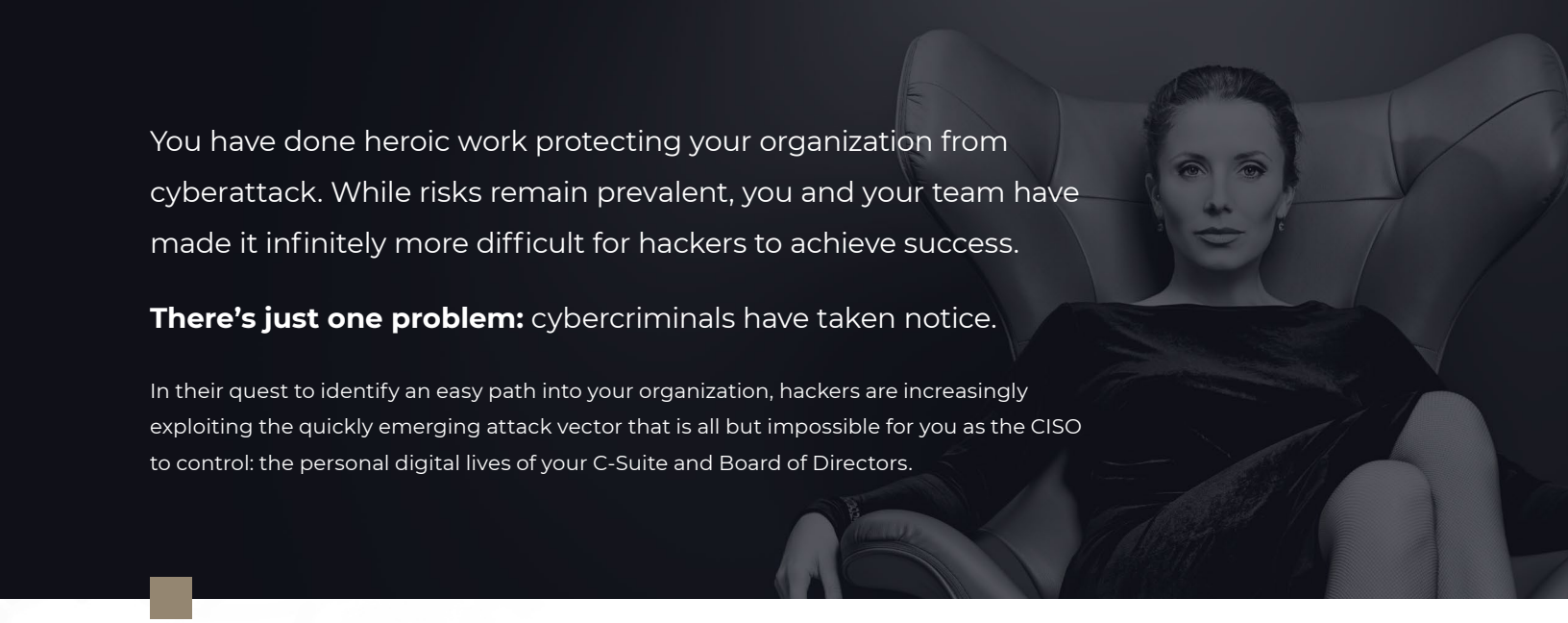
BLACKCLOAK™

Five Ways the Personal Lives of Your C-Suite & Board Members Add Risk to Your Organization

And how you can reduce threats and prevent lateral movement of attacks into the company without burdening your team

www.blackcloak.io



You have done heroic work protecting your organization from cyberattack. While risks remain prevalent, you and your team have made it infinitely more difficult for hackers to achieve success.

There's just one problem: cybercriminals have taken notice.

In their quest to identify an easy path into your organization, hackers are increasingly exploiting the quickly emerging attack vector that is all but impossible for you as the CISO to control: the personal digital lives of your C-Suite and Board of Directors.

A burgeoning attack vector outside of corporate control

Cybercriminals are not known to waive the proverbial white flag in the face of adversity. Instead, they evolve their tactics and techniques to gain an advantage over your defenses.

Hackers' transition from sending phishing emails consisting of malicious links and attachments to distributing payload-less social engineering messages across multiple mediums is a perfect example.

An unintended consequence of the successful hardening of your organization is the expansion of the attack surface to include the personal digital lives of company leaders.

Today, sophisticated cybercriminals recognize how vulnerable your C-Suite and Board Members are when corporate security is not in control. As such, hacking leadership in their personal lives to then move laterally into your enterprise has evolved from an occasional nuisance into a mainstream threat.

