

- **GAINING THE ABILITY TO GO BEYOND POINT-IN-TIME ASSESSMENTS**

  Continuous monitoring provides a way of identifying gaps within the cybersecurity controls, which can be conducted across 75 business risks. Thus, providing you with the ability to see how your security posture changes over time.

- **AIDS IN FACILITATING DATA-DRIVEN SECURITY CONVERSATIONS WITH STAKEHOLDERS**

  Organizations that implement Digital Risk Protection solutions that incorporate standardized KPI, which is based on objective, independent, and broadly accepted information, can effectively report on the effectiveness of the specific program in clear and easily digestible methods to board members, cyber insurers, regulators, and customers.

- **FORECASTING FUTURE PERFORMANCE**

  You get the opportunity to create action plans, develop model scenarios, track progress as a method of identifying paths to reduce cyber risk, and better allocate the organization's resources and data.

- **BENCHMARK YOUR PROGRAM AGAINST YOUR INDUSTRY PEERS**

  Your organization is able to get unprecedented visibility into the relative performance of your peers. Thus you're able to make informed and comparative decisions about where your business should focus its efforts as a way to achieve continuous improvement. In addition to this, an organization's security teams and leaders can also get insights into how to meet or surpass the benchmarks and standards of care within the respective industry.

WHY SHOULD YOU USE DIGITAL RISK PROTECTION RESOURCES AND SERVICES FOR YOUR COMPANY?

Digital risk is evident in all spaces of the internet, especially the dark web. With that being said, there has been a major acceleration of digital transformation due to the shift to work-from-home working conditions. From this, security teams have been left to play catch up as the use of old security tools have become redundant against fighting evolving digital threats.

This remote work and digital transformation have resulted in the hurried adoption, along with the reliance on Digital Risk Protection solutions. The leverage of full power digital transformation aids in minimizing this digital risk. DRP will help facilitate the Digital Transformation journey by mitigating numerous business and cyber risks faced by the organization.

This digital risk can spread to the organization's brand being tarnished as a result of threats across social media and app stores infiltration and impersonation. These solutions developed for Digital Risk Protection aid in monitoring (in real-time) these social media channels for new digital risks. Thus, providing social media protection for brand attack, surface and account takeover. Security leaders and security teams need the best tools to fight against malicious entities trying to steal these company's data and resources.

In addition to this, anti-invasion techniques that are incorporated into Digital Risk Protection strategies are used to detect malicious content, like posts, which can aid in dismantling the malicious attackers' infrastructure. This malicious content can include social media phishing scams (materialized as social media posts), account takeovers, digital asset impersonation, along with many others.

These Digital Risk Protection services are provided to go further than monitoring the surface for threats to the digital intelligence of a platform or platforms. In addition, these services incorporated adopt advanced technology as a method of protecting the data and intelligence of an organization by offering constant monitoring, identifying, and mitigation of any threats to the intelligence and data of a company.

There are new public attack surface activities and risks that are forever growing and changing. For this reason, there are always going to be new threats to platforms. After identifying and mitigating one threat, a new threat is going to come into view. It's for this reason that you integrate services that are going to provide constant monitoring, identifying, and mitigating any possible new threats on a platform or various platforms.

These Digital Risk Protection services also incorporate new and expert-curated intelligence into the systems of a platform to fight against these risks. These expert intelligence services are used to get a leg-up against phishing websites and other phishing attacks and protect web platforms and enterprises against these public phishing attacks. Not only can these be put into use for the sake of the company and its digital platform, but it can also be put into use for the sake of the customers of the respective company.

In addition to this, the response process of identifying these threats through the Digital Risk Protection process measures to aid in reducing the new risks of these data threats, as well as the lifespan of these threats. While these threats are being mitigated, the security workload of controlling this data is also reduced.

Meanwhile, the visibility of the company's performance is also enhanced. These particular Digital Risk Protection process measures are put into place, which aids in developing comprehensive visibility. This visibility is due to the large amounts of data that are being collected across different components within the company's infrastructure and resources. Not to mention, the effective threat intelligence that's delivered helps to minimize the need for additional review and analysis of the company's resources and data.

