



A Practical Guide to Reducing Digital Risk

Tools and Approaches for Security,
Intelligence, and Fraud Teams

digital shadows 

Dear Reader,

Thank you for taking the time to download our practical guide to managing digital risk. Al and I started Digital Shadows in 2011, at a time when social media was going mainstream; Infrastructure-as-a-service was transforming speed, method, and location of application development and online services; and the impact of consumerization of mobile and end user business computing were changing InfoSecurity for good. All of this meant the much-loved enterprise perimeter was becoming a thing of the past, and new “digital risks” emerged.

In 2011, we and others were tinkering with OSINT tools like Paterva’s Maltego, reconnaissance pen testing tools, services like Shodan were really getting going, and many of us were enjoying the work of Bishop Fox’s Diggity and Johnny Long’s much read “Google Hacking” books.

What we’ve attempted to do with this document is record some of the useful things that we discovered along the way, and consolidate some of the feedback and learnings we’ve gained from our prospects and customers who’ve embarked on their own journeys. Hopefully it will be useful for others exploring these risks. Our intention is to continue to iterate this document and grow it. We’ve published this document under a creative commons license, so you may feel free to use the content with attribution to us.

In everything we do, we thrive on feedback, and therefore I have only one ask of you in exchange for this document. Please do let us know what you think. Give us feedback at practitioner@digitalshadows.com. If you have additions or suggestions, please let us know. We’ll happily include your content and reference you in the process.



James Chappell

Co-Founder and Chief Innovation Officer

James has led teams in InfoSec and Cybersecurity since 1997, working across the private sector and government organizations helping them to understand the technical aspects of information security. James spent over 10 years of his career as a security architect and deputy head of the Information Security profession at BAE Systems Detica, and over five years prior to that in the telecommunications industry.

He is fascinated by technology and in particular the fields of systems and computer/information security. He has focused much of his career trying to help organizations see the bigger picture in computer security and this led to the establishment of Digital Shadows in 2011 where the exploration of digital footprints and the risks inherent in them continue to this day. He is a co-chair of FIRST’s Cyber Threat Intelligence SIG, IISP and a member of CREST’s international organization.

For those working to secure organizations, life isn't getting any easier. As businesses continue to invest in technology, the environment that must be secured has become more complex and challenging. Alongside the benefits of digital transformation, new risks have emerged - digital risk.

With cloud computing now best practice and data shared across a complex array of third parties, the perimeter is barely recognizable. How useful are controls, such as Data Loss Prevention or Cloud Access Security Brokers, when employees starting skunk work projects, or visit websites to use the latest software-as-a-service portal? Organizations are finding it increasingly difficult to know where their data is stored and shared, and do not have the tools or know-how to detect and mitigate this exposure.

The opportunity presented to adversaries by these increased attack surfaces has led to more incidents. They understand how to leverage and manipulate an organization's online presence; they make use of breached employee credentials to perform account takeovers, they imitate the people or brand to target employees and customers, and exploit vulnerabilities in the expanding attack surface.

This guide is written for people whose role it is to deal with this complexity: the practitioners. It provides advice to help understand how to identify critical business assets, understand the threat, monitor for exposure, and take action. This guide provides advice on tools and approaches which, alongside better quantification, cohesion, reporting, and documentation, will enable organizations to move towards a more mature approach to reducing digital risk.



Free tools organizations can use to monitor for exposure, such as exposed credentials, documents, and infrastructure weaknesses



Tactical, operational, and strategic mitigation strategies



The critical role of threat intelligence within digital risk



Attribution 4.0 International

Table of Contents

- Executive Summary.....3
- Characterizing Digital Risk.....5
 - Effects of Digital Transformation5
 - Evolving Understanding of Adversaries6
 - Security Teams Expected to Protect the Organization7
- Data Loss Detection.....9
- Online Brand Security.....11
- Attack Surface Reduction13
- Four Steps to Reducing Digital Risks15
 - Step 1: Identify Key Assets to Protect.....15
 - Step 2: Free Tools to Monitor for Exposure17
 - Step 3: Understand the Threat.....20
 - Step 4: Mitigation Strategies26
- Building Maturity in Digital Risk Protection.....30
 - Build Versus Buy30
 - Building Maturity is About More Than Tools31
 - Getting Started.....32
- Endnotes.....33
- Appendix 1: Copyright Details34

Characterizing Digital Risk

Effects of Digital Transformation

Most organizations will have the investment in digital as one of their strategic goals, believing it will increase speed, collaboration, efficiency, and profit. All of these benefits can (and should) be achieved, but this will only happen if the associated risks are effectively managed.

Digital transformation, in practice, means that organizations focus on four objectives, which are illustrated in Figure 1.

Every new technology, connection, or application increases complexity and data becomes stored in more places. The supply chain that provides the services or accesses that data is far greater, and weaknesses in legacy technologies make this world especially challenging to protect.

Digital footprints are vast and growing; as more technologies and third parties form a more complex ecosystem, it becomes hard to understand the growing attack surface, manage shadow IT, measure the ephemeral loss of critical data, and understand the integrity of the organization's identity. The chances of weaknesses or exposure in this growing footprint has increased significantly.

In our de-perimeterized world, much of the critical data assets exists beyond the perimeter. Third parties are actively sharing and exploiting data within their own digital transformation initiatives, which means risks extend well beyond these castle walls.

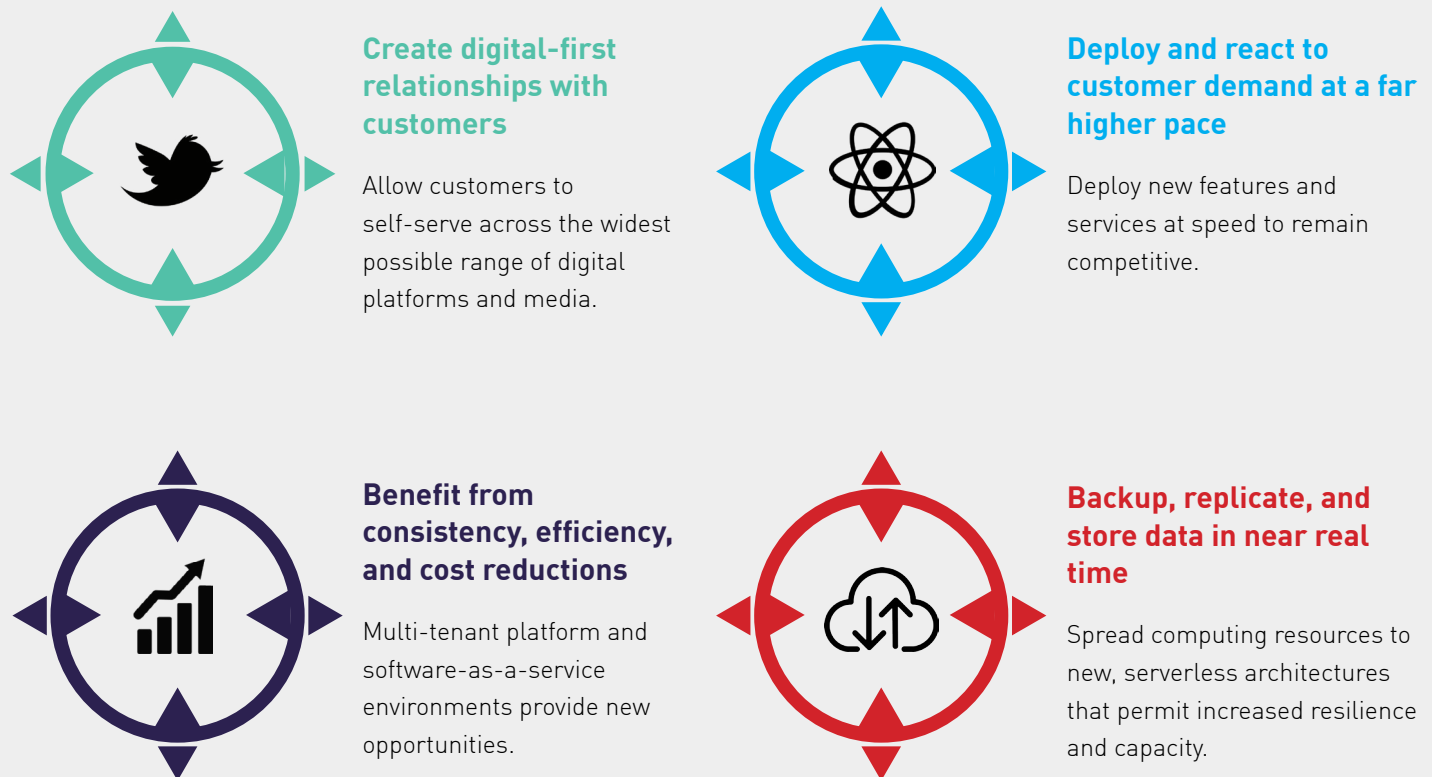


Figure 1: Four common objectives of digital transformation

Characterizing Digital Risk

Evolving Understanding of Adversaries

We know that opportunistic adversaries will actively seek and exploit exposed information; looking for an exposed admin password on GitHub, a leaked vulnerability assessment, or network diagrams.