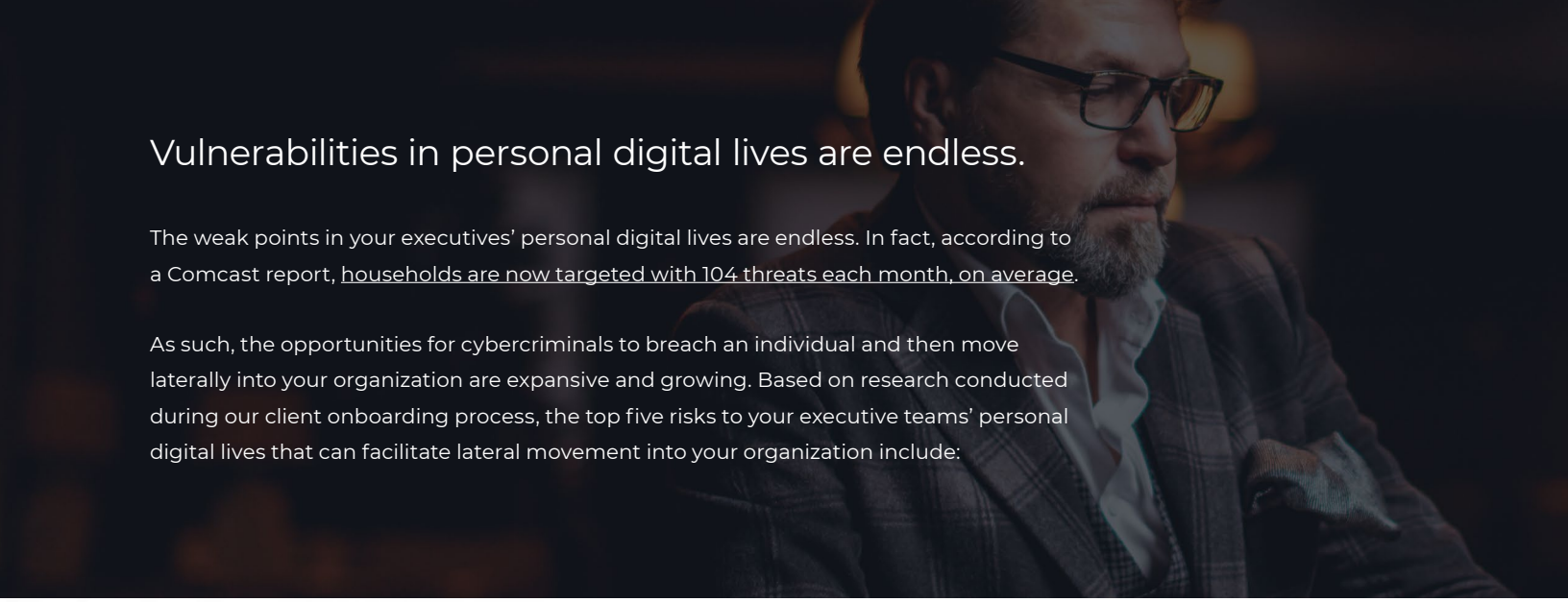
The unintended consequences of intended frictionless work

The lives of your C-Suite and Board Members have become frictionless between the personal and the professional. Even before the pandemic, work was increasingly being done from anywhere, on both corporate and personal devices, and while connected to either public or private internet.

For your company leadership, complete separation from the business is inconceivable. Even when leaders intend to "unplug," there is always a discussion to be had and decisions to be made.

To maintain accessibility, your C-Suite and Board Members are increasingly conducting business on their personal devices that are often connected to weak or compromised networks – either out of necessity, preference, or ease-of-use.

Unfortunately, organizational leaders' intended casualness has the unintended consequences of adding significant risk to themselves, their families, and by extension, the company that you have a mandate to protect.



Vulnerabilities in personal digital lives are endless.

The weak points in your executives' personal digital lives are endless. In fact, according to a Comcast report, households are now targeted with 104 threats each month, on average.

As such, the opportunities for cybercriminals to breach an individual and then move laterally into your organization are expansive and growing. Based on research conducted during our client onboarding process, the top five risks to your executive teams' personal digital lives that can facilitate lateral movement into your organization include:

1 Using Personal Devices to Access Corporate Data

On average, **87% of leadership's personal devices** have no security installed, and **75% are leaking data** due to improper privacy settings or no privacy settings at all, according to our research. As such, 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.

2 Family & Friends Connecting to Wifi

According to Deloitte, the average household now has more than 25 connected devices. Of those IoT devices, **nearly 40% of those registered to executives contain malware**, our research reveals. 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 your organization.

3 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 your 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.

4 Data Broker Websites

Like ordinary people, your 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 your company's sensitive assets. In 2021, Wired proclaimed data brokers a "threat to democracy."

5 Leaked Credentials

Our research shows that **more than 70%** of executives now have passwords for sale online. And because **65% of passwords are reused** across multiple sites, according to a Google 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 your organization - or to compromise the personal or corporate asset itself.

