



DIGITAL RISK PROTECTION:

**WHY INTUITIVE CROSS-PLATFORM
MONITORING IS THE NEW STANDARD**



TABLE OF CONTENTS

Introduction 3

Background: Digital Risk Protection 4

How Digital Risk Protection Is Changing..... 6

Addressing Gaps in Digital Risk Protection 8

Conclusion..... 10

INTRODUCTION

Some of the most damaging threats to any business now originate from online spaces, including social media, the searchable web, and more hidden deep and dark web networks. These threats largely target an organization's data—but also impact brand image, customer trust, and even threaten physical assets and personnel in real-world environments.

In 2019, a compromise of fewer than 100,000 records cost businesses \$3.86M on average.¹ Organizations with over 5,000 employees are also likely to experience, on average, one crisis per year—which PwC defines as “a major disruption to multiple functions of the enterprise” that causes significant fiscal and reputational damage.² While costly crises often involve cybercrime, they can also involve damaging viral content, as well as physical threats like terrorism and workplace violence that can be detected online.

The open, deep, and dark web provide timely information for organizations to strategically understand, detect, mitigate, and even predict such online business risks. Digital risk protection (DRP) solutions enable organizations to access relevant information across these sources quickly and effectively. This ultimately saves significant financial, reputational, and operational damage.

While costly crises often involve cybercrime, they can also involve damaging viral content, as well as physical threats like terrorism and workplace violence that can be detected online.

However, DRP solutions make up a relatively emerging market beyond traditional threat intelligence tools, despite their rapidly growing demand.³ This leaves much room for improvement on current offerings to meet requirements across multiple corporate verticals.

Where are there gaps in current DRP offerings, and what should enterprise security teams look for in a DRP platform?

¹ IBM Security, “Cost of a Data Breach Report 2020,” sourced August 6, 2020, page 5.

² PwC, “Crisis Preparedness as the next competitive advantage: Learning from 4,500 crises - PwC's Global Crisis Survey 2019,” sourced August 6, 2020, page 5.

³ Markets and Markets, “Risk Analytics Market worth \$45.9 billion by 2024,” July 2, 2019, <https://www.marketsandmarkets.com/PressReleases/risk-analytics.asp>

BACKGROUND: DIGITAL RISK PROTECTION

DRP solutions enable organizations to uncover threats to their digital assets and brand on the open, deep, and dark web. They are specifically meant to reduce negative business impacts, enabling users to easily identify and mitigate online threats. This differs from traditional threat intelligence services, which focus on integration and analysis of threat data feeds, often for highly technical users.

Demand for DRP solutions has increased due to digital footprint growth across a variety of sectors. This has expanded digital attack surfaces as more organizations adopt multiple third-party data storage solutions, a variety of hardware (like IoT and mobile devices) to support operations, and wide social media use.

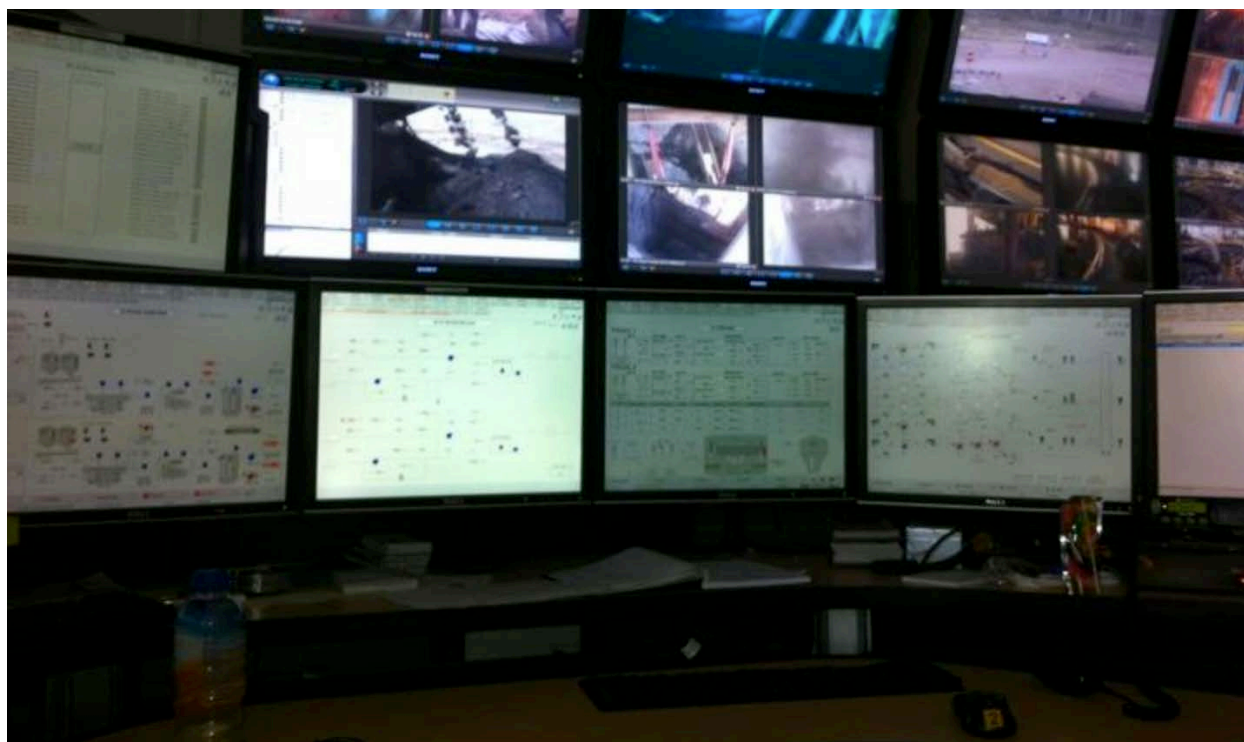
To locate and assess risks to an organization's digital footprint, DRP solutions search the open, deep, and dark web for:

