RISKIQ®

# A New Cyber Vulnerability: Executive Digital Footprints

## The Digital Footprints of High-Net-Worth Individuals: An Underestimated Vulnerability

# Table of Contents

# Introduction

## Criminals Swindle Hundreds of Thousands of Dollars with a Deepfake

In March 2019, an executive of a UK-based energy firm received a phone call from his CEO in Germany. The CEO directed the executive to transfer $243,000.00 to a new supplier, a common request. The executive recognized his CEO's voice—right down to his accent—and made the transfer. The executive had no reason to doubt this order, but it proved to be a massive mistake. The voice he heard was actually a cyber-criminal using artificial intelligence to imitate or "deepfake" the request. How could this happen?

The deepfake attack is part of a new and growing trend for cybercriminals. Malicious actors study executives and other high-net-worth individuals' digital footprints and use artificial intelligence-based software to mimic them almost to perfection.

# Abstract

Organizations, businesses, entrepreneurs, executives, high-net-worth individuals, and influencers must maintain a robust digital and online presence to connect with more people, enhance their brand, bolster their services, and cultivate financial growth. But financial success and increased publicity often compound security challenges and attract adversaries.

Firewalls, the standard line of defense for protecting intellectual property and sensitive information, have acted like a fortified moat that protects the castle from outside intruders. In this new age of information security, growing technology, and connectivity to social media, the standard firewall defense mechanism has proven less effective.

Security professionals must now maintain visibility across a company's or individual's digital footprint to detect, remediate, and investigate external threats. Furthermore, threat actors are shifting their sights from traditional hard targets (e.g., a company's servers) to softer targets—such as you, your executives, your spouse, and your children. This paper will explore why it's essential to protect your assets outside the firewall, why hackers target high-net-worth individuals and key executives, and how to reduce your vulnerability to these new threats.

## Hacking the Human

The human brain, or "human hard drive," can be compared to the hard drive and Random Access Memory (RAM) of a server or computer. Both store massive amounts of information in their memory, such as company sensitive data, intellectual property, personally identifiable information (PII), company plans, and historical data, all of which are critical to a company's success and viability. Individuals and technology both have vulnerabilities and susceptibilities to intrusion. Yet, the individual or "human hard drive" doesn't stay locked up within the confines of the data center or the company offices each night.

The human hard drive goes out every day into the world, connecting to other networks and people, using multiple personal devices, and engaging with other "human hard drives," who may have nefarious intentions. Despite these vulnerabilities to the human hard drive, many organizations spend vast sums on protecting a company's internal digital infrastructure while overlooking the human element's cybersecurity requirements.

## Targeting Our Digital Footprint Outside the Corporate Firewall

Cyberattacks affect hundreds of businesses, governments, and individuals daily. The U.S. Federal government in F.Y. 2019 invested $15 billion in cybersecurity, and Gartner estimates companies will allocate over $133.7 billion to cybersecurity by 2022. Cybercrime is on the verge of becoming the number one economic crime for U.S. businesses, reaching 54 percent of organizations surveyed by PwC's Global Economic Crime Survey.

Forty-one percent of executives surveyed said they spent at least twice as much on investigations and related interventions as they lost to cybercrime.[1] Last year, Cybersecurity Ventures predicted that, by 2021, cybercrime will cost the world $6 trillion annually, up from $3 trillion in 2015.[2]

## Know Your Digital Footprint and Attack Surface

The internet contains a wealth of information. Online sources such as social media platforms, real estate websites, and people search engines provide hackers with all they need to target you. Your home address, phone number, email address, employment, education, associates, family members, children's names, and frequented restaurants or places of interest may all be public.

In the U.S. alone, there are over 120 people search engines, which rely on an entire industry built around data brokers. The data brokers collect this type of information, then sell it to these search engines, companies (usually for marketing purposes), other data brokers, and even individuals. Public figures, executives, and high-net-worth individuals often have a more extensive public footprint than the average citizen. Because they are already a high-value target, this outsized exposure makes them even more vulnerable.

Your digital footprint is your and your company's presence in cyberspace. Many of your assets exist, change, and become vulnerable in cyberspace, often without your knowledge. Attackers performing digital surveillance will often find unknown, unprotected, or unmonitored corporate executives' assets or other critical employees to use as attack vectors. In today's Internet of Things (IoT), where our society is highly connected and more social, this information is available. With

[1] PwC's Global Economic Crime Survey for 2018.