Even organizations that claim to not be 'interesting enough' for an attacker will have computing resources that themselves have monetary value for criminals.

With the emergence of Cyber Threat Intelligence (CTI), organizations have some of the best insight in history into the various types of electronic criminality across the spectrum. Within CTI, the "what" is far better understood than the "how". Understanding attacker behavior can be strategic, operational, and tactical and, as we head up the levels, actions can move away from blocking individual indicators of compromise toward secure design that is targeted to prevent certain observed behaviors. We now focus on the tactics and techniques of our adversaries and use this to inform our defenses. This is great progress, and we will dig into this more in the "Understanding the Threat" section of this paper.

At the center of all organizations' strategies should be an approach to understanding and effectively managing risk, which must include Digital Risk. Risk managers describe an organization's risk as a product of the assets to be protected,

the weaknesses present in a system, and the opportunities presented that a given threat actor will exploit. CTI provides us valuable insight into the threat component of this risk relationship.

Combining this perspective of threat with an understanding of the organization's exposure can help organizations to prioritize defenses, and focus resources on protecting the right information assets.

The Emergence of Digital Risk Protection

To realize the benefits of digital transformation, organizations must manage the significant negative impacts, including the loss of sensitive corporate data, disruption of identity, violation of privacy laws, and damaged reputations. This is Digital Risk.

Yet organizations are still sprinting towards digital transformation without full consideration or an effective way to manage the associated risks.

Digital Risk Protection reduces risks that emerge from digital transformation, protecting against the unwanted exposure of a company's data, brand, and attack surface and providing actionable insight on threats from the open, deep, and dark web.¹

Characterizing Digital Risk

Security Teams Expected to Protect the Organization

Over the last three to five years, cyber security has been undergoing an encouraging shift from being solely the consideration of the IT department to being on the board's agenda. The same is true of Digital Risks. Gartner states that the management of digital risk is a "business performance issue".² Business leaders are excited about the new business models and opportunity unlocked by digital transformation programs, but are understandably concerned how digital transformation can be delivered without negatively impacting the business.

Delivering a low-cost, high-value customer platform that enables more profitable business is at the center of board agendas, but they realize this will all be for nothing if that transformation is dogged by problems in launch, suffers a betrayal of customer trust or, worse still, is subject to a damaging breach.

Chief Information Security Officers (CISO's) are rightfully being involved in these transformation programs. Failure to manage this risk effectively is serious – not just for the CISO's but for the whole business. Make no mistake, jobs are also on the line.³ Business leaders expect security teams to protect the business, but given we are shifting from traditional security models, to be successful organizations must take a more inclusive approach to the problem.

While the security team is the primary protector of this information, these risks are cross-departmental. According to Forrester, the most common departments to concentrate on Digital Risk Protection are Information Security (50%) and Threat intelligence (26%),⁴ although this also extends to fraud, compliance, and risk teams.

Characterizing Digital Risk

Security Teams Expected to Protect the Organization

Security Teams Want to Increase Communication with the C-Level

Teams that manage these risks are being asked to address new problems with the same tooling and processes that were deployed for the previous generation of online initiatives. Security teams sometimes only become involved at the last stages of the launch of a program or must deploy tests once the application is delivered. To avoid costly re-writes or program delays, security teams have been working hard to “shift left” toward the requirements stage of transformation programs.

Businesses are improving their involvement of information security in their transformation programs, but concerns about these new types of digital risk are not always reflected by the teams expected to manage them.

A recent report by Accenture found that “business risk improvement” was the least popular measure for security teams’ success criteria at 38% (behind system downtime [62%], restoration time [57%], and response time [56%]).⁵

Communicating business risk more effectively is at the top of security, fraud, and intelligence teams’ priorities; 64% of practitioners said that a top goal for 2019 was increasing communication with C-level executives and the board.⁶ Information security and risk professionals have been converging on models of Total Asset Values, using tools such as the FAIR Institute’s approach to risk modelling in an attempt to break down these barriers.⁷

This guide provides tools and approaches for those teams deemed responsible for securing the business in the digital age, and alleviating business concerns. We have divided Digital Risk Protection down into three areas of focus: detecting data loss, securing identity and online brand, and reducing the attack surface. In subsequent sections, we’ll provide tools to begin identifying and protecting weaknesses in organizations’ digital footprints.

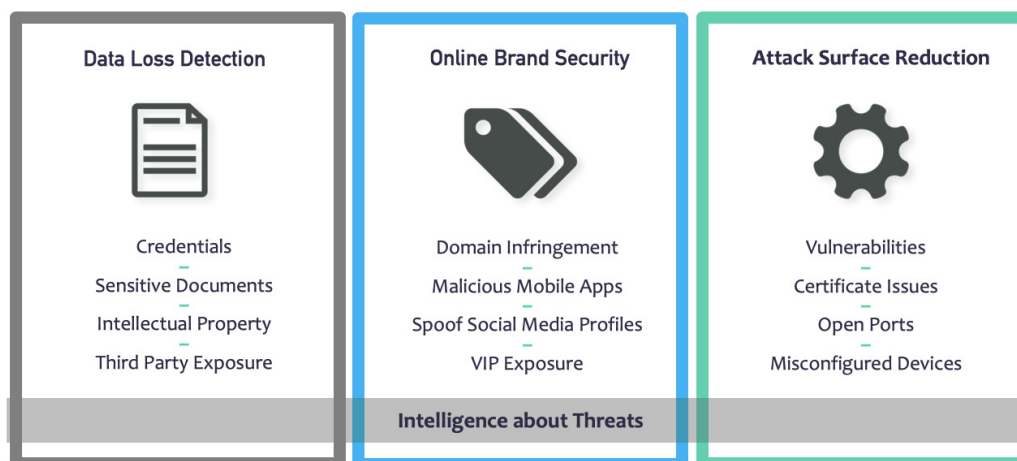


Figure 2: Three key components of Digital Risk

Data Loss Detection

Exposed Credentials, Sensitive Documents, and Code

A key responsibility for any IT security professional is to secure the information assets, be that customer data, financial information or any other critical information. Often the focus is on controlling flows of sensitive data over the perimeter or within the network, perhaps with Data Loss Prevention solutions. This approach misses data that is already exposed across the digital footprint of the business which extends beyond the perimeter, throughout the supply chain.

When we do consider where data is exposed outside the perimeter, we are often guilty of hyper-focusing on illicit channels where stolen data is traded. This is an important aspect - after all, what organization would not want to know if their intellectual property or sensitive data was on the dark web or a criminal forum? However, it's far better to detect these exposed assets before adversaries get to the stage of trading them online.

A great example is misconfigured online file stores. Barely a month goes by without a report of an S3 bucket exposing yet more sensitive information. However, our research suggests S3 buckets only account for 7% of exposed data; older, yet still widely used, technologies - such as SMB (33%), rsync (28%) and FTP (26%) - contributed the most exposure.

In total, we discovered over 1.5 billion files exposed across these misconfigured online file stores, as illustrated in Figure 3.⁸

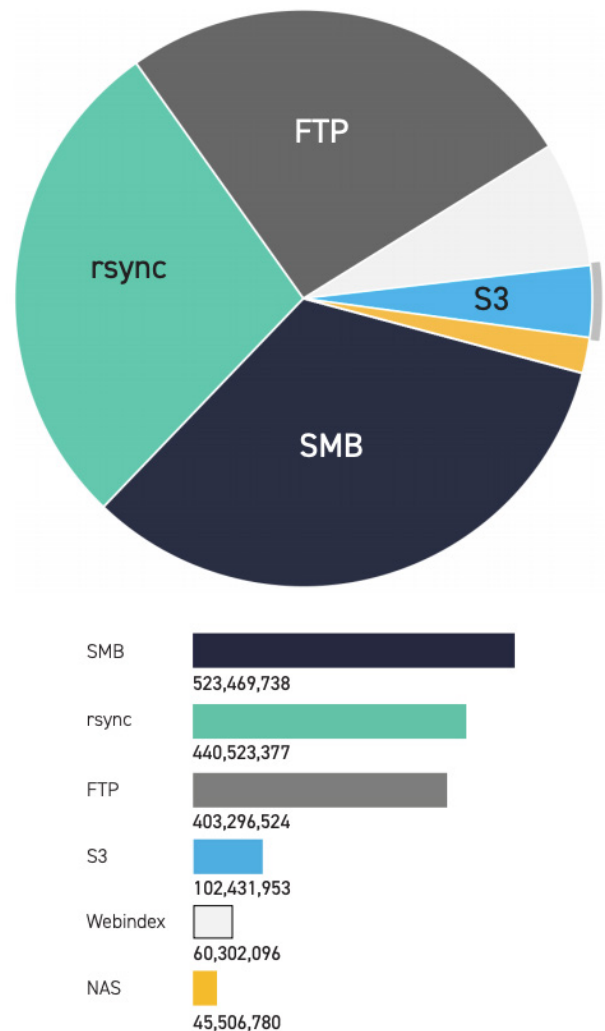


Figure 3: File exposure by technology type

Data Loss Detection

Exposed Credentials, Sensitive Documents, and Code


Exposed data can lead to regulatory pressure and fines, or it can be used by threat actors in the reconnaissance stage of their operations. While some information shared on criminal forums has been obtained through nefarious means, a great deal more is inadvertently exposed. For example, contractors backing up proprietary information on their misconfigured network attached storage (NAS) drives, employees over-sharing on social media, or developers exposing sensitive code on code sites. The opportunities for data to inadvertently land up online in a location where it should not be are numerous.

