Teneo

## The Digital Domain: How Overlooked Dark Corners and Unknown Exposures Pose a Threat to Executives and Companies Today

The rise in readily available information in the digital domain has fundamentally altered the risk landscape for both companies and their leaders. In today's omnipresent digital landscape, accessing information on an individual requires little more than a quick search on Google, Facebook and LinkedIn. Armed with basic information such as a first and last name, email address, education or employment history, anyone with internet access now has the potential to create a dossier to target executives, employees and in turn their company. A recent *Wall Street Journal* article highlighted the range of information available online that hackers can use to target business leaders for cyberattack, ranging from public posts about private information on social media, publicly posted contact information and even our profile pictures to cross-reference identities. Although the article highlights some of the ways in which a bad actor can obtain information, however, it fails to acknowledge that regardless of fame or notoriety, everyone from a CEO to an entry level analyst either regularly and unwittingly *personally* advertises information about themselves or in many cases has *close personal or professional networks* that do. While many companies today are taking steps to monitor emerging risks stemming from the deep and dark web, it is often the surface web and day-to-day practices of their own employees that present the greatest risks to them and their company.

Personal information can be used to target a company to devastating results. In the past several months, the world has witnessed several high-profile companies report cyber-attacks resulting in the exposure of private information. Of the ~5,200 reported cyber breaches that occurred in 2020, 61% of breaches involved personal information used to access business systems, using what IT professionals refer to as credential data.[1] Meanwhile, according to the FBI, phishing attacks nearly doubled in frequency from 2019 to 2020, and current projections indicate this trend will only worsen through the remainder of 2021.[2] The increase of cyberattacks using personal information to target company networks emphasizes companies' most expansive weakness – the amount of information accessible about its employees on the web. Armed with this information, bad actors can socially engineer phishing attacks tailored to maximize the potential for an employee to fall for the rouse, enabling bad actors to similarly launch an attack on the company at-large.

Although bad actors may cast a wide net at a company, most place an overwhelming focus on a target company's senior leadership. According to Aon's 2020 Cyber Security Risk Report, senior business leaders are about nine times more likely to be victims of cybercrime than other employees.[3] The primary driver of that focus is executives' information and financial access, as well as the link between their personal and reputational well-being to that of the firm. Additionally, bad actors focus on executives because there is often simply more publicly and readily available information to draw from, even in cases where there is an absence of a large social media footprint. However, media coverage such as the recent WSJ article which places a heavy emphasis on the vulnerabilities of social media – only further perpetuates the notion that higher-level executives or employees with a lesser number of social media accounts are exempt from the dangers of the digital realm. In reality, an executive's digital exposure goes beyond their social media and into other realms of the digital space, and often without their knowledge. As a result, the amount of

[1] https://www.varonis.com/blog/cybersecurity-statistics/
[2] https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf
[3] https://www.aon.com/report-cyber-risk-data-breach-impact-to-organization-ip-mergers-acquisitions-security-threats/index.html

information digitally available regarding a company's executives is increasingly a source of physical, reputational and enterprise security risk to the company itself.

Against this new reality, digital vulnerability is a critical issue that boards and C-suites must address. Beginning with a holistic audit of senior leaders' digital presence across multiple platforms, the company is then able to minimize availability of seemingly innocuous information while mitigating its dissemination moving forward. Below, we highlight some of the most common areas bad actors seek out this information, emphasizing how those insights can be weaponized against both the individual and the firm.

### Traditional News / Media Coverage

Media coverage is a critical component of any effective corporate strategy. Whether it's a cover story for a prominent publication or a profile on Wikipedia, media coverage is the most common way that executives and their companies convey their narrative, values, priorities and vision for the future to the public. Frequently, such media will also feature seemingly benign information about executives, their backgrounds, professional affiliations and associations. Out of context most of this information may seem non-threatening; however, when aggregated over time creates a fuller picture of an individual and often one that includes some of the more intimate details of their private life that bad actors can then exploit. For example, an online biography of executives may detail where they are based, if they have any children, their alma mater and even sometimes their past or upcoming attendance at professional conferences. A bad online actor can use this information in a range of ways, including for potential password retrieval questions when trying to gain access to private personal or professional accounts, as well as for more traditional physical security attacks. For the former, this may mean using the alma mater's mascot as a password retrieval question or finding the children's social media pages to gain more information about where the family vacations.

In addition to using this information to target an executive's cybersecurity, bad actors can also use it to pose a potential physical threat. Announcements of an individual's plans to participate at an upcoming event or conference enables bad actors to proactively prepare and anticipate an executive's movements, providing the opportunity for a physical confrontation, among other outcomes. Another type of media commonly pushed by the company itself is interviews. Interviews also provide bad actors with the opportunity to study their subject's voice and behavior. With an audio or video recording, these actors can familiarize themselves with an individual's mannerisms, voice characteristics and speaking cadence, all of which can be used to impersonate that executive in a vocal confirmation check or by using a deepfake. Deepfakes leverage machine learning and artificial intelligence to manipulate or generate highly realistic interpretations of a target using their biometric data to, for example, gain access to personal or company accounts. However, the use of deepfakes or otherwise synthetic content can also be deployed as a means to cause significant reputational and in turn financial harm to an individual and by way, company. While these types of attacks have historically seemed reserved for only the ultra-sophisticated bad actor and high-profile target, the FBI earlier this year warned that is no longer the case. As deepfakes increasingly become an extension of existing spear-phishing and social engineering campaigns, businesses will want to take a closer look at their media content and management practices to proactively mitigate opportunities for exploitation.