- **Data breach indicators.** This could include corporate email addresses, PII, and other confidential information on paste sites, social media platforms, deep and dark web forums, marketplaces, and publicly-available data breach repositories. These could apply directly to the organization as well as any contracted service providers.

Targeted financial data breach posted to a paste site: "Your financial website's security is flawed"—discovered by Echosec Systems



- **Brand impersonation, counterfeiting, and phishing.** While these threats could include fake social media accounts or websites, organizations can also use social media to find customer alerts for phishing attacks and other scams. The dark web hosts how-to discussions for carrying out impersonation strategies, and tools, such as scampages or phishing malware, for sale.
- **Internal threats.** Current and former employees sometimes post compromising information on mainstream and more obscure, anonymized social networks. This could include unintentional information leaks, like publicly posting a photo from within a control room. It could also include more malicious content, such as employees revealing attempts at internal fraud, participating in workplace harassment, or sharing sensitive company information.



Example of internal workplace information leaked on social media from security operations centre staff—discovered by Echosec Systems

- **Targeted attacks.** Adversaries and extremists often use social media and the deep and dark web to plan or post threats targeting organizations and their executives. This often occurs in the form of a dox, cyberattack, fraud scheme, or targeted physical threat.
- **Negative brand sentiment and PR risks.** Social media, news, and blogs are often the first sources of negative public response to a marketing campaign, event, data breach, or crisis response involving an organization. This content can easily escalate into a costly PR disaster if it's not detected and handled early on.

HOW DIGITAL RISK PROTECTION IS CHANGING

DRP requirements are quickly evolving as these risks become widespread across most sectors. To start, there is a persistent security analyst shortage.⁴ This is impacting organizations' ability to keep up with online data volumes and gather, contextualize, and triage results.

This shortage is symptomatic of a recent security industry transition—the shift between handling digital threats as a technical risk to handling them as business risks. As such, organizations must invest more in their DRP strategies and in-house solutions with features that mitigate security skills and staffing shortages.

Because digital risks are originating in a wider variety of online spaces, organizations also require DRP solutions that prioritize data diversity across open, deep, and dark web sources. However, many existing market solutions are siloed in their data access, specializing in either social media, unindexed online spaces, or more technical feeds. This differs from combining access within a single tool and allowing users to pivot seamlessly between different online spaces. Reconciling many specialized tools or searching networks manually is clunky and risks overlooking critical data on more inconspicuous sources.

⁴ Information Systems Security Association International, "Cyber Security Skills shortage Worsening for 3rd Year In A Row, Sounding the Alarm for Business Leaders," May 9, 2019, <https://www.issa.org/cyber-security-skills-shortage-worsening-for-3rd-year-in-a-row-sounding-the-alarm-for-business-leaders/>

Additionally, the online threat landscape is seeing more frequent turnover of social, deep, and dark web sources as nefarious websites are taken down or social media sources tighten their content policies. From a business risk perspective, security teams must stay current with more obscure or fringe sources that are not offered by most commercial DRP solutions but may host critical information in the event of a targeted threat.

The range of digital risks described above point to another shift: technical security personnel aren't the only business areas served by DRP solutions. Marketing, PR, HR, compliance, and executive protection teams, for example, also require these tools to detect external threats online and better inform their strategies.

Many existing DRP services are focused on a more technical impact, security-focused user base, and don't necessarily appeal to these other enterprise positions and their need for usability and business risk objectives. Traditional security and threat intelligence tooling has also been focused primarily on empowering individual users rather than enabling cross-enterprise collaboration and avoiding organizational silos.