[2] Cybersecurityventures.com

enough time, research, and data triangulation, you and your key personnel run the risk of becoming a target.

As technology becomes more interconnected and access to information expands, we must adopt a holistic approach to bridge the gap between cybersecurity's inner and outer worlds. In short, we need to focus on cyber bodyguards.

## Going Back to the Basics: The Art of Espionage

The field of cybersecurity is evolving. So are malicious actors' tactics and attack vectors. Cybercriminals no longer need sophisticated tools or methods to hack into a secure system or breach a hard target to damage a company. Instead, they now seek new target sets by focusing on key individuals with access to that same valuable information, sometimes referred to as 'soft targets.'

A company's ability to protect privileged and sensitive information through technology and advanced software has undoubtedly increased over the years. However, a human being's susceptibilities and vulnerabilities remain the weakest link when it comes to external meddling. Technology and firewalls alone are not enough to safeguard against intrusion and information theft. Many hackers are rediscovering the basics—focusing on gathering available information on people, not systems. In the world of international espionage, this is known as human intelligence or HUMINT.

As practiced by nation-states, traditional HUMINT comprises five stages: spot, assess, develop, recruit, and handle. In most cases, the targets for nation-state HUMINT operations are foreigners with access to intelligence vital to that nation's foreign policy and national security. During the first stage of the cycle—spotting—the intelligence officer identifies potential targets and then research them extensively. Once they assess that an individual could be a viable recruit, the intelligence officer then develops the target by building a personal relationship with them, creating trust, and learning their vulnerabilities. The intelligence officer may even learn their target's language and culture to add a level of sophistication. Actual recruitment may involve an appeal to financial gain or ideological beliefs.[3] At the very core of international espionage is gathering human intelligence.

Cybercriminals are increasingly reverting to these "basics" by using similar tactics as trained intelligence officers. But, instead of calling it espionage, the security industry refers to the human element of cyber attacks as *social-engineering.*

## Growing Trends: Cyber Attacks Based on Manipulating the Human Element

In the last few years, hackers have increased their use of social-engineering tactics in cyberattacks, making it a serious and growing threat on a global scale. Two evolving and sometimes overlooked social-engineering attacks, Business Email Compromises (BEC) and the use of Deepfakes, require some form of human and psychological manipulation. All social-engineering attacks follow the same trajectory.

The malicious actors study their primary target—or anyone associated with them—to build a personal profile. This research allows the threat actor to infuse their deception with authenticity to capitalize on the inherent trust vulnerable colleagues have in the target. How do the threat actors build this personal profile of their target? By collecting personal

[3] According to the Central Intelligence Agency's website.

information from publicly available sources and augmenting it with leaked PII.

**Social-engineering Attacks:** In Social Engineering Attack Examples, Template and Scenarios, Francois Mouton defines social engineering as “the science of using social interaction as a means to persuade an individual or an organization to comply with a specific request from an attacker where either the social interaction, the persuasion or the request involves a computer-related entity.”

A common technique is for hackers to focus on the behaviors and patterns a person exhibits on social media. The proliferation of social media has given rise to the greater willingness of so many to share their interests, hobbies, schedules, as well as names of family, friends, and colleagues. This information provides hackers with a gold mine of information. Just one example:

> In April 2013, the Associated Press (A.P.) tweeted “two explosions in the White House and Barack Obama injured.” This tweet was sent to A.P.s’ more than two million followers and within hours caused the Dow Jones to plunge 140 points, equivalent to $136 billion in equity market value. How could the A.P. Tweet such a thing?

The A.P. received an email appearing to be from an A.P.

employee. However, the email was actually sent by the Syrian Electronic Army. The email included a link to a page requesting the login details for the A.P. Twitter account. Once the attackers had the login details, the Syrian Electronic Army just had to post a single tweet to send the financial market into chaos.[4]

**Business Email Compromise (BEC) and CEO Fraud:** Business Email Compromise (BEC) and CEO Fraud:  BEC occurs when an attacker gains access to a corporate email account and forges the owner's identity to defraud the company or its employees, customers, or partners. The goal is most often financial gain. According to the FBI's 2018 Internet Crime report, BEC attacks are on the rise, and the total identified global exposed losses now exceed $26 billion. One example:

> In September 2019, Nikkei—a Japanese media conglomerate and publisher of the world's largest financial newspaper—lost approximately $29 million when an employee transferred the funds to a fraudulent bank account. The victim claims he simply followed the instructions of a person he thought was part of the Nikkei management team (From a Nikkei press release).