The type of information exposed can present a variety of business impacts for organizations. These business impacts matter; data loss is an issue that extends well beyond the IT security team. If we look at data loss as a whole, common types of documents we hear about include:

- **Confidential Business Documents.** Exposed confidential documents, broken embargos, M&A information, and board minutes.
- **Intellectual Property.** Product designs, proprietary code, and patents information that would lead to a loss of competitive advantage.
- **Customer Details.** Exposed customer data that can be in violation of compliance and privacy regulations.
- **Data for Reconnaissance.** Information that adversaries search for as part of their reconnaissance, such as employee credentials, private RSA keys, or exposed security assessments.
- **Code Exposure.** Developers and third parties can inadvertently exposed sensitive code and credentials on code-sharing sites like GitHub.

It's not just the organization that can expose this information; **third parties are a common point of data exposure**. This issue is exacerbated further still by shadow IT and the digital risks present in organizations' lengthening supply chains.

Data loss detection in action



A manufacturing organization used an accounting software that suffered a breach of the user accounts. The breach exposed millions of credentials, including hundreds belonging to the manufacturing organization's employees. Twenty percent of these credentials were valid, including the password of a system administrator. Unfortunately, the organization did not benefit from multi-factor authentication on a key remote access service. Attackers had the potential to exploit the credentials using a technique called credential stuffing, permitting control of internal systems. A breach of this sensitive data would lead to regulatory risks, as well as have a significant impact on the business and brand reputation. By quickly detecting these credentials and resetting the affected accounts, the organization reduced the opportunity for attackers to re-use compromised credentials.

Online Brand Security

Malicious Domains, Mobile Apps, and Social Media Accounts

The integrity of brand and identity is incredibly important in protecting a business. Adversaries are routinely impersonating businesses and key online services to target customers and important business transactions: they're registering domains, creating fake mobile applications, impersonating documents sent in email, spinning up spoof social media profiles of key executives - all with the aim of duping people to comply with their schemes allowing them to steal, disrupt, damage or destroy.

This misuse of online brand also affords adversaries ways of targeting an organization's employees. According to the SANS Institute, 95% of enterprise network attacks involve successful spear phishing attempts.⁹ This social engineering tactic that is routinely used by almost every type of adversary, from state-level actors to low-level spammers. The indictments issued by the United States Department of Justice (DOJ) in 2018 against an individual associated with Lazarus Group¹⁰ underscored just how effective well targeted phishing can be: culturally relevant, free from spelling and grammar errors, and hitting the right psychological buttons to yield a result.

A number of these phishing sites will allow an attacker to imitate your brand so accurately it is almost impossible to spot the difference. This can be difficult to detect as the infringing sites are set up quickly and used in short bursts before security teams receive complaints from customers and investigations reveal the subterfuge.

As an example, the technique of domain squatting relies on implementing permutations of a legitimate domain. A range of different permutations we commonly see are shown below. In a year, the typical Digital Shadows customer will detect approximately 300 spoof domains.

14 Top Approaches to Spoofing Domains

- | | |
|--------------------------|------------------|
| 1. Singularize/Pluralize | 8. Repeater |
| 2. Sub-Domain | 9. Omitter |
| 3. Strip-Dash | 10. Hyphenator |
| 4. Missing-Dot | 11. Bit Squatter |
| 5. Swapper | 12. Homoglyph |
| 6. Replacer | 13. Homophone |
| 7. Inserter | 14. TLD |

Read how to detect spoof domains in
"Free Tools to Monitor for Your Exposure"

Online Brand Security


Malicious Domains, Mobile Apps, and Social Media Accounts

Even the least sophisticated threat actors have access to a wide variety of forums and groups and tools where they can learn the latest phishing techniques, as well as purchase step-by-step tutorials and phishing templates to conduct their own campaigns. In serving our customers we regularly see business email compromise (BEC) and Whaling attacks routinely combine false domains with out of band communications on convincing looking web services. In some cases whole call centers are set up to perpetuate the subterfuge. Knowing the location of legitimate assets and detecting the anomalies can help manage this risk.

There are real business impacts in these operations. These types of impersonation are particularly acute for fraud teams, who are grappling with increasing online payment fraud risks, which are notoriously difficult to

measure on a global basis. It is a significant problem. Juniper Research estimates to have observed losses of \$22 billion throughout 2018.¹¹ Despite a host of eCommerce fraud prevention tools and processes employed by many fraud teams to detect anomalies, this number is estimated to rise to \$29 billion globally by 2023.¹² Organizations cannot rely solely on spotting anomalies in transaction data to detect fraud in online commerce and should proactively detect where customers may be targeted online. Different techniques spoof the brand, such as domain infringement, spoof social media profiles, and malicious mobile applications. By detecting these impersonation attempts, organizations can better detect the targeting of customers, as well of the sale of fraudulent and counterfeit goods.

Online brand security in action



A retailer discovered a domain imitating its brand, registered 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 suffer reputational damage. 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 takedown the domain in question - preventing the theft of customers' credentials.

Attack Surface Reduction

Infrastructure Weaknesses and Exposure

As organizations' infrastructure grows and becomes more complex, it can be difficult to keep up with their expanding attack surface. Indeed, only 29% of organizations believe they have sufficient visibility into their attack surface.¹³ The attack surface is becoming increasingly hard to reliably identify, nevermind reduce.

The Equifax breach, which exposed over 140 million customer records, is a good example of why it's important to get this right. Equifax reported that this breach occurred through an unpatched web application that was vulnerable to an exploit in the Apache Struts framework (CVE-2017-5638).¹⁴ This vulnerability had patches available for two months, and evidence of the exploitation of this weakness was widely known as many attackers had already been observed to have exploited this weakness in campaigns.

Part of the challenge for Equifax, and many other organizations, is knowing what assets exist in the IT estate in the first place. While Equifax may be an extreme example, all companies' IT departments are playing a constant game of catchup with their changing organizations and rarely have a complete view of what they are responsible for protecting. Shadow IT has become a very real problem for businesses globally as they grow, merge, and adapt their infrastructures.

Even those that have an effective vulnerability management program experience challenges prioritizing the range of work without disrupting IT operations. Worryingly, nearly 60% of organizations still have no set schedule to address vulnerabilities or do not do vulnerability scans.¹⁵ Even those that do have patch management processes can be easily overwhelmed and unable to prioritize which vulnerabilities to patch.



Attack Surface Reduction

Infrastructure Weaknesses and Exposure

SANS defines attack surfaces as “our exposure, the reachable and exploitable vulnerabilities that we have.”¹⁶ These weaknesses and exposure can include open ports, infrastructure vulnerabilities, or weak or expiring certificates. These exist across your known infrastructure, but also extends to shadow IT - those projects and software managed outside of the IT department, the existence of which may not be known to the security team.

By looking to manage and reduce the attack surface, and taking an outside-in perspective of the attacker, organizations have the ability to identify these untracked IT investments and greatly reduce the attack opportunities presented to an adversary.

The outside-in approach can also help organizations understand the attack surface present across third parties and the supply chain, which can greatly compound these risks.

Reducing the attack surface is already a focus for many organizations, as demonstrated by three of the top controls in SANS 20:

- Inventory of Authorized and Unauthorized Software (CSC 2)
- Continuous Vulnerability Assessment and Remediation (CSC 4)
- Limitation and Control of Network Ports, Protocols, and Services (CSC 9)

Attack surface reduction in action

For one large conglomerate, a vulnerability on an IP address 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.



Four Steps to Reducing Digital Risks

Step 1: Identify Assets to Protect

To reduce digital risks, a company must first identify what they care about, detect where that is exposed or disrupted online, understand the threat to the company, and then protect against it. These steps are iterative; once companies begin to monitor for exposure and assess the threat, they will have a better idea of what to protect.

Fortunately, there are a wide range of resources available to companies, including social media monitoring, search engine engineering, Open Source Intelligence, and security testing reconnaissance that can help organizations start to grapple with the effective management of these risks.

Step 1: Identify Key Assets to Protect

This first step is, of course, understanding what an organization considers to be their critical assets and wishes to protect. This is a familiar process for many who have performed a risk assessment. In accordance with good risk management practice, organizations will take the time to think about the type of sensitive data being held, and how this might be appealing to a range of adversaries.

It's possible to take a purely technical perspective, simply listing computers associated with a business, but an effective place to start is to think about common examples of critical business assets. Start with people (customers, employees, partners, service providers); organizations (peer organizations, service departments, common infrastructure) and the systems and critical applications that support them (websites, portals, databases holding customer data, payment processing systems, employee access systems, trading platforms, or Enterprise Resource Planning (ERP) applications).



