Solution Showcase

The Pressing Need for Digital Risk Management

Date: July 2017 **Author:** Jon Oltsik, Senior Principal Analyst

Abstract: There is good and bad news around cybersecurity these days. The good news is that many CEOs and corporate boards no longer accept "good enough" security, and are willing to invest in best practices and leading security defenses to protect their organizations. So what's the bad news? Many organizations continue to think of cyber-risk in terms of internal network penetration rather than as a more comprehensive strategy that includes all digital assets—websites, social networks, VIP and third-party partner exposure, etc. To address these risks, CISOs and risk officers must adopt a thorough digital risk management strategy that includes monitoring, filtering, prioritizing, and responding to threats across the public Internet and dark web. Digital Shadows specializes in this area and can help organizations with digital risk mitigation.

Overview

Most CEOs and corporate boards no longer shy away from cybersecurity strategy. Rather, progressive executives now realize that cyber-risk equates to business risk. As a result, businesses are prioritizing security in 2017. According to ESG research:[1]

- 39% of organizations claim that improving cybersecurity represents the biggest **business initiative** driving IT spending in 2017.
- 32% of organizations say that their most important IT initiative for 2017 is strengthening cybersecurity tools and processes.
- 69% of organizations are increasing their cybersecurity budgets in 2017, more than any other area.

This data clearly indicates that executives are protecting valuable and sensitive digital assets and are willing to invest in technologies and initiatives to accomplish this goal.

The Emerging Challenges of Digital Risk

While many business managers now recognize the need for security investment, new business models are making cybersecurity protection a lot more difficult. Market disrupters like AirBnB, Amazon, and Uber have led the way with new digital business models using an assortment of cloud-based technologies—including email, blogs, social networks, web-based promotions, ad networks, partnerships, etc.—to attract eyeballs, personalize content, and build stronger relationships with buyers and prospects.

[1] Source: ESG Research Report, *2017 IT Spending Intentions Survey*, March 2017.

Given the visible success stories of these and other firms, many other organizations are actively emulating these digital business models. Despite the perceived business benefits, however, digitalization trends can also exacerbate IT risk. Why? Digital business models sprinkle sensitive data to a variety of locations, greatly increasing the overall attack surface. Additionally, few security teams have the right intelligence or in-house skills to monitor risks across assorted digital vehicles, websites, or the dark web.

Many organizations continue to maintain a myopic approach to cybersecurity and risk by focusing on physical solutions, security controls, and monitoring tools to prevent and detect network compromises, exploits, and malware at the perimeter or within their network alone. Given today's digital business models, this type of internally focused cybersecurity strategy is no longer enough.

Organizations Must Address Digital Risks

Executive support and increasing cybersecurity investment are a good start, but a limited cybersecurity strategy exposes organizations to lots of risks across the deep, dark, and open web, leaving them vulnerable to the potential for significant impact to their business, brand, and reputation. Given today's threat landscape, organizations need intelligence and insight to help them proactively monitor, manage, and mitigate these threats by adopting a digital risk management strategy. ESG defines a digital risk management strategy as:

A comprehensive set of risk management policies, procedures, and technologies intended to control, manage, monitor, and respond to digital risks arising anywhere on the public Internet and dark web.

A strategic digital risk management strategy should include policies and monitoring for:

- **Targeted cyber threats.** Organizations need to monitor threat intelligence to track threat actor campaigns as well as tactics, techniques, and procedures (TTPs). This knowledge can help them fine-tune controls for threat prevention.
- **Infrastructure exposure.** CISOs need a broad understanding of where their IT infrastructure may be at risk. This means monitoring dark web hacker chat sites for chatter about topics like 0-day vulnerabilities and exploit kits.
- **Data loss.** Most organizations have some controls to monitor data leakage egressiing the corporate network but fail to monitor sites for events like credentials leakage and technical leakage. This sensitive data is often shared accidentally on source code and paste sites, for example.
- **Brand exposure.** Cyber-criminals and hacktivists often use corporate brands for social engineering campaigns or digital sabotage. Addressing these risks demands continuous and comprehensive monitoring across the web.
- **VIP exposure.** Similarly, VIPs are often targets of offensives like doxing campaigns, impersonation, or phishing attacks. Countermeasures must be based on vigilant threat intelligence collection, analysis, and action.
- **Physical threats.** Occasionally digital risks can include physical threats to individuals or property. Digital risk strategies must encompass methods to detect and respond to these threats as they arise.
- **Third-party risk.** Digital risk strategies must also extend to third parties like business partners, suppliers, and customers. In fact, visible cyber-attacks like OPM and Target began with the compromise of trusted third parties so CISOs must be especially vigilant in monitoring third parties for potential hazards.

Digital risk management starts with extensive analysis of public and commercial threat intelligence of cyber threat activities across the dark web and public Internet, but data analysis is not enough on its own. Rather, organizations must be able to

act upon new and unanticipated risks as they arise. Therefore, a thorough digital risk management program must also include:

- **Operational considerations.** These include day-to-day details about who will receive threat intelligence, the tools used for analysis, and processes needed for action. For example, discovery of physical threats may require cybersecurity teams to reach out to law enforcement, while remediating risks may require an organization to collaborate with third-party partners. Even internal actions like changing network configuration settings may involve cooperation between security and IT operations groups.

