Digital Risk Management

Identifying and Responding to Risks Beyond the Boundary

digital shadows_

Executive Summary

Organizations' digital footprints are expanding and changing at an overwhelming rate. Employees, suppliers and other third parties are unknowingly exposing sensitive information. This information can leave organizations exposed.

Attackers are using this information to exploit organizations and launch their attacks. While adversaries are becoming more sophisticated, they too leave their footprints in online forums, market places and chat rooms.

Traditional security solutions that focus on the perimeter can't address these risks by themselves because the boundary is disappearing. By monitoring and managing their digital footprint and those of their attackers, organizations can manage their external digital risks.

External digital risk management allows organizations to not only continuously monitor for risks across the open, deep and dark web, it also enables organizations to quickly respond to and mitigate these risks.

Table of Contents

Executive summary 02
Organizations unwittingly expose sensitive information 04
Attackers exploit organizations' digital shadows 05
Digital risk management minimizes the risks of digital shadows 06
Cyber threat 06
Data leakage 07
Reputational damage 08
Digital risk management needs humans in the loop 09
Six tips to manage your digital risk 10
End notes 11

Organizations unwittingly expose sensitive information

We live in a complex world, which has transformed the way we do business. Social media, mobile computing and cloud services have increased the ease and speed of communication, while simultaneously reducing the cost. This digital disruption has provided new ways to deliver services and, in so doing, created new risks and challenges. Business is occurring beyond the firewall and the digital footprints of organizations are expanding and changing at an unprecedented rate.

Digital Footprint - the information about an organization or individual that exists on the Internet as a result of their online activity.

Digital footprints are also dynamic; they are constantly evolving and exist across a wide range of online sources. Much of an organization's digital footprint is not controlled by the organization itself; employees, suppliers and other third parties are unknowingly exposing sensitive information.

While third parties and supply chain partners enable business, they also introduce risk. The PNI Photo hack that led to compromises of online photo services at CVS, Costco and Sam's Club[1] illustrates these risks. Organizations need to understand their supply chain risk, including what sensitive information they have access to, and where that is being shared online. A failure to understand where their data exists can cause real risks for organizations. The Yahoo breaches illustrate the risks associated with mergers and acquisitions. Data breaches can have serious financial implications.[2]

Further risks emerge from the use of corporate email addresses for personal accounts. A recent Digital Shadows study found that for 97 percent of the largest 1,000 organizations, breached data includes employee work credentials.[3] Adversaries can use this for account takeovers, post-breach extortion or credential stuffing.

Shadow IT is another area beyond the control of organizations. A report by Frost & Sullivan found that more than 80% of survey respondents admit to using non-approved applications in their jobs.[4] With so many ways for information to leak out, it is little surprise that organizations struggle to control and secure their assets.

These examples show that there is a lot of potentially sensitive information that exists beyond an organization's control that can leave them exposed. The challenge for leaders is to pull their heads out of the sand, identify these instances and find new ways to manage this digital risk.

Attackers exploit organizations' digital shadows

Most of an organization's digital footprint is benign; digital footprints enable business. However, there is a subset called a 'digital shadow' that puts organizations at risk. These digital shadows are inadvertently giving attackers opportunities to exploit organizations.

Digital Shadow - exposed personal, technical or organizational information that is often highly confidential, sensitive or proprietary.

An organization's digital shadow can take many forms. It might include:

- An insider offering to sell confidential company information on a dark web market place;
- Employees publicly sharing their private encryption keys on code-sharing sites;
- Administrator credentials for the corporate website exposed in clear-text on a paste site by a penetration testing organization that had inadvertently synchronized their account;
- Personal details of an executive that affords vital information for a spear-phishing campaign;
- Floor plans of an organization's headquarters campus;
- Systems information publically accessible.

All of this exposed information gives attackers the upper hand and can constitute a risk to organizations.