FINDING THE RIGHT SOLUTION FOR YOUR BUSINESS

When evaluating the various Digital Risk Protection offerings, the security leaders and security teams making up an organization should ensure that they choose the right solution based on the business's scale, size, and specific needs.

An enterprise that's made up of thousands of sensitive digital assets that are scattered around the globe are going to benefit from a complete Digital Risk Protection solution that's equipped to offer extensive Digital Asset Management abilities and useful public and confidential web data. As a result of this, these organizations are then given the use of Security Policy Model (SPM) to get the context, as well as visibility into the performance of this specific tool.

A FULL DIGITAL RISK PROTECTION SOLUTION INCLUDES:

- DIGITAL ASSET MANAGEMENT INCLUDING:
  - Brand protection including phishing detection- detecting malicious entities impersonating the brand and targeting these executives of the company.
  - Threat Intelligence is used to determine which assets belong to the organization and which are impersonating the organization.
  - Data Leakage detection It feels like leaked credential dumps are ever increasing and growing in size each time. With an extensive digital risk protection program in place these are identified and acted against swiftly. See how data leakage is prevented here.
- 3rd Party Cyber Risk - It's not only important to protect your own brand from threat actors. If you're using suppliers, and virtually every business is, 3rd party cyber risk management is crucial.
- Threat landscaping and hunting - to detect and identify malicious campaigns against the brand themselves or against the industry the brand operates in. One method of doing this digital risk surface monitoring.
- Fraud prevention - acting against gift card cloning and similar activities. See how it's fraud is prevented here.
- Cyber exposure mitigation - every threat intelligence into the system in an extensive Digital Risk Protection solution must provide actionable data (and resources), remediation, and alerting workflows as a means of quickly and effectively mitigating attack surface threats.

With that being said not every organizations that implement a DRP solution will benefit from all the robust risk protection capabilities immediately.

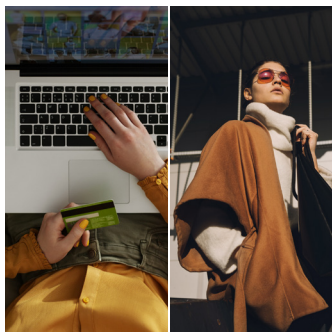
In cases like this, organizations can benefit from Threat Intelligence provided to get accurate context and visibility into malware infections, leaked credentials and vulnerabilities impacting them threat intelligence still provides the organization with the ability to get accurate context and visibility into the vital infections and vulnerabilities that are impacting the organization. This includes those that aren't being detected from other types of tools. You're also provided with the ability to get insights to help improve performance and resolve key business challenges. A partial solution could include any one or a combination of the aforementioned digital risk components.

USE CASES

FULL DIGITAL RISK PROTECTION

DIGITAL RISK PROTECTION IN PLAY AT A KEY GLOBAL RETAIL ORGANIZATION

The following is an example of an organization that chose to use our partial Digital Risk Protection solution. Cyberint helped a large U.S. retailer boost its Cyber Threat Intelligence (CTI) capacity. Our team of expert cyber analysts combined with Argos™, our proprietary threat intelligence platform worked closely with their in-house CTI team



Large U.S. Retailer's in-house CTI Program

Boosted with Best-in-class Managed Intelligence Suite

Cyberint

Cybering ensured the Retailer identified threats prior to them becoming problematic and allowed the cyber analysts to investigate, contextualize, and prioritize alerts. This led to an effective cyber threat mitigation program.
See the full threat intelligence story here.

DIGITAL RISK PROTECTION DIGITAL ASSET MANAGEMENT

CyberInt Researchers and Check Point worked together to help EA Secure its 300 million gamers. They disclosed vulnerabilities in EA's subdomain management, whilst also protecting against brand impersonation and phishing threats.
See more here.