- **Strategic considerations.** Some threats like a potential DDoS attack or a physical threat to company facilities could result in extensive financial damages. A digital risk management strategy must include formal escalation and remediation processes for rapid crisis management and risk mitigation.

Digital Shadows Provides a Pragmatic Way to Address Digital Risk

Many CISOs recognize the need to transition from perimeter-focused cybersecurity to a more holistic digital risk strategy but don't have the resources to do so effectively. After all, analyzing threat intelligence, monitoring deep web activities, tracking the posting of sensitive data, and overseeing third parties can require advanced skills, experience, and tools that only elite organizations can even afford.

In these cases, smart organizations should seek out services partners who not only possess these capabilities but also can work closely with the existing security staff to identify and mitigate digital risks. Digital Shadows fits this description well. Digital Shadows monitors and manages an organization's digital risk across the widest range of data sources within the visible, deep, and dark web to protect the company's business and reputation. Digital Shadows builds its services on top of SearchLight, a scalable security data analytics platform used to assess risk across the Internet and dark web. Digital Shadows services enhance SearchLight by adding:

- **Qualified personnel with the right skills and experience.** Digital Shadows employs an international team of cybersecurity analysts, data scientists, linguists, and services professionals with broad public and private sector experience. This group is especially proficient in combing the back alleys of the Internet and dark web to find early evidence of threats—before these threats turn into damaging security events.

- **Tailored service offerings.** Rather than providing canned threat intelligence feeds, Digital Shadows tailors its coverage to its customers' cybersecurity and business needs. For example, Digital Shadows can be tuned to look for threats based on an organization's industry, location, VIPs, geography, etc.

- **Tools and methodologies.** Digital Shadows starts with SearchLight to continuously monitor the visible, deep, and dark web for mentions of your company's assets and unique identifiers. Armed with this extensive data, Digital Shadows uses machine learning to filter out irrelevant citations and isolate real threats. To supplement its technology, Digital Shadows analysts are called upon to verify automated incidents, remove false positives, conduct further research, and categorize each incident with an appropriate security level. Finally, Digital Shadows shares prioritized incidents with customers through its management portal or API.

The Digital Shadows team also works with customers to help them understand both operational and strategic considerations in order to protect IT and business assets. For example, Digital Shadows offers a global takedown service to help its customers mitigate digital risks in a timely fashion. Digital Shadows also provides passive infrastructure monitoring to help customers find live exploits and prioritize remediation tasks. In these ways, Digital Shadows can help organizations improve incident prevention, detection, and response across all types of digital threats (see Table 1).

Table 1. Digital Shadows Services Can Help with Incident Prevention, Detection, and Response

Use Case	Digital Shadows Example	Response
Incident prevention	Tailored threat intelligence can be used to detect an impending attack against the organization.	Use information about cyber-adversary's TTPs to modify security controls. Alert users to look for details that indicate malicious attack campaigns.
Incident detection	Organization sees suspicious network connections associated with third-party partners.	Security analysts search Digital Shadows portal or submit search request to Digital Shadows analysts to check TTP libraries for threat actors exhibiting associated known behavior.
Incident response	Leaked privileged user credentials are discovered in hacker chat site on the dark web.	Verify that credentials have only been used for legitimate purposes over the last 90 days. Revoke and reissue credentials. Notify all privileged users. Explore technologies for privileged user management.

Source: Enterprise Strategy Group, 2017

The Bigger Truth

As Benjamin Franklin said, "An investment in knowledge pays the best interest." In this case, the investment must be in knowledge that can help organizations understand and react to digital risks. Unfortunately, knowledge in this area can be hard to come by. Many organizations continue to deal with *all* risks the way they always have—with perimeter and host-based security controls—but these security technologies were designed to block known malware and network behavior anomalies rather than widespread digital risks that threaten an organization's brand, VIPs, or infrastructure.

Yes, some organizations have a better understanding of digital risk, but many of these firms still struggle because they lack the right skills for digital risk analysis and can't hire experienced cybersecurity professionals to fill this void.

Given these limitations, CISOs should:

1. **Educate business executives.** While many business leaders recognize the benefits of digital marketing and business models, they most likely don't understand the associated risks. CISOs should make sure to take the lead on educating these executives and recruiting them into efforts around digital risk management.

2. **Assess internal skills.** Many organizations have some skills in threat intelligence analysis and security investigations but CISOs must assess whether these skills are adequate for a digital risk strategy. CISOs will often find gaps that can only be addressed through third-party services.

3. **Partner with services experts.** CISOs and risk officers should look for service providers, like Digital Shadows, that not only understand digital risks but also can tailor analysis and remediation services to an organization's industry, geography, and overall risk management strategy. The goal? Partner with an expert that can augment the internal staff to help find and address all types of digital risks as quickly as possible.