At the same time, threat actors are also leaving behind their own digital shadows:

- Conversations about their targets;
- The details of their motivations;
- The infrastructure they leverage to launch attacks;
- The infrastructure they use to conduct commerce;
- Artifacts from the tools they use to accomplish their goals.

It's possible for defenders to observe the attacker's digital shadows to gain insights and plan their mitigation strategies.

Digital risk management minimizes the risks of digital shadows

Risk is a well-developed concept within cybersecurity. The National Institute of Standards and Technology (NIST) defines risk as: "A function of the likelihood of a given threat-source's exercising a particular potential vulnerability, and the resulting impact of that adverse event on the organization."[5]

NIST goes on to define the field of risk management as: "The process of identifying risk, assessing risk, and taking steps to reduce risk to an acceptable level."[6] Applied to cyber security, we can define the field of external digital risk management as:

> *"The process of identifying, assessing, and taking steps to reduce external digital risk to an acceptable level. External digital risk management considers: 1) cyber threats 2) data leakage and 3) reputation risks."*

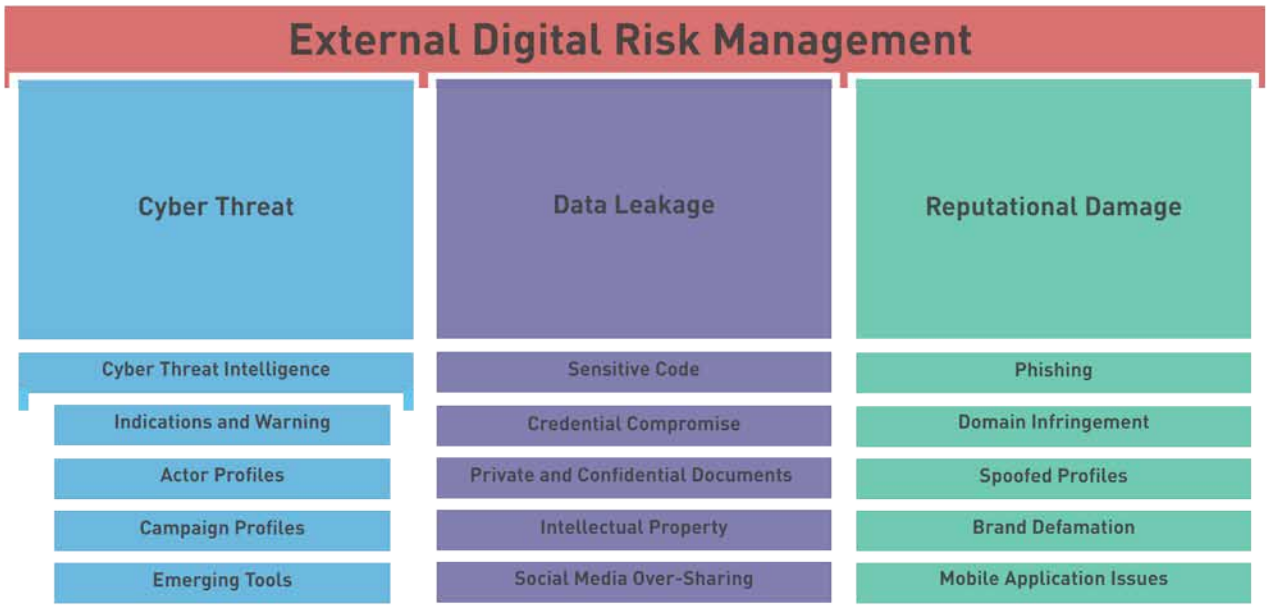

Figure 1: External digital risk management overview

Cyber threat

Understanding cyber threats requires a threat intelligence capability and consists of these four main areas, as shown in Figure 1:

1. **Indications and warnings.** Leverage threat intelligence to get advance information regarding an adversary's planned activities. This can include being named on a hacktivist target list or being discussed on a known criminal forum.
2. **Actor profiles.** Profile actors' tactics, techniques, and procedures (TTPs) in order to better understand how an attacker might target you and what tools they are likely to use. This can be used to stack up an organization's defenses to the threats they are likely to face.