THE IMPORTANCE OF CYBERINT AS A DRP VENDOR

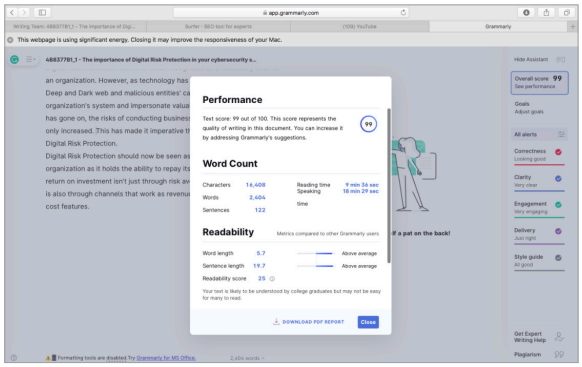
Cyberint has the ability to offer exceptional Digital Risk Protection to all businesses, big or small. Cyberint is a reccomended solution by all key analyst firms including Gartner and Forrester. Cyberint's DRP Managed Detection and Response facilities offer services that span over a global platform. We provide these services to allow our clients the ability to combat and respond to all advanced cyber threats that generally go unnoticed when using standard security controls. Taking out these advanced cyber services aids in protecting the business's brand, customers, and digital assets.

Cyberint's unique approach combines human intelligence (our in-house CTI team) and our Argos Edge™ platform to provide a complete and encompassing Digital Risk Protection solution. We also have a self service option allowing users to monitor and manage their own cybersecurity. See the full details of our approach here.

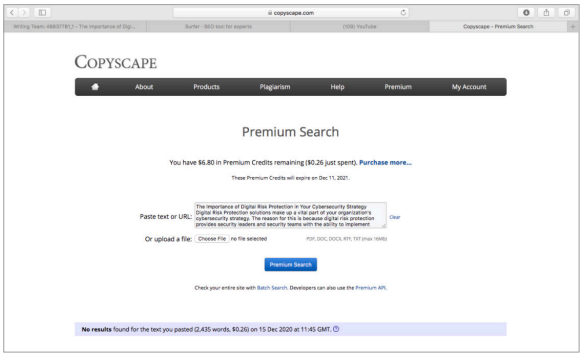
> ***Working very closely with the Cyberint team, I am able to use data from the Argos Edge™ platform to add insights to our management meetings. This highlights our value to not only senior management but the rest of the company to adhere to high standards of security and data privacy necessary for governance and compliance.***
>
> *Mark Frogoso, CISO at GCash*

THE BOTTOM LINE

Digital Risk Protection (DRP) has never been recognized as a necessary cost for an organization. However, as technology has been advancing, so has the Deep and Dark web and malicious entities' capabilities to invade an organization's system, public and confidential web data, and impersonate valuable digital assets. As time has gone on, the new risks of conducting business in the digital sphere have only increased because of such an invasion of public and confidential data. This has made it imperative that organizations invest in Digital Risk Protection as a way to protect against such attacks.



Digital Risk Protection should now be seen as an investment to any organization as it holds the ability to repay itself several times over. This return on investment isn't just gained through risk avoidance and elimination of the company's stored public and confidential data. It is also provided through channels that work as revenue protection and proactive cost features. That's why the expert use of Digital Risk Protection is useful to protect the company's stored public and confidential data from cyber attacks and get revenue recovering resources.



CONTACT US

www.cyberint.com | sales@cyberint.com | blog.cyberint.com

USA
214 W 29th St
New York, 10001
Tel: +1-646-568-7813

Israel
17 Ha-Mefalsim St
4951447 Petah Tikva
Tel: +972-37-286-777

United Kingdom
6 The Broadway, Mill Hill
NW7 3LL, London
Tel: +44-203-514-1515

France
67 Avenue de Wagram
75008 Paris
+33 1 77 50 58 91

Singapore
135 Cecil St. #10-01
MYP PLAZA 069536
Tel: +65-3163-5760