**Deepfakes:** A deepfake is AI-generated audio or video which impersonates someone. The film industry used early applications (e.g., the late actor Paul Walker's posthumous appearance in 2015's Furious 7). Malicious actors now use the same technology to defame, embarrass, create conflict, or extort money. The term deepfake was coined in 2017 when a prolific Reddit user published a series of fake celebrity porn videos using machine learning tools like TensorFlow, which Google makes freely available.

In 2018, a deepfake creation desktop application called

[4] Phoenixnap.com, "7 Most Famous Social Engineering Attacks in History, Be Prepared" September 27th 2018.

FakeApp launched and brought deepfakes to the masses. That same year, a deepfake video of Barack Obama went viral and served as a warning of this technology's dangerous potential. This emerging threat has now become a concern for the private sector, politicians, high-net-worth individuals, and governments alike. According to the cybersecurity firm Symantec, A.I.-generated technology is so accurate that in 2019 three of its clients experienced attacks in which employees were duped into transferring millions of dollars because they thought their bosses had requested them to.

Governments and politicians are worried that deepfakes could be used to spread misinformation or manipulate election results. Imagine a deepfake imitating a world leader and saying something that could purposely lead to conflict, or worse, start a war. Or, a public figure saying or doing something controversial that they never did or said, smearing their reputation or setting them up for some sort of physical retaliation. One example:

In the run-up to Iraq's elections in 2018, two female candidates were humiliated with explicit videos, which they say were fake. As a result of the videos, the candidates dropped out of the race.

The common thread of cyber-attacks that use social engineering, BECs, or deepfakes? The targets aren't servers, systems, or other infrastructure—they're *people*.

## Why a Hacker Targets Executives and High-Net-Worth Individuals

Hackers who target humans find their vulnerabilities an easier avenue to gain access to the networks and digital platforms

[7] The Economist. "Women in public life are increasingly subject to sexual slander. Don't believe it...As deepfake technology spreads, expect more bogus sex tapes of female politicians"

where data and other valuable information lies. Kevin Mitnick, a notorious hacker, said he found it easier to manipulate people than technology. Most of the time, organizations overlook the human element—and yet that is where most hacks start.

Executives are desirable targets because they have both access to critical areas of a company and essential proprietary knowledge. In short, executives hold the "keys to the kingdom." For example, the CEO is the highest-ranking corporate officer and oversees a company's policy and strategy, which means they can access everything. The CFO has access to all the financial affairs of the organization. A CTO or CIO usually retains access to all technology and security in an organization.

This new strategy is proving successful for malicious actors, especially when it comes to business email compromises. Executives are now six times more likely to be a target of social engineering than they were only a year ago, according to the Verizon 2019 Data Breach Report. Also, C-suite executives are 12 times more likely to be a target.

## Motivations

What motivates a hacker or malicious individual? What are their intentions? Motivation seems to be a murky area that is rarely addressed when hacks are made public, but it is important to understand that people are motivated by an array of factors. Hacks can be personal or completely random, but outsider threats account for 69% of breaches, according to the Verizon study. This percentage point means that we do not know the criminal most of the time—even if they dupe us into thinking that we do.

- One of the most prominent motivators for hackers is

**financial gain**—to extort monetary payment and capital. For example, in May 2019, hackers withdrew $40 million worth of Bitcoin in a single transaction from Binance, the world's largest cryptocurrency exchange. The hackers used various techniques, including phishing and viruses, to obtain a large amount of user data.

- Some hackers are motivated by **political or ideological** reasons. Hackers who breach systems to make political or ideological points target businesses and governments and use cyberattacks such as "denial-of-service" campaigns to disable websites. For example, in 2010, the hacktivist collective Anonymous used "Operation Payback" to try to take down the websites of financial services companies that had stopped processing donations to the WikiLeaks campaign, including PayPal, Mastercard, and Visa.

- **Ego** is also a driving factor for many cybercriminals. Some hackers may not hack out of malicious intent or financial benefit but simply because they can. Rachel Tobac is a celebrity among hackers. She is known as a white hat—a good hacker—and demonstrates in front of audiences how easy it is to get hotels, airlines, and businesses to handover your personal information without verifying it is you they are speaking to on the phone.