3. **Campaign profiles.** Understand the threat actor's tools, target geographies and target industries. This can include the examination of malcode or the analysis of a new phase in a hacktivist campaign. This allows organizations to be better prepared for developing threats.
4. **Emerging Tools.** Track new tools being developed and shared on the dark web and criminal forums. This can include the inclusion of new CVEs in an exploit kit, which can help to prioritize patching procedures.

The value of threat intelligence is directionally proportional to how tailored it is to an organization. For external digital risk management to be effective, a threat intelligence doctrine should be applied. In applying the intelligence doctrine to the concept of cyber threat, organizations can methodically understand what they care about, create collection plans, identify collection gaps and ultimately deliver tailored intelligence. Digital Shadows' process is shown in Figure 2.

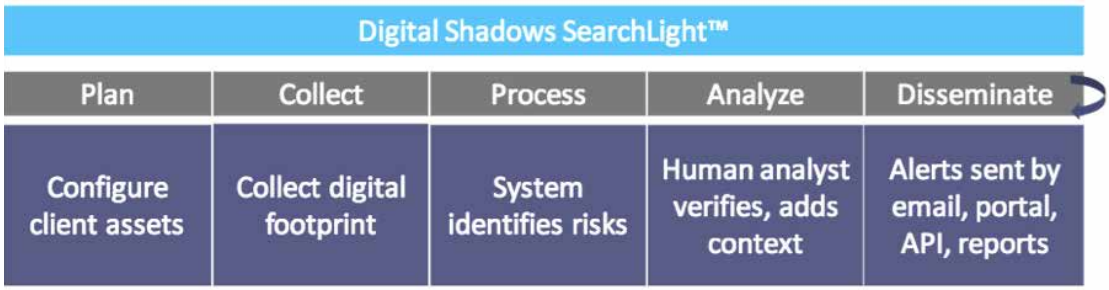

Figure 2: Digital Shadows SearchLight™ flow, mapped to the intelligence cycle

Despite a maturation of the cyber threat intelligence marketplace, all too often it is still synonymous to receiving generic, automated threat feeds that consist of large amounts of potential indicators of compromise, that quickly become indicators of exhaustion. This is simply not useful for any organization.

Data Leakage

Leaked information can provide valuable clues for adversaries. Here are five main areas that contribute to data leakage risks:

1. **Sensitive code.** Sensitive code and private encryption keys that are publically available on code-sharing sites. This can allow attackers to better tailor their attacks to an organization.
2. **Credential compromise.** Employee credentials are exposed in third-party breaches. These credentials are then used by attackers for account takeovers, spam lists, credential stuffing, spear-phishing and post-breach extortion.
3. **Private and confidential documents**. Sensitively marked documents are inadvertently leaked out by partners and employees. As well as opening up organizations for corporate espionage, it also allows attackers to weaponize legitimate-looking documents and launch targeted attacks.

4. **Intellectual property.** Intellectual property is freely available and shared online, inadvertently and by malicious actors. This can leave organizations vulnerable to corporate espionage. But if an organization is aware that a new design, for example, has been leaked early, they can get it removed and mitigate accordingly.
5. **Social media over-sharing.** Employees reveal information about security procedures, software and hardware. This information can be used by attackers as they perform reconnaissance on an organization, seeking out specific software to exploit.

This information leaves organizations vulnerable to corporate espionage and competitive intelligence. Worse still, criminals and hostile groups can exploit this leaked data to find the organization's weak points and launch targeted cyber-attacks. By monitoring for this leakage, organizations can gain an awareness of where they are exposed and remediate.