Four Steps to Reducing Digital Risks

Step 1: Identify Assets to Protect

Think about tangible assets such as money, intellectual property and how important intangible properties such as trust, reputation and goodwill rely on them. Also consider how those relate to the core business processes that generate profit or give a competitive advantage to the business. The information security profession has many best practice guides for identifying assets and they can provide an excellent guide to establishing an asset register. Indeed information asset management is a whole discipline in itself, and the effective collection, maintenance, and validation of these asset registers continues to be an important mission for most technology teams.

Best practice is to center asset management activities around the critical business or economic functions of an organization. In performing risk assessment working out the business critical assets and prioritizing them pays dividends later in the risk management process. Criticality should consider operational resilience, intellectual property, market advantage (for new products and service announcements), business- or investment-sensitive, or other regulated information.

Some assets will depend on the company itself. For example, for a technology or pharmaceutical company, this might include patents and intellectual property. For a retail company, they may include upcoming product names and their customer websites. For an investment bank, it might be a pending merger or acquisition.

In digital risk, there is an additional and important step to think about: how these assets are referenced or appear in the digital domain. It is a good practice to list a wide range of identifying text strings which may be helpful in identifying particular types of assets, be they technical watermarks, footers, domains or protective markings used to mark confidential documents. Working out the digital footprint and other properties of these assets helps in the process of building a suitable collection plan that identifies them online and in the process of securing them.

From there, organizations can begin to think about where they might be exposed, and the ways adversaries might access this information.

This process isn't always straightforward. A company's own measure of criticality may not match the thought process of an attacker, which means that it can be tricky to understand what constitutes a "critical asset". To some attackers a generic computer is an attractive asset as it has monetary value. Social media accounts may not be considered a critical asset by the business, but they are routinely targeted by attackers. One useful place to start is with the regulator who will often mandate this themselves. PCI compliance around payment card information is one example of this, but healthcare, pharmaceuticals, financial services, transport, energy and environmental services all have regulations that apply.

Four Steps to Reducing Digital Risks

Step 2: Understand the Threat

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 (tactics techniques and procedures), motivations, and the opportunities the threat may exploit. The broad discipline of CTI, if executed effectively, can provide useful insight into these threats. A recent shift towards a strategic focus on attacker behavior through frameworks like MITRE ATT&CK,¹⁷ provide a common language that is giving us promising insight into how defenses can be aligned to real-world threats. Collecting and understanding behavior data across a broad range of threat actors can give highly useful context to those responsible for protecting businesses. Either in deducing the likely next step in an observed attack, or in supporting decision making in putting in place defenses.

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, targeting the lowest hanging fruit or the shortest path to success. Adversaries will make use of online exposure; using exposed credentials to conduct account takeovers, assessing the digital footprint, impersonating the brand to launch phishing attacks, and exploiting vulnerabilities in external infrastructure.

Organizations need to reduce the opportunities available to these threats, thereby reducing digital risk. The first stages of any attack use reconnaissance techniques to reveal the most effective path to exploiting the target. Professional red teams have developed techniques based upon OSINT (Open Source Intelligence), hostile reconnaissance techniques to enumerate their targets without touching a computer to prepare an effective campaign.

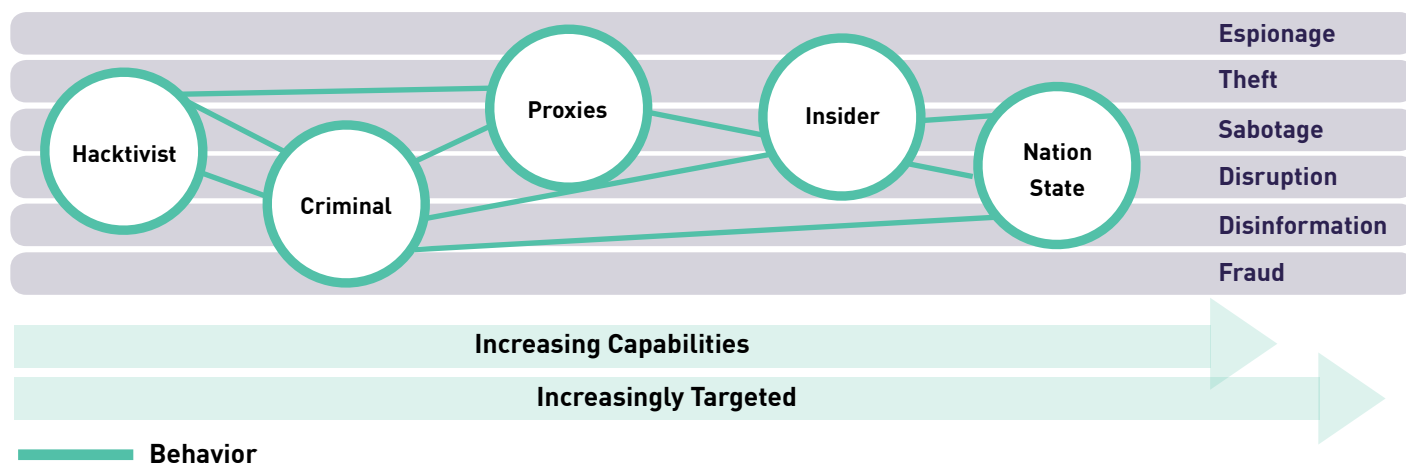


Figure 4: Threat actor spectrum

Four Steps to Reducing Digital Risks

Step 2: Understand the Threat

Threat Models: Focus on What Attackers Want

The term “threat model” can be deceptive, as it’s less about the “threat” and more about you as an organization in relation to that threat. Threat modelling, as defined by OWASP, “works to identify, communicate, and understand threats and mitigations within the context of protecting something of value”.¹⁸ It is a way of structuring thinking around what critical assets an organization has and which are the likely threats to that organization.

Different threat actors have different goals. FIN7, for example, went after payment card data and non-public information.¹⁹ The GRU sought emails, analytics and internal documents.²⁰ The Syrian Electronic Army (SEA) targeted social media accounts.²¹ The Dark Overlord seeks customer data, primarily of medical and dental practices, in order to extort the victim company.²²

Consider that data might serve as a stepping stone as part of another campaign. For example, gaming organizations were targeted for their cryptographic material, which was used to sign certificates in later attacks. It is, therefore, worth keeping in mind that an organization may be a target for the sole reason of their connectivity into other environments.

Applying MITRE ATT&CK to Your Exposure

Organizations can make use of frameworks such as MITRE ATT&CK, which provide promising ways to describe attacker behavior through observed tactics, techniques, and procedures (TTPs). Combining this behavioral information with threat models, organizations can then consider why a particular type of threat actor would target the organization, what they would hope to gain, and what their goals would be.

MITRE is compiling a heatmap of commonly observed behaviors. At time of writing, be on the lookout for campaigns that employ the following top 3 TTPs across MITRE ATT&CK and Pre-ATT&CK which are relevant to online exposure:

1. [Valid Accounts](#). Consider how many of the organization’s credentials have already been exposed and could be used in an account takeover.
2. [Exploit Public-Facing Application](#) is a common TTP for adversaries. Combining this with an analysis of the attack surface will give a good indication of risk.
3. Many campaigns will involve a reconnaissance stage, where [People Weakness Identification](#) and [Technical Information Gathering](#) will be relevant.

There are many more TTPs employed by threat actors. However, by understanding these three and protecting against the exposure of data that could enable them, it can really reduce an organization’s risk profile.

