Digital Risk

The C-Suite's Critical
Missing Part of Overall Risk

digital shadows_

Executive Summary

digital shadows_

Gartner notes that 62% of CEOs have a management initiative or transformation program to make the business more digital.[1] However, hardly any understand how to manage the security risks that have emerged as a result.

As organizations become more interconnected to their supply chain, customers, and partners, new types of risk have emerged. Unmanaged, these can lead to the loss of sensitive corporate data, violation of privacy laws, and damaged reputations. When surveyed by the Ponemon Institute, 72% of leaders agreed the rush to digital transformation increases data breach and cybersecurity risks, and 65% agreed the digital economy significantly increases the risk to Intellectual Property.[2]

These risks directly impact business leaders: in North America, 32% of breaches lead to a C-level leader, manager, or president losing their job.[3] While 77% of business leaders understand the need to manage digital risk,[4] they face a sizeable challenge to understand the impact of digitization and create a coherent approach to protect against digital risks.

Digital risk, and particularly that which manifests from outside an organization's traditional boundary, is a critical missing part of a company's overall risk profile. **Organizations need to identify their exposure and understand the threats to their critical assets to better manage digital risks. By detecting data loss, securing their online brand, and reducing their attack surface, organizations can reduce the loss of revenue, intellectual property, and reputational damage.**

Alastair Paterson - CEO and Co-Founder, Digital Shadows

Table of Contents

Digital Business Transformation
Insufficient Approaches to Risk

Digital Transformation and Risk Management

Gartner defines digital business transformation as the "process of exploiting digital technologies and supporting capabilities to create a robust new digital business model".[5] The overarching benefits are obvious: improved collaboration, decision-making, and customer satisfaction will inevitably lead to increased profits. However, these benefits are only realized through effective risk management.

Digital transformation touches all aspects of the business, and every new technology, connection, or application results in increased complexity. Accompanied by a more acute threat, this transformation frequently **leads to the loss of sensitive corporate data, violation of privacy laws, and damaged reputations.**

These incidents put every organization at risk - and it's the C-Suite who bear the ultimate responsibility. From Target to Equifax, the last several years have seen numerous instances where CEOs have been dismissed following data breaches. Up to 32% of breaches led to a C-level leader, manager, or president losing their job in North America.[6] As innovation increases and organizations become more digital, companies need new ways to manage these digital risks.

$3.6m **Average cost of a data breach, according to the Ponemon Institute**

CEOs in the Firing Line: 2014-2019

- **May 2014** - CEO of Target resigns following a data breach
- **February 2015** - Chairman of Sony dismissed following a data breach
- **May 2016** - CEO of FACC dismissed following a Business Email Compromise incident
- **February 2017** - CEO of TalkTalk leaves, four months after the company was fined for a data breach
- **September 2017** - CEO of Equifax resigns following a data breach
- **November 2017** - CSO of Uber dismissed following the announcement of a hack
- **November 2018** - CFO of Pathe Films dismissed following a Business Email Compromise incident
- **January 2019** - CEO of SingHealth fined following data breach

Digital Business Transformation
Insufficient Approaches to Risk

Departmental Silos Prevent Progress

According to Gartner, 77% of leaders understand the importance of managing digital risks,[7] but few have a coherent approach to identify, quantify, and manage digital risks across the business. CEOs and other C-level executives are unlikely to be able to grasp the technical details of many security issues and so struggle to determine the real risk to the company.

Conversely, the security team - which the company relies on to protect against these risks - is not equipped to think about the overall business risk. A recent report by Accenture found that "business risk improvement" was the least popular measure for security teams' success criteria (38%), behind system downtime (62%), restoration time (57%), and response time (56%).[8]

There is a clear disparity between how business risk and security are understood, which constitutes a barrier to progress.

Integrated Risk Management:

"A set of practices and processes supported by a risk-aware culture and enabling technologies, that improves decision making and performance through an integrated view of how well an organization manages its unique set of risks."

- Gartner[9]

Blurring Departmental Lines

The burden to manage digital risks should not fall on a single department, and these new challenges extend beyond the purview of the security team. In today's increasingly stringent regulatory world, any attempt to manage risk without involving legal, fraud, and compliance teams falls short of providing an understanding of business risk. However, these teams do not have the skills and resources to monitor overall risk effectively and communicate it to the board.