ADDRESSING GAPS IN DIGITAL RISK PROTECTION

To meet security requirements in the current digital risk landscape, organizations must seek out DRP solutions that:

- **Allow for automated, real-time alerting and threat categorization.** Automated alerts and machine learning capabilities allow organizations to address security skills shortages. These features help reduce the time and human resources required to continuously scan multiple areas of the web for potential threats. They also help quickly separate and categorize real business risks from noise and false positives.
- **Deliver a wide variety of sources.** Robust security strategies never rely on a silver bullet tool. However, tools that aggregate content from a wider range of data sources rather than focusing only on social media or dark web, for example, allow for ease of use and more comprehensive protection. In a DRP platform, this looks like crawling a variety of social media, deep, and dark web sources, and a vendor who continuously pursues new sources relevant to the online threat landscape.
- **Are intuitive and user-friendly.** Since DRP is no longer delegated strictly to technical security personnel, solutions must be usable without sacrificing the details required for traditional cybersecurity objectives. Features and functionality should be designed to meet user requirements in multiple business areas—from risk and compliance to marketing.

LEVERAGING DATA DIVERSITY FOR EARLY BREACH DETECTION

In April 2020, thousands of global health organizations' emails and passwords were posted online by an unknown source. While the World Health Organization, who was implicated in the leak, claims that only 457 of the WHO accounts posted were active, this information put the organization's digital security at risk and was leveraged to spread disinformation about the COVID-19 pandemic.⁵

The credentials originated on the text-sharing site Pastebin and were also posted on 4chan, Twitter, and Telegram. In this event, a DRP solution with active asset monitoring features across a variety of social, deep, and dark websites would have detected breach indicators like email handles early on. Such data source diversity and early detection features aid in faster content removal and response as leaks spread, helping prevent security risks from escalating.

⁵ Souad Mekhennet and Craig Timberg, "Nearly 25,000 email addresses and passwords allegedly from NIH, WHO, Gates Foundation and others are dumped online," The Washington Post, April 22, 2020, <https://www.washingtonpost.com/technology/2020/04/21/nearly-25000-email-addresses-passwords-allegedly-nih-who-gates-foundation-are-dumped-online/>



- **Allow for cross-enterprise collaboration.** Traditional cybersecurity and threat intelligence tooling are focused on supporting individual user workflows. However, because DRP services now appeal to multiple business roles, organizations require solutions with collaboration and usage permission feature options. This enables more streamlined operations when security goals overlap multiple departments.

THE VALUE OF CROSS-ENTERPRISE FUNCTIONALITY FOR DRP

In the first half of 2020, the video-conferencing app Zoom faced a number of security threats after its usage exploded in response to COVID-19. Adversaries could gain access to private meetings (known as “Zoom bombing”) and even send malware links to meeting members due to insufficient security features.

A DRP solution with access to a range of social, deep and dark web sources would enable Zoom’s security teams to locate content critical to their response. This includes targeted strategy discussions and exchange of Zoom account and meeting credentials on the deep and dark web, and less-regulated social platforms like 4chan.

Zoom’s security issues also evolved into a PR nightmare as the public reacted negatively to their response and feature updates.⁶ In this case, a DRP solution enabling cross-enterprise usability and collaboration is highly valuable for marketing and PR teams addressing this added business risk.

⁶ Kate O’Flaherty, “Zoom’s Security Nightmare Just Got Worse: But Here’s The Reality,” Forbes, June 5, 2020, <https://www.forbes.com/sites/kateoflahertyuk/2020/06/05/zooms-security-nightmare-just-got-worse-but-heres-the-reality/#16ef45aa2131>

CONCLUSION

Digital risk protection is no longer strictly a technical security concern. It is a business concern across many corporate teams, from executives and board members to marketing, HR, and compliance.

Organizations must reevaluate their DRP approach as the market quickly evolves outside of traditional threat intelligence offerings. DRP solutions that support digital security and cross-enterprise functionality are now essential as more enterprise roles integrate online risk data into their strategies.

DRP platforms that prioritize data diversity and machine learning features will also save organizations time and resources amidst a cybersecurity skills shortage. These capabilities are invaluable as threat data volumes grow, digital risks span a greater range of obscure sources, and relevant sites evolve faster than analysts can keep up. Multi-platform aggregation and alerting helps security teams avoid navigating data sources directly and combining incompatible, highly specialized threat intelligence tools.

With these capabilities, organizations can ensure no stones are left unturned, streamline their DRP strategies, and better protect their brand and assets from damage to their capital, infrastructure, and reputation.

Organizations must reevaluate their DRP approach as the market quickly evolves outside of traditional threat intelligence offerings.

TO LEARN MORE ABOUT THE SOLUTIONS PROVIDED BY ECHOSEC SYSTEMS, PLEASE CONTACT US AT 1-844-ECHOSEC, OR USING THE CONTACT OPTIONS BELOW.

SALES INQUIRIES: SALES@ECHOSEC.NET

MEDIA INQUIRIES: ARIEL@ECHOSEC.NET

ECHOSEC.NET