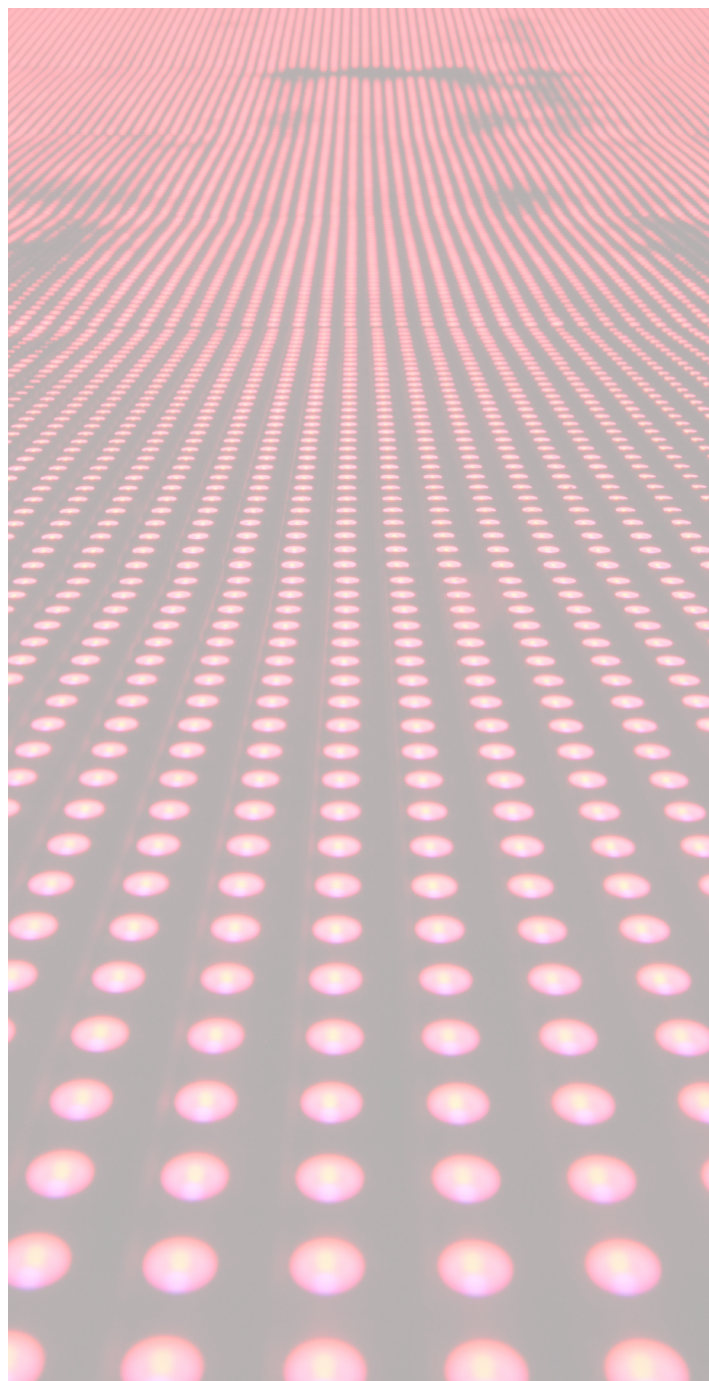
Four Steps to Reducing Digital Risks

Step 2: Understand the Threat

Criminals are Also “Going Digital”

Adding further complexity, adversaries are similarly “going digital”; online criminality is experiencing its own digital transformation revolution manifested largely by:

- The speed at which compromise methods and attacker behaviors are distributed as tools.
- The evolution of the criminal eco-system which is migrating away from the older online forum models towards more distributed, private channels.²³
- The availability of tools and services that lower the skills bar for the attackers to effectively carry out attacks.
- The almost entrepreneurial nature of organized online crime which aims to scale the threat to maximize profits.
- The innovative trust models that continually evolve, creating ‘trust among thieves’ that enable the fencing of stolen information, or the anonymized payment of ransoms.
- The innovative methods for disrupting the identity of organizations and their critical services.



Four Steps to Reducing Digital Risks

Step 3: Free Tools to Monitor for Exposure

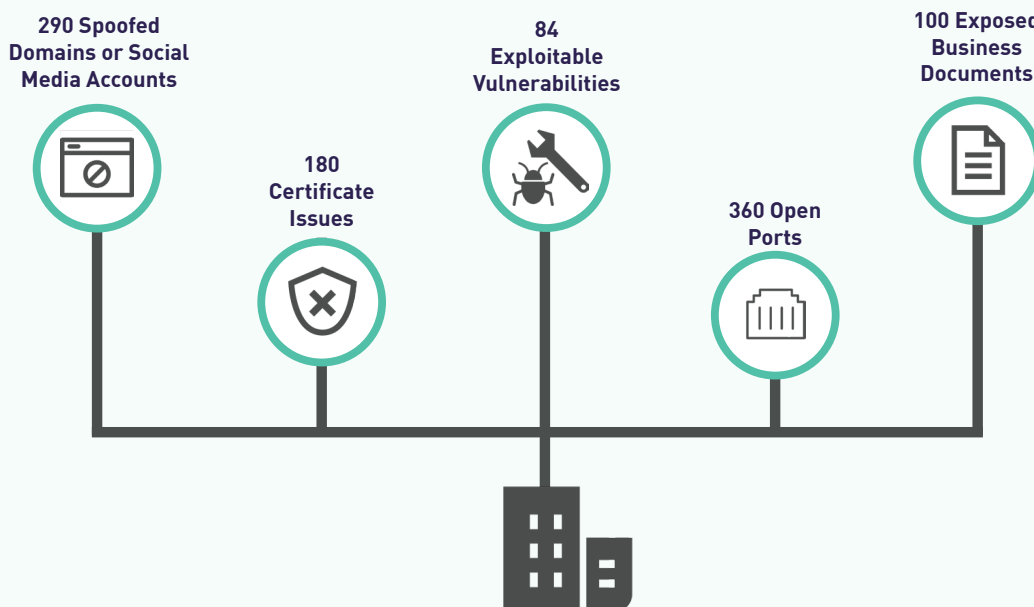
As previously discussed, organizations are no longer in control of where their data and critical assets reside. To detect exposed assets, organizations should consider a wide range of sources and prioritize those that are most relevant to them across the open, deep, and dark web, including Git repositories, paste sites, social media, file-sharing sites, criminal forums, dark web pages, and misconfigured online file sharing services.

Detecting exposed assets can be a daunting task. To give a sense of scale, Figure 5 illustrates the typical exposure of a mid-sized organization served by Digital Shadows.

To make this slightly less daunting, on the following pages we've broken this down into easy, medium, and hard methods to monitor for exposure. Note there is no need to start by diving into criminal forums; there's plenty to do that's easier and will provide you good visibility and a good starting place for a risk management program.

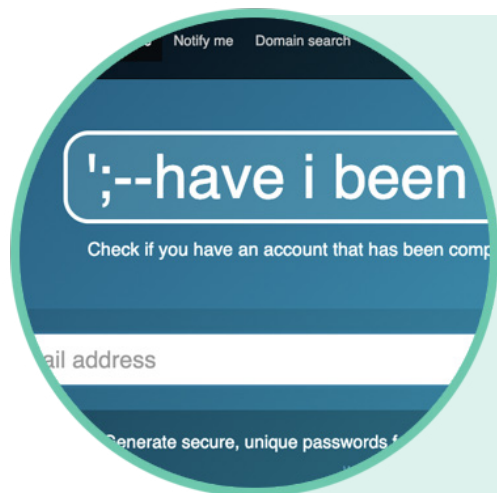
One important distinction exists between services and tools. Services may provide a monitoring capability, but tools will need to be run periodically and comparisons made from previous results sets in order to be effective.

Figure 5: Typical Exposure of a Mid-Sized Organization



Four Steps to Reducing Digital Risks

Step 3: Free Tools to Monitor for Exposure



Exposed Employee Credentials

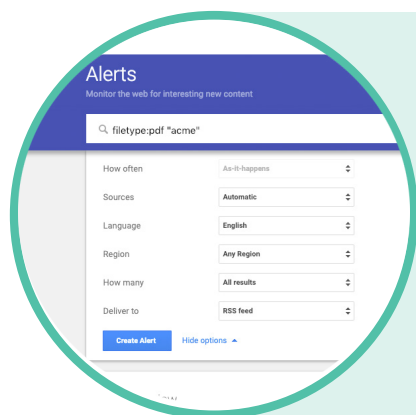
[Have I Been Pwned](#) provides a free way to get alerted to the latest instances of credential exposure. With their Enterprise version, you can register your company domain, too. Note, this will alert you to instances of exposure, but not the passwords themselves.

Difficulty: Easy

Exposed Sensitive Documents

Google hacking (Site:s3.amazonaws.com “confidential” AND “company name”). [Google hacking database](#) and [Bishop Fox's Diggity Project](#) both provide excellent guides. An excellent set of books by Johnny Long can take you through the basics. For those unfamiliar with Google Hacking, [Yandex](#) provides intuitive drop-downs to filter by document type. In fact, it's useful to not rely on a single search engine, as results will vary.

Difficulty: Easy



Get Alerted

Set up and input these Google hacks into [Google Alerts](#) to be notified if data is exposed. For example, “site:pastebin.com” AND “acme.com” will show you anytime your company domain is posted on Pastebin and Indexed by the Google search engine spider.

Difficulty: Easy

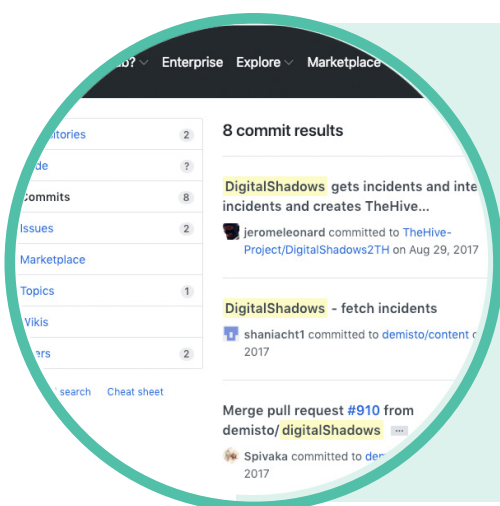
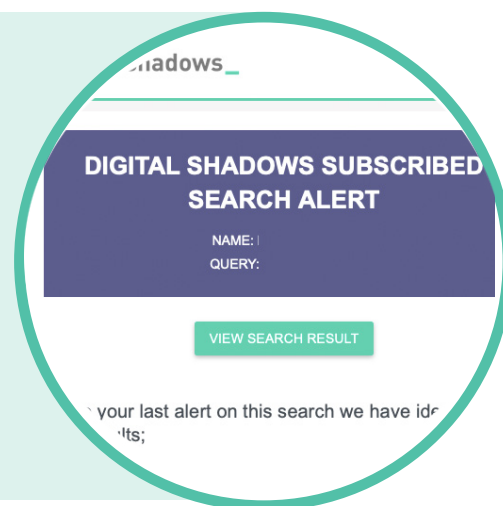
Four Steps to Reducing Digital Risks

Step 3: Free Tools to Monitor for Exposure

Customer Accounts

Get insight into data traded across criminal forums, marketplaces and paste sites with [free access to SearchLight](#) for 7 days. This can help identify exposed credentials, as well as search criminal forums for counterfeit goods.