There are several approaches to blur the lines between departments and remove these silos. First, Integrated Risk Management (IRM) seeks to combine security risk and business risk. In the digital age, digital risk is a key component of Integrated Risk Management.

Additionally, McKinsey & Company have outlined a framework for greater interaction between different C-Level roles. The proposed "strategic security partnership" is a framework for CISOs, CIOs, and CROs to work together and move to a collaborative, enterprise-wide approach to risk.[10] By doing so, silos are broken down, friction is reduced, and risk becomes embedded in the CISO's program.

The Emergence of Digital Risk Protection

Don't Neglect the Risks From the Outside

The Perimeter Doesn't Exist

There is plenty to contemplate when attempting to reduce the risks that result from digital transformation. Scalability, platform hardening, application monitoring, resilience, and insider threat programs are all considerations for managing digital risks. This would be sufficient if perimeters were neatly defined and data resided safely within the organization's view.

However, the interconnectivity of the digital age means we need to widen our view. Indeed, when surveyed by the Ponemon Institute, 72% of leaders agreed the rush to digital transformation increases data breach and cybersecurity risks, while 65% agreed the digital economy significantly increases the risk to Intellectual Property.[11]

A physical network no longer determines the organization's boundary; the very data organizations seek to protect is spread across third parties, social media, mobile devices, and the cloud. This means organizations need to gain visibility beyond their traditional perimeter.

72% **Of leaders agreed the rush to digital transformation increases data breach and cybersecurity risks[12]**

65% **Of leaders agreed the digital economy significantly increases the risk to Intellectual Property[13]**

Digital Risk Protection reduces risks that emerge from digital transformation, protecting against the exposure of assets and giving actionable insight to threats across the open, deep, and dark web.

- Digital Shadows

A Framework for Protecting Digital Risks
Identifying Your Critical Assets

What Are Your Critical Assets, and Where Are They?

According to Forrester, organizations are looking at ways to "deal with the heightened exposure their organizations' digital infrastructure, assets, and accounts face online." By doing so, organizations can "fix issues before bad actors exploit them...and limit the effects of successful attacks when they occur."[14]

There are four steps to achieving this visibility into digital risks, which are outlined in the diagram below.

This first step is, of course, understanding what an organization considers to be their critical assets. This will vary from organization to organization. For a technology or pharmaceutical company, it might be their patents and intellectual property. For a retail company, it may be upcoming product names and their customer websites. For an investment bank, it might be an pending merger or acquisition.

Exposure of these assets often leads to business risks, such as loss of revenue, reputation or competitive advantage.

Adversaries will make use of your online exposure; using exposed credentials to conduct account takeovers, leverage intellectual property to conduct corporate espionage, impersonating your brand to launch phishing attacks, and exploit vulnerabilities in your external infrastructure.

Therefore, a useful exercise for organizations is to begin thinking about the type of sensitive data you hold, and how this might be appealing to a range of threat actors. From there you can think about the ways adversaries might access this information, and where you might be exposed.