Reputational Damage

It is easy for organizations to be unaware of how their brands are being used online and what impact this can have on customers and employees. The top five main risks in this area are:

- **Phishing.** Phishing campaigns are conducted against organizations. Using digital risk management to identify campaigns, raises security awareness and mitigates the campaign's impact.
- **Domain infringement.** Typosquat domains are registered to spoof your websites to hijack your brand. By monitoring for typosquatted domains, organizations can protect their reputation and minimize the implications of domain infringements.
- **Spoofed profiles.** The social media accounts of key executives or brands can be spoofed. Unwary consumers might mistake these unsanctioned accounts as legitimate and get incorrect information or, worse, succumb to social engineering attacks.
- **Brand defamation.** Swift detection of online brand defamation helps to keep customers happy and prevents damage occurring to the organization's brand.
- **Mobile application issues.** Spoofed or maliciously modified applications can leave customers and employees exposed. Organizations need to identify and remove these risky mobile applications to have confidence that their employees' and customers' information is protected.

A failure to detect and remediate these risks to customers and employees can have a real business impact.

Digital risk management needs humans in the loop

In the previous section, we discussed the need to move beyond generic, automated feeds or indicators of exhaustion that fail to provide relevant information. Organizations need information that is specific to their organization, as well as their industry and geography. This is similarly true for reputational and data leakage risks.

At the same time, the dynamic nature of digital footprints means that organizations require access to a broad range of sources to ensure they understand the breadth of risks they face and none are missed.

Machine learning is a key component as technology and automation enable digital risk management, but purely automated solutions aren't able to provide the necessary context. Effective digital risk management requires human analysts in the loop to make sense of this information and make assessments.

With any human analysis, there is the added need for structured analytical techniques that reduce cognitive biases. Techniques such as Analysis of Competing Hypotheses (ACH), SWOT analyses and various forecasting methods help analysts to remove their cognitive biases.

By having an effective balance between technology and human analysts, external digital risk management can scale to ensure coverage of a broad range of sources with the right context applied in order to avoid being overwhelmed with false positives.

Six tips to manage your digital risk

While it is clear that organizations cannot scale to monitor for external digital risks on their own, there are many things they can do easily and for free. At a basic level, if you're not doing them already, consider these six things:

1.	Set Google Alerts to monitor for threats you are interested in
2.	Engage in CSIRTs and sharing communities to gain better intelligence about threats
3.	Use free tools such as Shodan.io to scan for vulnerabilities on your infrastructure
4.	Monitor for credentials that are leaked out of your organization and can leave you exposed. Troy Hunt's haveibeenpwned.com provides a great resource for this
5.	Increase employee education and awareness, particularly about privacy settings on social media, to reduce their exposure
6.	Develop and follow a list of security questions and risk assessment controls in order to effectively understand the risk presented by your supply chain

All risk management programs must include external digital risks. This not only helps to prevent and mitigate ongoing threats, but it helps organizations at a strategic level; prioritizing spending and, ultimately, making better decisions.

End Notes

1. https://www.privacyandsecurityforum.com/wp-content/uploads/2015/10/25092-Privacy-and-Data-Security-Breach.pdf

2. http://www.telegraph.co.uk/technology/2017/02/15/verizon-buy-yahoo-250m-less-deal-goes-ahead-despite-data-breaches/

3. http://info.digitalshadows.com/CompromisedCredentials-WhitePaperPage.html

4. https://www.mcafee.com/us/resources/reports/rp-six-trends-security.pdf

5. http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

6. Ibid

About Digital Shadows

Digital Shadows provides insight into an organization's external digital risks and the threat actors targeting them.

The Digital Shadows SearchLight™ service combines scalable data analytics with human analysts to monitor for cyber threats, data leakage and reputational risks. Digital Shadows continually monitors the Internet across the visible, deep and dark web, as well as other online sources, to create an up-to-the minute view of an organization and provide it with tailored threat intelligence.

The company is jointly headquartered in London and San Francisco.

digitalshadows.com

London

Level 39, One Canada Square, London, E14 5AB

+44 (0) 203 393 7001 info@digitalshadows.com

San Francisco

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

+1 (888) 889 4143

digital shadows_