CISO EDITION

BLACKCLOAK®

The Home is the New Battleground for Cyber Threats:

How to Safeguard Your Executives and Extend Cybersecurity Beyond the Corporate Walls

Introduction

Home. It's our sanctuary, the place we feel most comfortable and safe. It's where we create and share memories with our families, where our material goods are stored, and where we lay our head to sleep soundly at night. But for CISOs, it has also evolved into the new battleground for cybercriminal activity because it is where executives—and therefore the cybersecurity of the organizations they work for—are most vulnerable.

Recent events, including the deadly attack on the CEO of UnitedHealth, have highlighted the increasing sophistication of attacks on home territory. Cybercriminals are now exploiting the personal devices, home networks, and publicly shared personal information of executives and their families to gain unauthorized access to corporate systems or in perceived retaliation.

This significant change in approach necessitates a reevaluation of cybersecurity strategies to protect both the personal and professional digital lives of executives, to ensure the safety and integrity of the entire organization as well as the physical and private safety of executives and their families.

Why **Executives Represent Risk** to Organizations

The digital footprints of corporate executives are larger than most, spanning across their own organizations, the multitude of individuals they interact with, and their personal lives. Given their high visibility and access to sensitive information, cybercriminals have identified them as high-value targets.

The challenges are compounded when these leaders use personal devices, connect to home networks, and interact with smart home devices, all of which become entry points to the corporate environment. Each of these scenarios presents unique vulnerabilities, from data breaches and malware infections to sophisticated social engineering attacks.

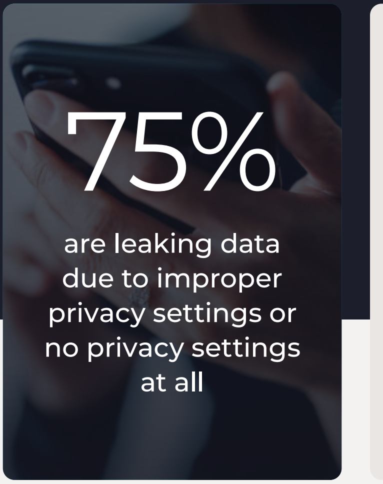
There are five specific ways in which executives introduce cyber risk to their respective organizations.

Using Personal Devices to Access Corporate Data

Due to the sensitive nature of information that is handled by executives, it's often a mandate not to mix corporate work with personal devices. Meaning, that work must be done only on business-sanctioned devices because they have the proper cybersecurity installed. But even with the highest level of cyber training available, mistakes are made by executives when at home and doing their jobs. They may use their iPads, personal laptops, or smartphones to access email, messaging platforms, or corporate folders.

87%

of leaderships' personal devices have no security installed



75%

are leaking data due to improper privacy settings or no privacy settings at all

Personal phones, tablets, and laptops are highly vulnerable to data loss, unauthorized access, credential theft, and lateral malware spread, among other attacks of consequence to their families and the enterprise.

According to Ponemon Institute research, commissioned by BlackCloak

Family & Friends Connecting to Wifi

Wifi is the common denominator in homes, where every family member or visitor can access the internet via a single home connection.

According to Deloitte, the average household now has more than 25 connected devices. Of those IoT devices, a large percentage of those registered to executives contain malware. The intermixing of compromised and vulnerable devices on the same network being used for work purposes elevates the risk of botnet-driven attacks and lateral malware spread into the executives' organizations.

Smart Homes & IoT Devices

A significant number of smart devices, like TVs, cameras, doorbells, and speakers, have open ports and hardware or software vulnerabilities. These devices, when improperly connected or configured, can compromise the executive's privacy, which subsequently adds risk to the business. Eavesdropping, device hijacking, man-in-the-middle attacks, and DNS spoofing are some of the most common IoT-driven threats.

Data Broker Websites

Like ordinary people, C-suite and board members' personal information is available on hundreds of data broker websites. Cybercriminals can legally purchase this information or breach it, and then use it to conduct social engineering attacks, bypass multi-factor authentication controls, engage in identity theft and account takeover, and obtain unauthorized access to the company's sensitive assets.