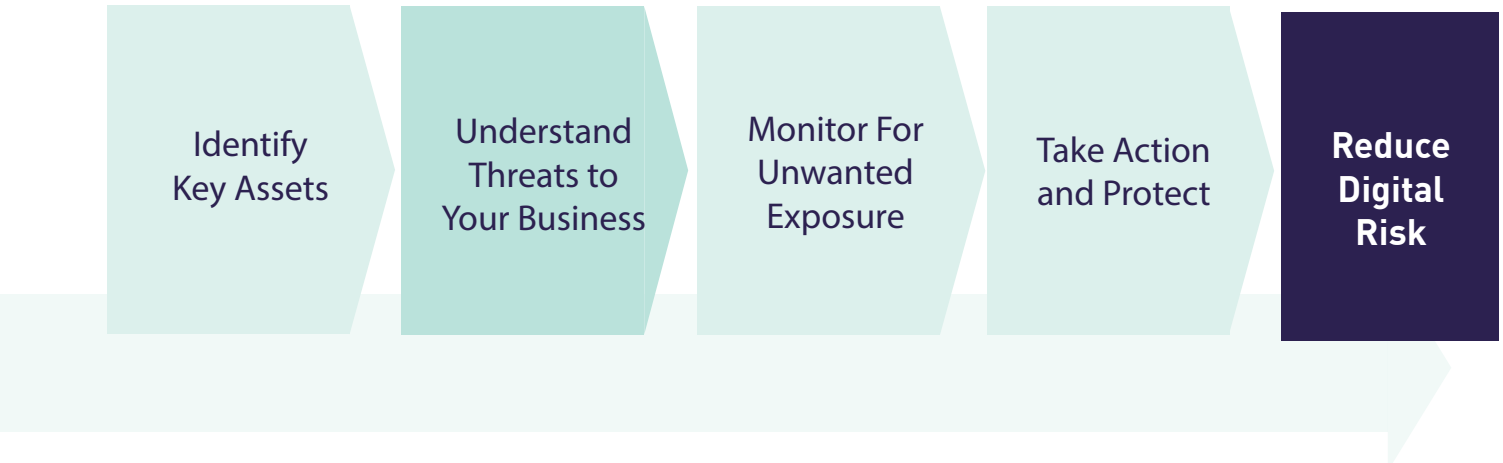
Understanding Threats to Your Business

Adversaries understand the value of this exposure and look to exploit it, but what they target will vary based on the adversary's motivation and goals. A group known as FIN7, for example, went after payment card data and non-public information.[15] The GRU (Russian Intelligence) sought emails, analytics, and internal documents.[16] The Syrian Electronic Army (SEA) targeted social media accounts.[17]

The ability to understand the threat is a key part of calculating risk, and there are a number of factors to consider when assessing it; we need an understanding of a threat's behavior (capabilities and tactics), motivations, and the opportunities the threat may exploit. The broad discipline of Cyber Threat Intelligence, if executed effectively, can provide useful insight into these threats.

A recent shift towards a strategic focus on attacker behavior through Tactics, Techniques and Procedures (TTPs) and frameworks like MITRE ATT&CK,[18] provide promising insight into how defenses can be aligned to real-world threats. In understanding Digital Risk, Digital Shadows continually monitors the threat landscape, actors, and tools to understand the latest behaviors.

However, behaviors are just one piece of understanding the threat. Critically, organizations need to understand the opportunities available to the threat actor. Adversaries exploit opportunities and will prioritize their attacks accordingly.



A Framework for Protecting Digital Risks

Exposure of Your Data, Brand, and Attack Surface

How is Your Business Being Exposed?

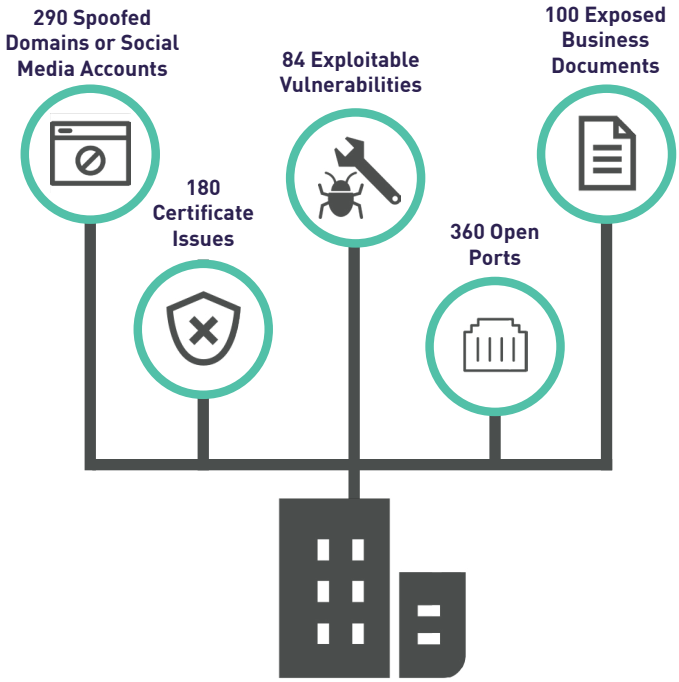
Organizations' exposed data, brand, and attack surface afford adversaries a wealth of opportunities. For example, contractors often back up proprietary information on their misconfigured file sharing drives, employees over-share on social media, or developers expose sensitive code on code sites. Data always ends up online.