  She showed a CNN tech reporter first-hand. To get his home address, she called up a furniture company he had tweeted about. Tobac claimed she was his wife and that she wanted to check that the company had his correct home address on file before she placed another order. She deliberately gave the wrong address, and the person on the other end of the line corrected her with the CNN reporter's full home address. It was that simple.[5]
- Another common motivation is to gain a competitive

[5] CNN, "We asked a hacker to try and steal a CNN tech reporter's data. Here's what happened."

advantage by conducting **industrial espionage** and stealing confidential information. Industrial espionage tends to involve "inside jobs," in which an employee steals secrets for financial reasons. Governments may also conduct industrial espionage as they pursue economic or financial goals. Social media is a new frontier for industrial espionage, and its full impact and utility is still being measured.

In 1997, Gillette brand paired up with Wright Industries to help in the development of its next-generation shaver system. A disgruntled Wright Industries employee leaked the designed technology's blueprints to Gillette's competitors through emails and fax.[6]

- And, of course, there's one of the oldest motivations of all: **revenge**.

## Next Wave Mitigation Strategies: Know Your Enemy...

*"If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle."*

In his famous Art of War (ca 500 B.C.), the great Chinese military strategist, writer, and philosopher Sun Tzu warned us that we must know our enemy to defeat them. This means we must know what they know about our weaknesses and strengths.

Understanding your or your company's digital footprint means understanding everything outside the firewall, a collection of far-flung, client-facing assets cyber threat actors can and will discover as they research their next targets. We call this data

[6] http://blog.inventus.com/blog/5-most-famous-cases-of-industrial-espionage

outside the firewall attack surface. When organizations and individuals take the time to analyze their entire digital attack surface, they understand what they look like from the outside-in, i.e., what they look like to a threat actor. In this way, they can develop a strategy that allows them to discover everything associated with their organization on the internet, both legitimate and malicious, and shrink that attack surface down to a manageable size.

## Recommendations: Getting Ahead of the Curve

There are common mitigation strategies in securing your digital footprint, which you likely already employ:

- Changing and creating complex passwords
- Keeping social media accounts private
- Refraining from using geolocation applications
- Avoiding disclosing information about your associates, family or friends

With hackers growing more sophisticated, the above efforts are no longer enough to protect ourselves or our assets. Therefore, we must expand and improve our mitigation strategies. Five recommendations:

- Build a comprehensive protection plan for executives and high-net-worth individuals that bridges the gap between the physical and cyber realm of security. Such a plan should focus on protecting and preventing attacks against a person's reputation, sensitive data, brand, intellectual property, PII, and financial assets.

- Build a security program that includes digital protection and full visibility for executives and key personnel. This program should seek out, then monitor and mitigate online activity that can be leveraged by threat actors to conduct attacks.

- Develop a personal habit of cloaking activities online to limit the exposure of personal data.

- Establish a routine cadence of reports and briefings focused on counterintelligence. An example would be annual exposure and vulnerability reports on executives and key employees prepared by intelligence and security professionals.

- Establish quarterly or semi-annual training sessions for the entire workforce to ensure they are kept up to date on the latest tactics and techniques used by threat actors.

## Conclusion

At RiskIQ, we provide customers full visibility over their internet presence, spell out for them the associated risks, and tailor mitigation plans like those outlined above. In particular, to proactively prevent harm against executives and key employees in both the cyber and physical realms, RiskIQ Executive Guardian™ continuously monitors the web for indicators of attacks, including online digital risk, personal threats, and leaked sensitive information. A fully managed and customized service, Executive Guardian is a secure data room that adheres to rigid compliance standards. To find out more about our services, please visit us at www.riskiq.com or contact us at info@riskiq.com. attacks, including online digital risk, personal threats, and leaked sensitive information. A fully managed and customized service, Executive Guardian™ is a secure data room that adheres to rigid compliance standards. To find out more about our services please visit is at www.riskiq.com or contact us at info@riskiq.com.

**RiskIQ, Inc.**
22 Battery Street, 10th Floor
San Francisco, CA. 94111

✉ sales@riskiq.net
☎ 1 888.415.4447

**Learn more at riskiq.com**