Leaked Credentials

Ponemon Institute research shows that more than 70% of executives' passwords are for sale online. And because 84% of people admit to reusing passwords across multiple sites, according to a Bitwarden study, cybercriminals know that a stolen password for a personal website is more likely than not to also be used to access a company system or device. Hackers are increasingly obtaining leaked credentials to launch password spraying and brute force attacks - either to breach personal assets and then move laterally into the executives' organization - or to compromise the personal or corporate asset itself.

70%

of executives' passwords are for sale online

According to Ponemon Institute research,

Challenge for CISOs

As the guardians of organizational security, CISOs must navigate these complexities to protect the professional digital environments of their executives, ensuring the safety and integrity of the entire enterprise.

This task, however, becomes increasingly complex when these executives are not working on corporate devices or are away from the office. As cyber threats continue to evolve, the challenges facing CISOs in this context are multi-faceted and demanding.

01

The Invisible Perimeter: Extending Security Beyond Corporate Devices

One of the primary challenges for CISOs is the invisible perimeter created when executives use personal devices or access the internet from outside the corporate network. These devices often lack the robust security measures implemented on corporate-issued hardware. Personal smartphones, tablets, and home computers may not have the latest security updates, making them vulnerable to malware, phishing attacks, and other cyber threats. Additionally, the absence of corporate-level firewalls and intrusion detection systems increases the risk of unauthorized access.

02

Blurred Boundaries: Work and Personal Life Intersect

Executives often blend their professional and personal lives, using the same devices and online accounts for both purposes. This intersection creates a broader attack surface, with sensitive corporate data potentially being exposed to the same vulnerabilities as personal information. Cybercriminals can exploit this overlap by targeting personal accounts to gain access to corporate resources. The challenge for CISOs is to implement security measures that protect both worlds without being overly intrusive.

03

The **Rising Threat** of Social Engineering

Executives are prime targets for social engineering attacks due to their high visibility and access to valuable information. Cybercriminals employ sophisticated tactics, such as spear-phishing and whaling, to deceive executives into disclosing sensitive information or granting access to corporate networks. These attacks often occur outside the office, leveraging social media platforms and personal email accounts. CISOs must continuously educate executives on the latest social engineering techniques and encourage vigilance in all online interactions.

04

Home Network Vulnerabilities

Executives bring their work home with them, highlighting the vulnerabilities of home networks. Unlike corporate environments, home networks often lack stringent security protocols. Weak passwords, outdated routers, and unsecured IoT devices can provide easy entry points for cybercriminals. CISOs face the challenge of extending corporate security policies to home environments without infringing on personal privacy. This requires a delicate balance between enforcing security standards and respecting both privacy legislation and the personal autonomy of executives.

05

The Challenge of Monitoring & Response

Monitoring the digital activities of executives outside the corporate network poses significant challenges. Traditional security monitoring tools are designed for corporate environments and are not effective in personal settings. Furthermore, CISOs must navigate privacy concerns and regulatory compliance when implementing monitoring solutions. In the event of a security breach, rapid response and containment are crucial. However, coordinating incident response across personal and corporate devices adds complexity to the process.

Digital Executive Protection **by BlackCloak**

CISOs need a strategy to protect the privacy, personal devices, and homes of their C-suite, board members, and key personnel when they are outside the corporate perimeter. This strategy must recognize executives will use personal devices and connect to networks that lack enterprise-grade controls. Extending enterprise-level coverage is critical and providing high-level visibility into the status of that coverage is important to CISOs.

BlackCloak is the pioneer of Digital Executive Protection™.

The BlackCloak platform and suite of concierge services is purpose-built for corporate executives and high-profile individuals. It becomes an extension of enterprise-grade services to protect the company by safeguarding executives in their personal digital lives without burdening internal resources.

By combining proprietary technology with 24x7x365 Security Operations Center and white-glove concierge support, BlackCloak secures the C-suite, board members, and their families' privacy, reputation, and finances on behalf of the CISO while aligning to the organization's cybersecurity strategy. In doing so, Digital Executive Protection actively reduces the risk of advanced threats moving laterally into the organization for nefarious purposes.