Malicious actors look to target your brand to access the information of your employees and customers or dupe them into buying fraudulent goods. Tactics include domain infringement, rogue mobile applications, spoofed social media accounts and counterfeit sites.

Finally, weaknesses and exposure exist across your known infrastructure, which increases your attack surface. This is further complicated by shadow IT - those projects and software managed outside of the IT department. This is why only 29% of organizations believe they have sufficient visibility into their attack surface.[19]

Detection can be difficult, and so we'll outline ways that organizations can begin to detect unwanted exposure at the end of this paper.

To give a sense of scale, below is what a typical mid-sized organization finds in one year with Digital Shadows.



A Framework for Protecting Digital Risks

Take Action and Protect

How Can You Protect Your Organization?

Next, organizations need to find ways to protect themselves against this heightened exposure. Here are three ways organizations that we have worked with have mitigated their exposure, through 1) detecting data loss, 2) securing their online brand, and 3) reducing their attack surface.

1. Data loss detection.

A manufacturing organization had recently moved to a third party to manage their payroll. Unfortunately, this accounting software soon suffered a breach. The breach exposed millions of credentials, including hundreds belonging to their employees. Twenty percent of these credentials were valid, including the password of a system administrator. Worse still, the manufacturing organization did not have multi-factor authentication, which would have allowed attackers to perform account takeovers and access internal systems. A breach of sensitive data would lead to regulatory risks, as well as have a significant impact on the business and brand reputation. By quickly detecting the exposed credentials and resetting the affected accounts, the organization reduced the opportunity for attackers to re-use compromised credentials.

2. Online brand security.

A retailer discovered a domain imitating its brand, with a slight variation on their legitimate domain. To the untrained eye, the domain was an identical replica of the retailer's log-on page. Criminals could take these harvested credentials and gain access to customer accounts. The organization would lose money on refunding lost customer balances and fraudulent transactions, but it would also lose a great deal of reputation. The retailer was able to detect the impersonation and assess the similarities with its own domain. With this information, the organization worked with its legal team to take down the domain in question - preventing the theft of customers' credentials.

3. Attack surface reduction.

For one large conglomerate, a vulnerability in an application of a recently-acquired organization was discovered. By monitoring for vulnerabilities in their external IP addresses, the organization learned that an IP address of a recently acquired entity was vulnerable. If this vulnerability were to be exploited, encrypted confidential information and encryption keys could be exposed. This would have a significant impact on the organization's business. The organization was able to prioritize this patch and avoid a potential compromise.

Reducing Digital Risk

Maturing Digital Risk Protection Brings Business Benefits

Despite all the challenges associated with digital transformation, a mature Digital Risk Protection capability can improve collaboration, decision-making, and customer satisfaction. If risk can be managed at a business level, rather than siloed into security departments, this will allow for more comprehensive risk prioritization and bring greater business benefits.

A mature approach to digital risk does not happen overnight, and organizations should build towards this. While some organizations are unaware of their digital risk, most have some level of visibility through manual processes or tooling that is highly reactive and limited in scope. As organizations increase their maturity, they become more proactive, their processes and roles become more defined, and their tooling becomes more extensive. At the optimal level, gaps in collection and processes are known and continually reviewed. Most significantly, risks are effectively quantified and reported throughout the business.

Questions the C-Suite Should Be Asking

How confident would you and the rest of your leadership team be if asked the following questions:

1. **Who is "in charge" of managing digital risk? Are we relying solely on the CISO or does risk extend beyond silos?**
2. **Are we extending digital risk management beyond the company, into our partner and vendor ecosystem? What tools does the organization have in place to detect and remediate risks outside the traditional perimeter?**
3. **Does our CISO address security in terms of business risk? Do we measure the success of the security team in terms of business risk?**

Protect Your Customers

Avoid Regulatory Fines

Safeguard Intellectual Property

Maintain Competitive Advantage

You Don't Need to Do it Alone

Three Ways Digital Shadows Can Help

Digital Shadows minimizes digital risk by identifying unwanted exposure and protecting against external threats.

Since 2011, we have been developing our core product, SearchLight, which enables organizations to minimize their digital risk by detecting data loss, securing their online brand, and reducing the attack surface.