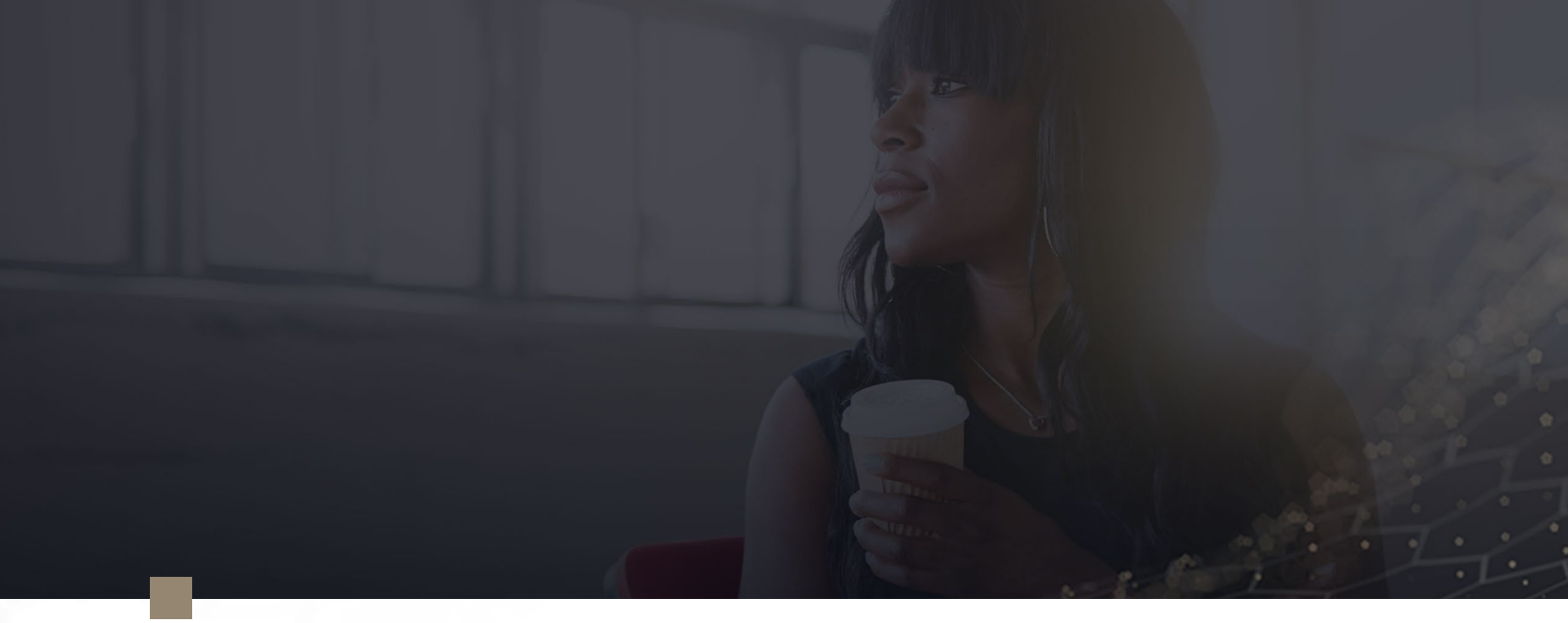
The only cyber risk that you cannot and don't want to control

You make a living solving complex cybersecurity problems. Unfortunately, protecting your company leadership when they are outside of the corporate walls is the one challenge that you cannot fully control.

You can't simply extend corporate security policies like Bring Your Own Device or secure remote access into your executive's personal life. You don't have the authority to mandate training, configure personal devices or enforce proper usage requirements. And you certainly cannot penalize your executive's family members for noncompliance.

But even if you could solve the problem of burgeoning risk to your executives' personal lives, would you really want to? **Probably not**.

Having access to private and highly-personal information would expose both you and your company to heightened privacy, disclosure, and legal scrutiny. You have enough to worry about without adding an additional headache to your plate.



Introducing digital executive protection from BlackCloak

In today's threat landscape, you need a strategy to protect the privacy, personal devices, and homes of your C-Suite, Board Members, and key personnel when they are outside of corporate security.

This strategy must recognize that executives will use personal devices and connect to networks that lack enterprise-grade controls. It must report back to you on specific threats while separating company personnel to ensure privacy. And it must maintain service level agreements.

BlackCloak is a pioneer of digital executive protection specifically for corporate executives and high-profile individuals. We help CISOs like you protect your company by protecting your executives in their personal digital lives.

Our holistic, SaaS-based Concierge Cybersecurity & Privacy Platform™ is purpose-built to defend your executive's and their family's from security and privacy risks such as **cyberattack, financial fraud, credential theft, impersonation attempts, identity theft, and harassment,** among other threats.

By combining proprietary technology with white glove concierge support, we eliminate a growing burden to your resource-strapped security team by securing your C-Suite and Board Members, and their families, privacy, reputation, and finances. In doing so, we're actively reducing the risk of advanced threats moving laterally into your organization for nefarious purposes.

With BlackCloak, we help protect your executives' personal digital lives — and ensure your peace of mind — anytime, anywhere.

For more information on digital executive protection, visit **www.blackcloak.io**

Follow **@blackcloak** on social media to learn more about our technology and how we help our clients attain peace of mind.