Reasons Why CISOs **Trust BlackCloak**

CISOs have long trusted BlackCloak as an extension of their security teams to protect the private digital lives of their executives because we deliver on the following promises:

01

Executives maintain their privacy

Executives' personal information is everywhere online. BlackCloak, with our team of highly skilled and experienced digital privacy experts, removes the executives' private information from nearly 400 data broker sites. Upon request, executives can request that the team remove information from hundreds of additional websites, forums, and social media sites.

BlackCloak continuously monitors the dark web, ensuring that members' personal devices, networks, IoT, apps, and passwords meet the most stringent privacy, hardening, and authentication controls.

02

CISOs can ensure executives' digital safety during travel and work hours, thereby enabling CSOs to safeguard their physical security

The collision of the physical and digital worlds emboldens cybercriminals to exploit security gaps, putting executives and, by extension, their companies at risk. Through holistic privacy and cybersecurity protection, BlackCloak proactively reduces the risk of executives and their families becoming victims of cyber extortion, cyberstalking, cyberbullying, online and in-person harassment, impersonations, and threats to physical safety.

03

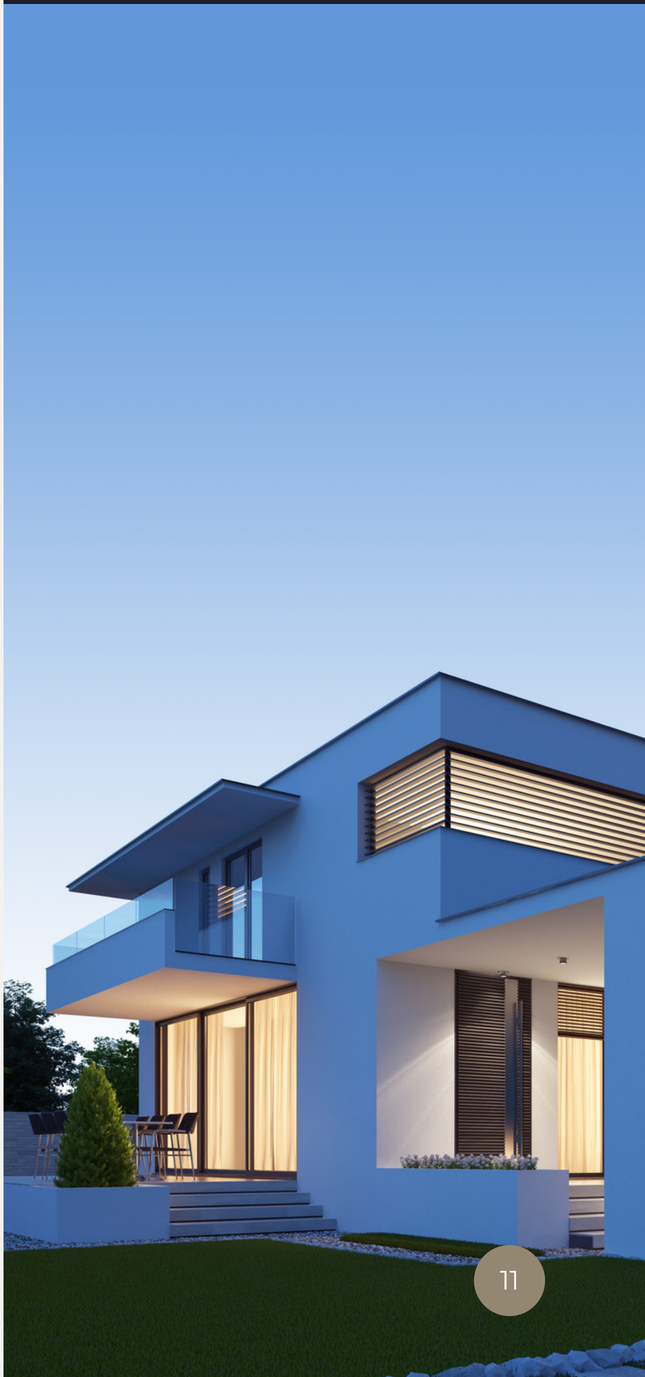
Personal data breaches are prevented, protecting company data

To bypass corporate security, cybercriminals increasingly target executives in their personal lives to obtain credentials for accessing proprietary, sensitive, and lucrative company data. BlackCloak's 24x7x365 US-based Security Operations Center (SOC) uses a combination of enterprise-grade and proprietary technology to prevent, detect, and respond to cyberattacks on executives outside of enterprise security control. BlackCloak performs home network scans, secure personal devices, monitor social media accounts, and more to keep them safe.