Difficulty: Easy



Sensitive Code Exposure

Search across [GitHub](#) for your company name and any identifiers, which can help to show if any developers or third parties are exposing data, such as AWS keys or proprietary code.

Difficulty: Easy

Leverage Existing Solutions

Ask your marketing or brand management teams what they use for monitoring social media and see if they will donate a spare license. An extra seat to these tools can provide a useful insight into what is being discussed about your organization online.

Difficulty: Easy



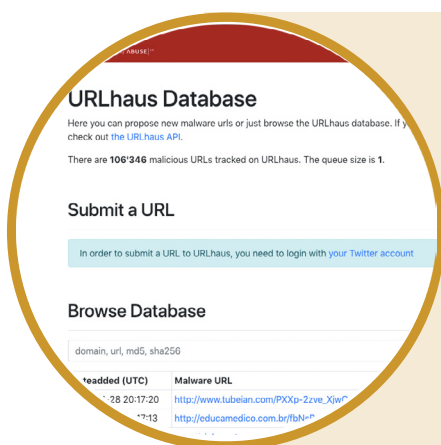
Four Steps to Reducing Digital Risks

Step 3: Free Tools to Monitor for Exposure

Phishing Sites

For online brand security, you can detect permutations of your domain with [DNS Twist](#). Taking a slightly different approach is the [Phishing Catcher](#) by X0rz. If you're using Kali Linux, consider using [URL Crazy](#) to generate different types of domain spoof. As you can imagine, there are plenty of permutations for domains and many different techniques. We've provided a more detailed overview of these in Appendix 1: Fuzzing Approaches.

Difficulty: Medium



Phishing Sites (2)

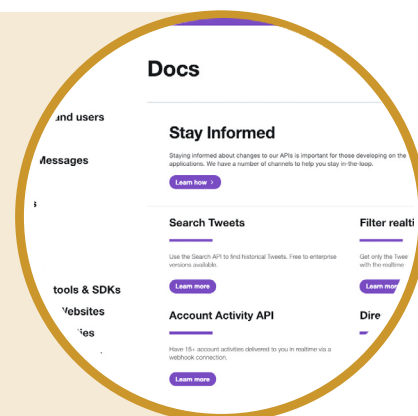
Look for known phishing URLs. If you're in financial services or retail, consider pulling information from [urlhaus.abuse.ch](#), which has some really good data on domains registered as part of spam and other campaigns.

Difficulty: Medium

Spoof Social Media Accounts

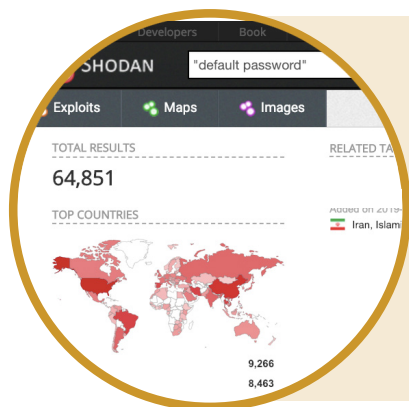
Use the [Twitter API](#) to pull in data specific to your key terms, this can help to detect spoof social media accounts, as well as inadvertent exposure on Twitter.

Difficulty: Medium



Four Steps to Reducing Digital Risks

Step 3: Free Tools to Monitor for Exposure



Infrastructure Weaknesses and Exposure

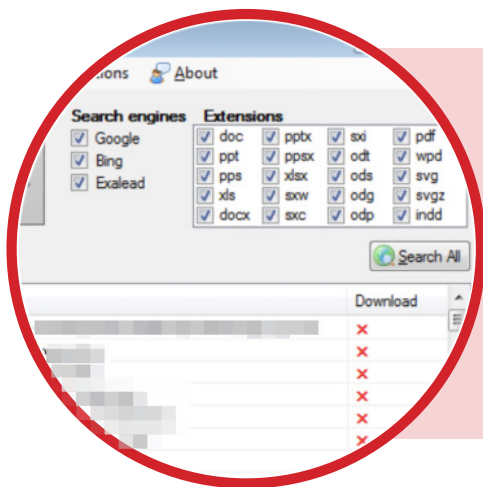
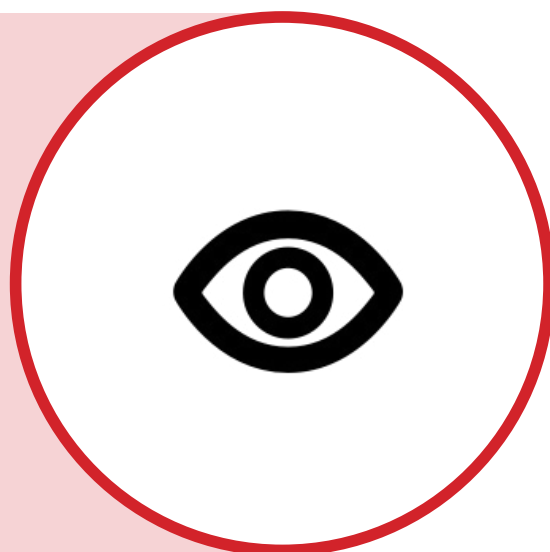
Look for misconfigured databases, servers, and devices with [Shodan](#) and [Censys](#). Check for weak or expiring certificates on your infrastructure with [Testssl](#).

Difficulty: Medium

Develop “Attacker Eye view” of Infrastructure

Developing a map of the technical attack surface of both your organization and your third parties can pay dividends. This can be done almost entirely passively if done correctly. For experienced users, free tools are available via the Kali Linux distribution for information gathering tools, [Paterva’s Maltego](#) community edition, and OSINT frameworks such as [Recon-ng](#). Michael Bazell’s [Buscador](#) tools can also help build up a picture of this attack surface.

Difficulty: Hard



Exposed Documents

Discover exposed documents and investigate the contents and metadata with the [Fingerprinting Organizations with Collected Archives](#).

Difficulty: Hard

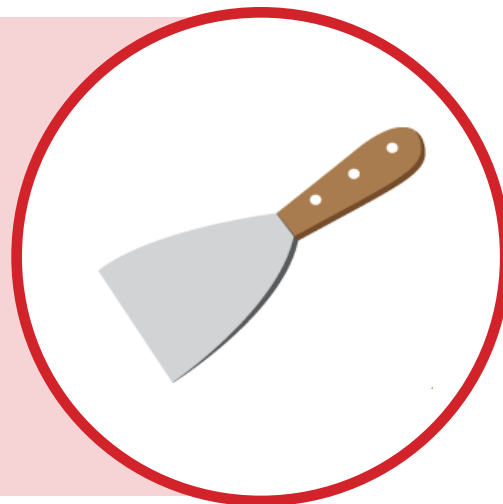
Four Steps to Reducing Digital Risks

Step 3: Free Tools to Monitor for Exposure

Scraping Sites

Use [Scrapy](#) or [BeautifulSoup](#) to scrape sites of interest. Take caution with scraping criminal or nefarious sites, as you'll need to take into account new infrastructure and legal ramifications.

Difficulty: Hard



Gated/Closed Sources/HUMINT

Develop a Closed Source capability to gain access to hard-to-reach sources. This is not something to be rushed. Note that there are plenty of third parties that provide this capability if you wish to outsource (including, but not limited to, Digital Shadows).

Difficulty: Hard



Four Steps to Reducing Digital Risks

Step 4: Mitigation Strategies

Detecting exposure and understanding the threat is important, but if you can't protect against that threat, the value is minimal. Taking action to resolve or mitigate risks is critical. A risk without a mitigation strategy is a potentially futile endeavor after all.

When considering mitigation strategies it's worth thinking about immediate (tactical), responses that may be done on an ongoing basis (operational) and those that may involve investment or directional influence (strategic), as illustrated in Figure 6.

Of course, there's not always an immediate response that organizations can take, but it can tie into broader defenses or inform more strategic investment in defenses. For example,

an organization that has identified large numbers of exposed credentials may look at implementing Multi Factor Authentication (MFA) and change timeout strategies across those that do not implement it. Similarly, if employees are discovered backing up their work on home computers with misconfigured devices, consider providing more effective storage solutions or working on the security culture within the organization.

By understanding where assets are exposed, their value to attackers, and how attackers target this data, organizations can make better decisions about their defenses.