As the market-leader in Digital Risk Protection, this guide outlines a framework for how organizations can better understand and manage this critical, missing part of overall risk: digital risk.

For organizations interested in doing so, here are three ways we can help.

1. Download our Free "Practical Guide to Digital Risk"

Gaining visibility into an organization's unwanted exposure and external threats can be challenging. That's why we've created a guide to help Security, Intelligence, and Fraud Teams to develop their capabilities. Download "A Practical Guide to Reducing Digital Risk" for information on tools and approaches.

2. Test Drive SearchLight for Free

Explore our portal's capabilities at your pace and experience the industry's most awarded digital risk solution hands-on. For 7 days, you can search across dark, deep, and dark web, and explore examples of risks we identify.

3. Get in Touch to Learn More

To learn more about how Digital Shadows can help your organization to reduce digital risk, get in touch.

Email us at messages@digitalshadows.com

Endnotes

1. Gartner, Fuel Digital Business Transformation via a Digital Risk Management Solution Stack
2. Ponemon Institute, Bridging the Digital Transformation Divide
3. Kaspersky, Businesses and personal data, https://www.kaspersky.com/blog/data-protection-report/23824/
4. Gartner, CEOs and CIOs Are Seeking Digital Risk Leaders, https://blogs.gartner.com/john-wheeler/ceos-and-cios-are-seeking-digital-risk-leaders/
5. Gartner, Digital Business Transformation, https://www.gartner.com/it-glossary/digital-business-transformation
6. Kaspersky, Businesses and personal data, https://www.kaspersky.com/blog/data-protection-report/23824/
7. Gartner, CEOs and CIOs Are Seeking Digital Risk Leaders, https://blogs.gartner.com/john-wheeler/ceos-and-cios-are-seeking-digital-risk-leaders/
8. Accenture, 2018 State of Resilience, https://www.accenture.com/t20180416T134038Z__w__/us-en/_acnmedia/PDF-76/Accenture-2018-state-of-cyber-resilience.pdf
9. Gartner, IRM, https://www.gartner.com/it-glossary/integrated-risk-management-irm
10. McKinsey, Cybersecurity and the risk function, https://www.mckinsey.com/business-functions/risk/our-insights/cybersecurity-and-the-risk-function
11. Ponemon Institute, Bridging the Digital Transformation Divide
12. Ibid
13. Ibid
14. Forrester, The Forrester New Wave™: Digital Risk Protection, Q3 2018, https://go.forrester.com/blogs/blog-digital-risk-protection-drp-wave-18/
15. Digital Shadows, Mitre ATT&CK™ and the FIN7 Indictment: Lessons for Organizations, https://www.digitalshadows.com/blog-and-research/mitre-attck-and-the-fin7-indictment-lessons-for-organizations/
16. Digital Shadows, Mitre ATT&CK™ and the Mueller GRU Indictment, https://www.digitalshadows.com/blog-and-research/mitre-attck-and-the-mueller-gru-indictment-lessons-for-organizations/
17. Reuters, Syrian Electronic Army says hacked into Skype's social media accounts, https://www.reuters.com/article/usa-syria-hack/syrian-electronic-army-says-hacked-into-skypes-social-media-accounts-idUSL2N0KC01020140102
18. Mitre ATT&CK, https://attack.mitre.org/
19. Ponemon Institute, Managing the Cyber Risks to Business Operations

About Digital Shadows

Digital Shadows minimizes digital risk by identifying unwanted exposure and protecting against external threats. Organizations can suffer regulatory fines, loss of intellectual property, and reputational damage when digital risk is left unmanaged. Digital Shadows SearchLight™ helps you minimize these risks by detecting data loss, securing your online brand, and reducing your attack surface.

To learn more and get free access to SearchLight, visit www.digitalshadows.com.

London

Columbus Building, Level 6,
7 Westferry Circus,
London, E14 4HD

+44 (0) 203 393 7001

messages@digitalshadows.com

San Francisco

332 Pine St. Suite 600,
San Francisco, CA 94104

+1 (888) 889 4143

Dallas

5307 E. Mockingbird Ln.
Suite 200
Dallas, TX 75206

digital shadows_