04

CISOs can protect against threats coming through executives without having to invade their personal lives

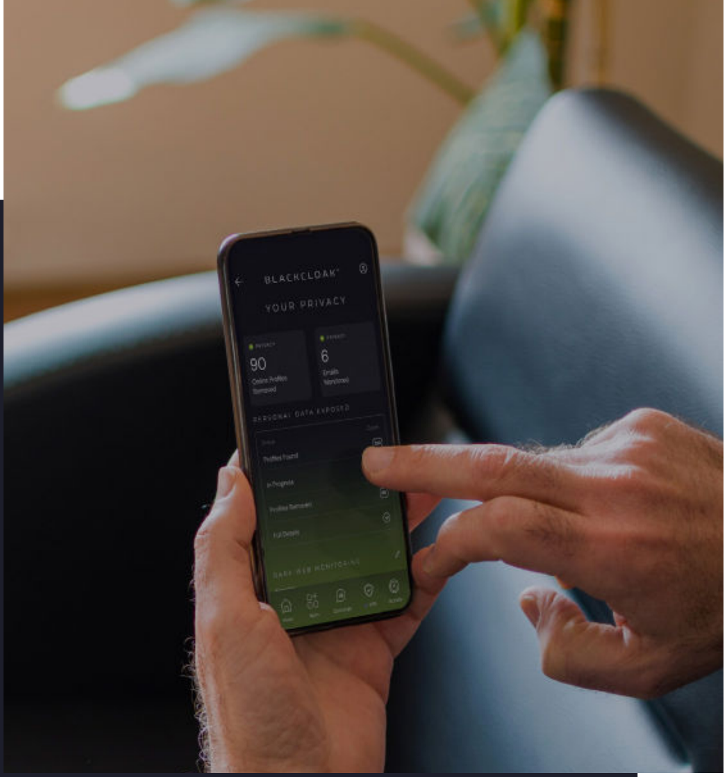
Security teams have a lot on their respective plates, and protecting the personal digital lives of executives is difficult to navigate. Even if security teams have capacity, having visibility into a company leader's personal life is a liability and can breach privacy legislation. BlackCloak's veteran team of threat intelligence, privacy, and security operations professionals manage executives' personal cybersecurity and privacy protection needs from start to finish. This allows the security team to focus on what they do best: protecting the enterprise.



05

CISOs and executives achieve peace of mind

Executives are very busy people with limited time and a lot to lose. While a CISOs ability to protect them in their personal lives is limited, they need more than just credit monitoring and antivirus solutions to safeguard their personal privacy and security. From onboarding forward, BlackCloak's Concierge team provides the white-glove service executives expect, sharing only essential information with the security team while keeping corporate leaders' privacy intact.



BC

About **BlackCloak**

BlackCloak secures the personal digital lives of corporate executives, high-net-worth individuals, and their families. We tailor our cutting-edge technology, expertise and support to protect clients from evolving threats, safeguarding reputations, finances, and peace of mind in an increasingly connected world.

Used by Fortune 500 companies, recommended by wealth management firms, and trusted by private family offices, the BlackCloak Platform is an award-winning holistic cybersecurity solution, complete with 24/7 personalized support. With BlackCloak, executives and high-profile individuals get peace of mind knowing their family, privacy, reputation, and finances are secured, while CISOs and CSOs can be confident that their people, brand, intellectual property, data, and finances are protected without invading their executives' personal lives.

BLACKCLOAK®

Contact info@blackcloak.io to learn more
or visit **www.blackcloak.io**