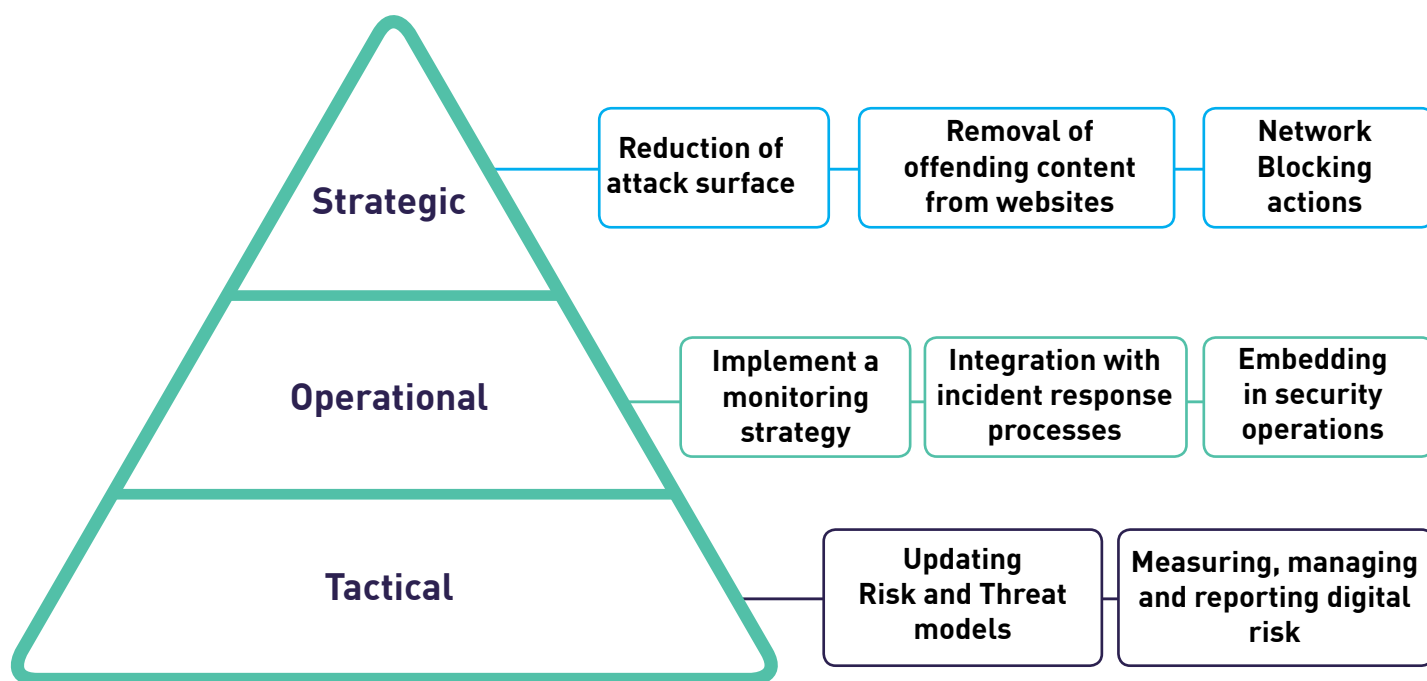
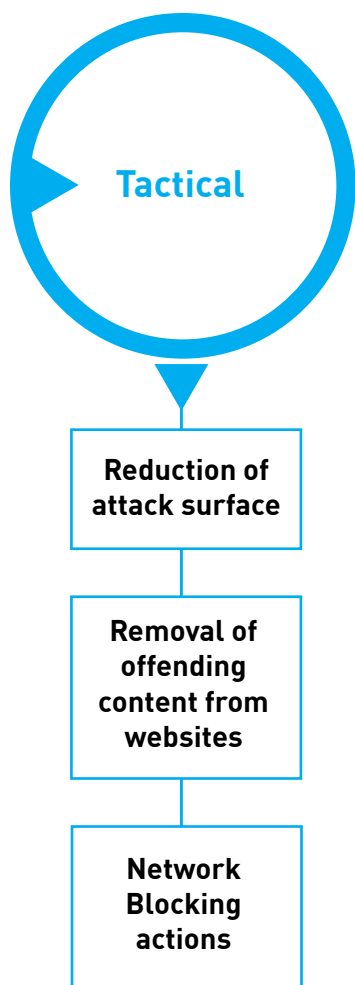


Figure 6: Three tiers of mitigation strategies

Four Steps to Reducing Digital Risks

Step 4: Mitigation Strategies



Examples of Tactical Mitigations

Reduction of attack surface

We always advise customers to build an “attacker’s eye view” of their technical infrastructure. Using the tools above it’s possible to enumerate computers, network, and services associated with the organization. Step one in reducing risks should be to retire and deprecate services wherever possible. The fewer services online, the less there is to attack and the lower the risk. This is often a process of collaborating with colleagues across the business. Compelling arguments for closing down a service can be presented if the identified asset is vulnerable and a threat can be shown to be exploiting the same issue elsewhere. The organization’s risk appetite should drive it to decommission content quickly.

Removal of offending content from websites

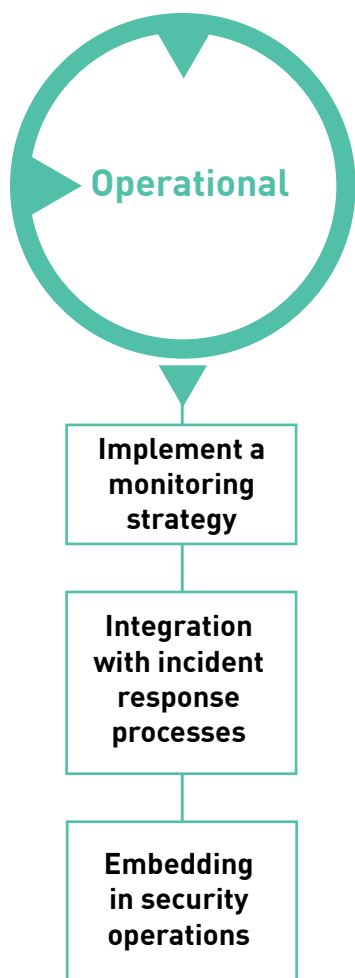
Today social media sites, ISP abuse notification processes, and legal notices offer a range of tools to companies to remove offending content from the internet. These may include the complaints and trademark procedure, or via a notification of breach of terms. Web hosts and Web platforms alike have developed numerous means of registering a complaint about content. Takedown of material must be assessed on a case by case basis, and in some cases attempts to remove may be futile (for example on a criminal site). In our experience, it is possible to takedown a large proportion of offending content.

Network Blocking actions

For organizations fortunate enough to have a ticketing system or, even better, security orchestration and automation – then take common use cases for commonly observed behaviors and implement blocking actions. Be careful, you do not want to block Google, but it should be possible to look at threats such as squatted sites or phishing attempts and either block the domain, IP or offending content using existing proxy, firewall or perimeter controls. This should at least have a positive impact on the user community.

Four Steps to Reducing Digital Risks

Step 4: Mitigation Strategies



Examples of Operational Mitigations

Implement a monitoring strategy

Looking at tools one tool at a time and one view at a time is a good start, but operationalizing that to get an ongoing perspective and to feed into detection strategies is a much better approach. You can build this out by use case; start with domain monitoring then add more capabilities over time. As one source is mastered add another to build confidence in the level of coverage, or at least know which parts of the digital risk picture are being managed.

Integration with incident response processes

Alerts to potential digital risks are just as important as any other type of security event. Steps that apply to digital risks include: determining what risks to cover, putting a detection strategy in place, conducting investigations, containing risks, removing issues, and review. Digital risks should be triaged and managed alongside existing incident management and forensics strategies.

Embedding in security operations

Security operations teams spend much of their time doing important and good work detecting anomalous behaviors on network or on premises. As they detect incidents that result from external risk, these teams consider context. The type of context obtained from understanding digital risks can be valuable. For example the hosting history of a squatted domain, the status of password leakage for a given account, historic threat actor behavior and tools that can support tier 2 and 3 investigations are all critically important. Security operations can benefit by continually maintaining a map of the “attack surface” that is exposed online. Operationalizing this process has long term benefits to reducing risk.

Four Steps to Reducing Digital Risks

Step 4: Mitigation Strategies



Examples of Strategic Mitigations

Updating Risk and Threat models

"All models are wrong but some are useful," as the British statistician George EP Box once said. The models that record and estimate an organization's risk posture will always be subject to some degree of inaccuracy, but in risk reduction the deeper the understanding of the inputs the more accurate and the less room for error in the model. Updating risk assessments to account for critical digital assets, and accounting for third party and supply chain risk provides significant value. Comparing risk models against what incidents were actually seen also pay dividends.

Measuring, managing and reporting digital risk

If teams can get a reasonably complete view, then they can feasibly measure the level of incidents and exposure relating to an organization. Teams must balance detection strategies to ensure that coverage can give a more complete view of risks. Reporting frequency and trending along with integration into incident management offer opportunities to communicate to business stakeholders the value of a digital risk management approach, justifying investments in tools and processes.

Building Maturity in Digital Risk Protection

Build Versus Buy

The concept of Digital Risk has been discussed since 2010,²⁴ but increasing reliance on online digital technologies has caused organizations to look at specifically investing in capabilities that protect against digital risks.

We have already in this paper proposed examples of tooling that can support organizations seeking to understand digital risks. This is the start of the journey, since technology alone will never be the silver bullet. Integration with skills, process, culture, and investment in resources also all play a role.