### Personal & Extended Social Media

The rise of social media has only further catered to bad actors' agendas in the digital domain by providing them with a centralized and easy-to-access space in which private or personally identifiable information

(PII) can be easily ascertained. For this reason, social media accounts have become the treasure trove for bad actors seeking "low hanging fruit" that still yields high returns. According to a 2020 report from security company Tessian, 90% of social media users post information related to both their personal and professional lives online. While younger generations are more likely to have a social media presence than older generations, older generations are less likely to have proper privacy settings enabled.[4] Every photo, status update and location check-in can reveal valuable information about the user. Bad actors can then use that material to craft targeted and effective social engineering attacks against people and businesses, fooling them into granting access to otherwise secure systems.

As companies evaluate the risks an individual and in turn the business may face from social media, they must consider the broader social network as just as big of a vulnerability as the individual's own network. Although an executive may maintain a low social media profile and feel that they do not face the same level of risk as some of their counterparts who may be more active in the social domain, far too many underestimate or overlook the exposure they face from their extended social network through friends and family. Executives under the impression that they have evaded the risks of social media by maintaining little to no footprint on mainstream platforms in reality often face the same or similar levels of exposure as their counterparts who do, just through the accounts of their friends and family.

Whether this be in the form of content posted by a spouse, such as a wedding anniversary or extended family details, mentions, tags, or open Venmo transactions from kids citing recent purchases and whereabouts – all of this information can be used for similarly exploitative purposes – impacting both the individual and potentially the company. For example, some of the most basic criteria in the "About" section on Facebook alone solicits highly personal details, such as: job, high school, hometown, date of birth, religion, and other life events like when you became a homeowner or had your first child or dog. Even if not posted directly, many family and friends still disclose all of these details – and more – through their shared photos, check-ins, likes, and wall posts. This, coupled with limited privacy settings and, e.g., a spouse's post featuring photos of your new car or favorite annual vacation spot, can give a bad actor everything one would need to successfully crack intimate password retrieval questions and more.

### Deep & Dark Web Marketplaces

The deep and dark web make up roughly 90% of the true internet. While most sites are harmless, a small percentage are malicious sites that are hidden for nefarious reasons such as the buying, selling or releasing of individual or company information – it is nearly impossible to extricate information from these locations. The Dark Web and its marketplaces attract cybercriminals and other nefarious users, which use these forums to buy and sell stolen data, illegal or contrabanded goods.

Frequently, information on the Dark Web involves corporate data illicitly extracted from the so-called "Deep Web", the segment of the Internet that requires some form of authentication to access, ranging from password-protected websites to ultra-secure corporate datacenters. Cybercriminals will pilfer information from the Deep Web and then sell it on the Dark Web, offering records that can feature names, addresses, phones, emails and passwords stolen from websites and exposed databases. Some of this information may also come from less nefarious deep web spaces, such as flight tracker forums where airport-goers post information about tail numbers they saw fly in or out that day, among other unique deep web chat forums

[4] https://www.tessian.com/research/how-to-hack-a-human/

and community pages. Regardless of where the information derives from, all of this data in aggregate form presents significant financial, reputational, cyber, and physical security risks to the target and his or her associated business interests.

Given the number of systems breaches in recent years – perhaps the best example being the Experian breach in 2020 – most people, including business leaders, have personal information available on either the Deep or Dark Web. To further put things into context, over 70 percent of Americans have their social security number for sale on the Dark Web today. Without discrediting the significance of that statistic, sophisticated bad actors are typically seeking the true treasure trove, in which a purchase of a social security number comes *along with* all of the other PII – first and last name, current and past address, DOB, credit card numbers, and more. It is this kind of aggregated, attributable information on an executive that can present a real threat to companies and their leadership.

Unfortunately, managing deep and dark web exposure is more about awareness than it is maintenance. Regular checks of deep and dark web sources for potentially leaked credentials such as emails, passwords, social security numbers or credit card numbers can help executives know their exposure and proactively change passwords or credit information before they are targeted.

## Managing Digital Risk

Understanding the digital landscape and the multifaceted threats a company and its executives face is an integral part of developing an effective enterprise security and risk management program. Companies must take a holistic approach that evaluates individual and corporate exposure and takes actions to minimize vulnerability. The first step in this process is identifying what information key actors have available, understanding how it can be used against the company, and implementing effective sanitation and future cyber hygiene to minimize the impact while also monitoring for further exposure.

To achieve these objectives, Teneo Risk works with clients to develop a Digital Vulnerability Assessment (DVA), a 360-degree analysis of the information available on an individual or entity across the media, surface, deep, and dark web. By cataloguing the scope of accessible information within the public domain, Teneo Risk can assume the mindset of a malicious actors to anticipate how they may those findings to target executives or companies physically, reputationally or financially. We then work with clients to minimize the extent to which information can aid those objectives.

However, because the range of potential threats and motivations of bad online actors is uniquely vast in the digital domain, the intent of an executive DVA is not to examine the wide range of actions bad actors could take, but rather to focus on the tangible vulnerabilities that exist today and that are a byproduct of a company or its executives' digital hygiene. Rather than hypothesizing about unknowns and uncontrollables, such as the range of bad actors and the potential ways in which they may one day strike and why, DVA's should be prioritized to focus on the threat landscape that falls within a company or individual's control. This prioritization of risk can help companies create an actionable digital risk mitigation playbook to improve company and individual cyber hygiene practices.