Build versus Buy

In putting together an approach to addressing digital risk an organization may want to compare building internal capability versus going out to seek a solution from the vendors in the market. When considering embarking on an internal strategy it is worth working out some of the engineering and operational considerations.

Expertise and retention of talent. Monitoring and managing digital risks will need someone to act as recipient of alerts, and someone to action issues that have been discovered. Wherever possible an organization will need to leverage existing processes and resources, but if this is to be built internally, resource to develop, maintain and operate a capability is key.

When it breaks, who fixes it, and what is the allocation of resource? The internet is constantly changing as are the sites. If data collection is performed on specific sites, they will alert for

changes to APIs and interfaces. This means that infrastructures require regular monitoring to confirm what worked yesterday still works today.

Relevance - volume of false positives and triage.

Quite a few of the tools available today do a good job of covering content, but the downside of that is that what is detected may be a false positive. In our experience different content types generate different signal to noise ratios. Working out how to deal with the false positives in an efficient manner to get to the valuable results is an important consideration.

Ensuring a consistent service level. The internet moves apace and the frequency with which a tool is run or a query performed can have an impact on the time to detect a risk. Any service needs to consider what a baseline for coverage is.

Coverage. The Web and the various services on it is large. Covering main services is a core concern, but sometimes risks come left of field from a source or service that was previously not monitored. Even relatively popular sources such as Twitter present interesting engineering challenges as any organization that has processed the Twitter firehose knows. Working out acceptable coverage for risks is an important step.

Ensuring there is a suitable legal framework for monitoring activities. It's important to make sure that activities that are carried out conform with national and international rules concerning copyright, privacy, computer misuse legislation, in addition to complying with the various terms and conditions of the sources of data.

Building Maturity in Digital Risk Protection

Maturity is About More Than Tooling

Unfortunately, there is no silver bullet for building maturity. Required tools include detection, integration, and remediation. These enable organizations to detect risks across the open, deep, and dark web; correlate external and internal information; and create workflows for automating responses. These tools may be built internally or purchased externally. Whichever approach taken, this paper provides free ways to get started and progress over time.

Analysts are already defining maturity models for digital risk. While this topic is relatively new, we can start to think about what defines a mature organization. We will shortly publish more on this topic, but we can begin considering factors like reporting, quantification, leadership, organizational cohesion, and process documentation.



Reporting

Because of a lack of reporting tools and relevant frameworks, communicating these risks to the Board and C-Level executives has been challenging. Reporting must be both vertical (to the C-Level and Board), as well as horizontal (communicating risk across the departments).



Organization Cohesion

While no leadership is bad, it's often a case of too many stakeholders operating in silos. Security, intelligence, fraud, IT, marketing, and legal teams all have their own approaches to managing risk. The extent to which this is joined up in one partnership to manage digital risk, however, varies significantly.



Risk Quantification

There are many different risk management frameworks and processes, such as NIST,²⁵ ISO/IEC 27005,²⁶ and Factor Analysis of Information Risk (FAIR)²⁷ that can help the quantification of risk. None of these are mutually exclusive, and organizations can combine frameworks for the most effective approach.



Process Resilience

Finally, with these processes in place, new processes must be documented, trained, rehearsed, and culturally reinforced. The optimal level of maturity will look to continually identify gaps, update processes and tooling, and reflect those changes in the documentation.

Building Maturity in Digital Risk Protection

Getting Started

This guide provides advice and free tools that practitioners can turn to. Some can be done next week, some next year, and some will be aspirational.

To assist, we've opened up SearchLight to use for 7 days. This will give you an idea of your exposure across the open, deep, and dark web, as well as insight into threat actors and their campaigns.



1. 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.



2. Intelligence-led Learning

How ready is your team to deal with the types of digital risks happening right now? Read more about how [our partnership with hands-on labs provider Immersive Labs](#) is helping our customers to reduce a mean time to learn about digital risk.



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

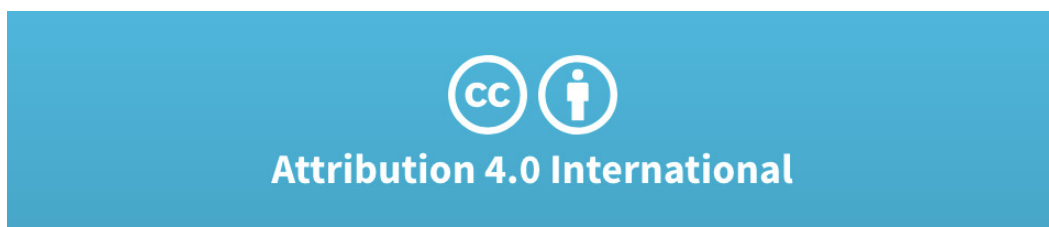
1. Digital Shadows, Digital Risk: The Critical Missing Part of Overall Risk
2. Gartner, CEOs and CIOs Are Seeking Digital Risk Leaders, <https://blogs.gartner.com/john-wheeler/ceos-and-cios-are-seeking-digital-risk-leaders/>
3. Kaspersky, Businesses and personal data, <https://www.kaspersky.com/blog/data-protection-report/23824/>
4. Forrester, The Forrester New Wave™: Digital Risk Protection, Q3 2018, <https://go.forrester.com/blogs/blog-digital-risk-protection-drp-wave-18/>
5. Accenture, 2018 State of Resilience, https://www.accenture.com/t20180416T134038Z__w__/us-en/_acnmedia/PDF-76/Accenture-2018-state-of-cyber-resilience.pdf
6. Ibid
7. <https://www.fairinstitute.org/fair-risk-management>
8. Digital Shadows, When Caring in Not Sharing, <https://www.digitalsadows.com/blog-and-research/when-sharing-is-not-caring-over-1-5-billion-files-exposed-through-misconfigured-services/>
9. <https://www.techrepublic.com/article/too-smart-to-fall-for-a-spear-phishing-message-think-again/>
10. <https://www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and>
11. <https://www.mediapost.com/publications/article/328474/online-payment-fraud-to-reach-48b-study.html>
12. Ibid
13. Ponemon Institute, Measuring & Managing the Cyber Risks to Business Operations , http://static.tenable.com/marketing/research-reports/Research-Report-Ponemon-Institute-Measuring_and_Managing_the_Cyber_Risks_to_Business_Operations.pdf
14. <https://www.synopsys.com/blogs/software-security/equifax-apache-struts-cve-2017-5638-vulnerability/>
15. Ponemon Institute, Measuring & Managing the Cyber Risks to Business Operations , http://static.tenable.com/marketing/research-reports/Research-Report-Ponemon-Institute-Measuring_and_Managing_the_Cyber_Risks_to_Business_Operations.pdf
16. SANS Institute, The Attack Surface Problem, <https://www.sans.edu/cyber-research/security-laboratory/article/did-attack-surface>
17. <https://attack.mitre.org/>
18. OWASP, Threat Modelling, https://www.owasp.org/index.php/Application_Threat_Modeling
19. Digital Shadows, Mitre ATT&CK™ and the FIN7 Indictment: Lessons for Organizations, <https://www.digitalsadows.com/blog-and-research/mitre-attck-and-the-fin7-indictment-lessons-for-organizations/>

Endnotes

20. Digital Shadows, Mitre ATT&CK and the Mueller GRU Indictment, <https://www.digitalsadows.com/blog-and-research/mitre-attck-and-the-mueller-gru-indictment-lessons-for-organizations/>
21. 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>
22. Digital Shadows, The Dark Overlord, <https://www.digitalsadows.com/blog-and-research/thedar-koverlord-out-to-kickass-and-cash-out-their-data/>
23. Digital Shadows, Seize and Desist, https://info.digitalsadows.com/SeizeandDesistReport-WebsiteNav_Reg.html
24. Lloyds, Managing digital risk, [https://www.lloyds.com/~media/lloyds/reports/360/360-digital/lloyds_360_digital_risk_report-\[2\].pdf](https://www.lloyds.com/~media/lloyds/reports/360/360-digital/lloyds_360_digital_risk_report-[2].pdf)
25. [https://csrc.nist.gov/Projects/Risk-Management/Risk-Management-Framework-\(RMF\)-Overview](https://csrc.nist.gov/Projects/Risk-Management/Risk-Management-Framework-(RMF)-Overview)
26. <https://www.iso.org/standard/75281.html>
27. <https://www.fairinstitute.org/fair-risk-management>

Appendix 1

Copyright details



You are free to:

Share — copy and redistribute the material in any medium or format.

Adapt — remix, transform, and build upon the material for any purpose, even commercially.

This license is acceptable for Free Cultural Works.

The licensor cannot revoke these freedoms as long as you follow the license terms.

Under the following terms:

Attribution — You must give appropriate credit, provide a link to the license, and indicate if changes were made. You may do so in any reasonable manner, but not in any way that suggests the licensor endorses you or your use.

No additional restrictions — You may not apply legal terms or technological measures that legally restrict others from doing anything the license permits.

Notices:

You do not have to comply with the license for elements of the material in the public domain or where your use is permitted by an applicable [exception or limitation](#).

No warranties are given. The license may not give you all of the permissions necessary for your intended use. For example, other rights such as [publicity, privacy, or moral rights](#) may limit how you use the material.

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_