DATA REPORT

BLACKCLOAK™

Quantifying the Business Need for Digital Executive Protection

How threats and vulnerabilities originating in the personal digital lives of your corporate executives, Board Members, and high-profile employees add new risks to your organization that can lead to lost revenue, decreased productivity, disruption of business continuity and more.

www.blackcloak.io

Executive Summary

The attack surface has expanded. The soft-underbelly of enterprise security is now the personal digital lives—the digital privacy, personal devices and home networks—of your executives, board members, and high-profile employees with access to finances, confidential information, and proprietary data.

As protected as your company's leaders are when inside the organization's four walls, as soon as they head home or switch to working on their personal devices, home networks, or personal email accounts, the security team loses control, and both the individual and the company become exponentially more vulnerable.

This report quantifies the personal digital privacy and cybersecurity risks to your executives and other high-value employees in their personal lives. It examines the specific threats posed to them as individuals and to the organization, while also highlighting potential business impacts of concern.

Methodology

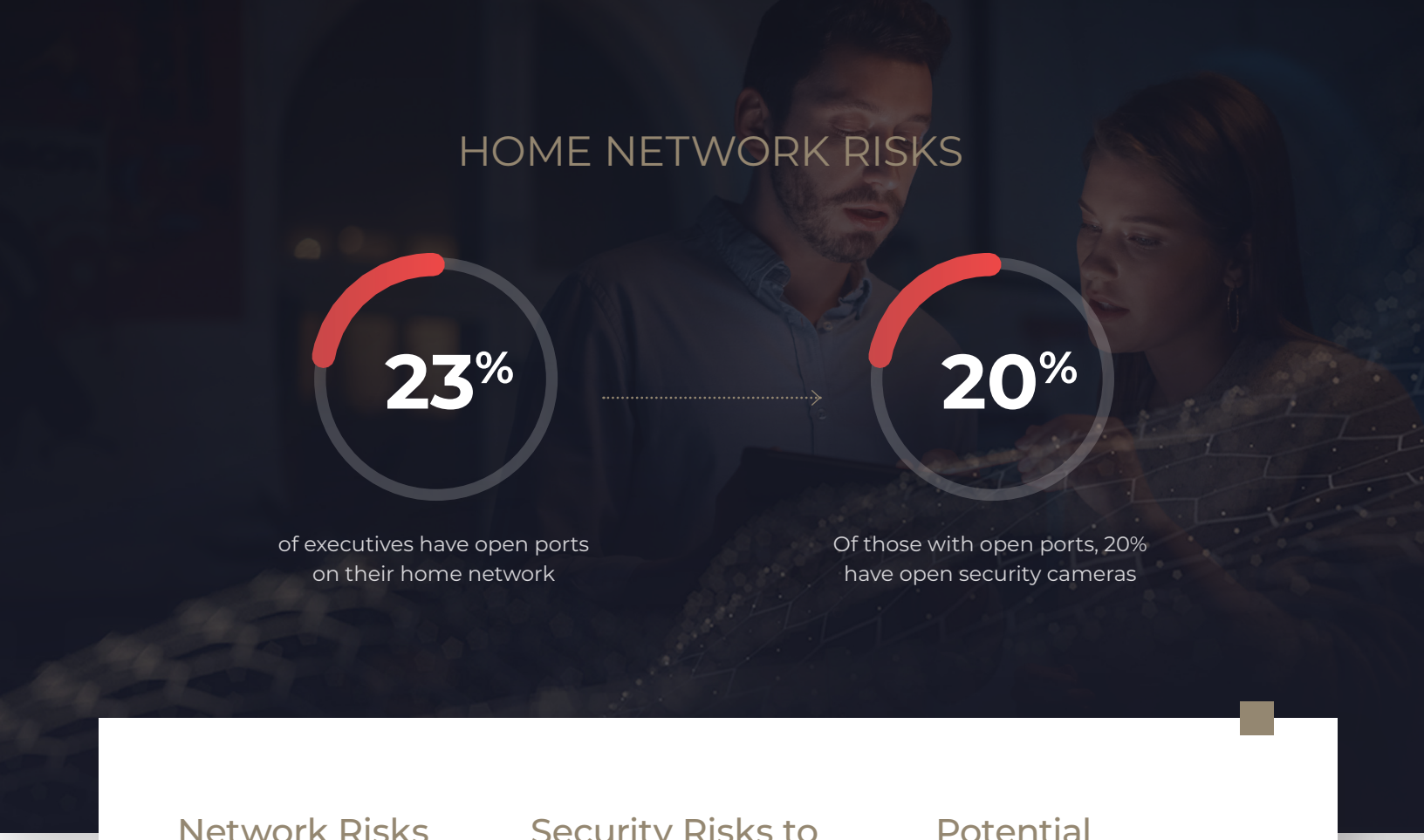
BlackCloak researchers aggregated and anonymized home network, personal device, and online privacy data from over 1,000 members prior to their onboarding. The individuals are members of the C-Suite and Board, or are high-profile executives at more than 55 US-based Fortune 1000s, with roles spanning CEO, finance, legal, operations, sales, R&D, engineering, IT, and other positions of prominence and great responsibility.

Home network security is an afterthought

The connected home is a prime target for cybercriminals. But few executives or CISOs realize the threat. BlackCloak research has found that nearly a quarter of executives have open ports on their home network public IP (Internet Protocol) address.

This is an unusual setup, as open ports are not typically accessible in standard home environments. These ports are often devices setup by third party solution providers for home theater and automation, internet accessible security cameras, networking devices like routers, firewalls and VPNs, and other IoT uses. Oftentimes they are misconfigured or running out of date firmware and have multiple vulnerabilities.

This open port prevalence expands the opportunity for threat actors to target your company by compromising the home network. After all, it is infinitely easier to breach an open port on a home network and move laterally into an organization than it is to compromise a corporate network protected by multiple layers of security controls.



HOME NETWORK RISKS

23%

of executives have open ports on their home network

20%

Of those with open ports, 20% have open security cameras

Network Risks to Executives

- Privacy Intrusions
- Email Account Takeover
- Communications Hijacking/Eavesdropping
- Man-in-the-Middle Attacks
- Network Compromise /Internal Device Compromise
- Physical Security
- Botnet Infections
- Blackmail/Extortion
- Social Media Account Compromise

Security Risks to the Company

- Loss of Confidential Data /Intellectual Property
- Lateral Attacks on the Company
- Compromised Passwords Used at Work
- Reputational Risks
- Network Compromise/Internal Device Compromise
- Work Device Compromise
- Denial-of-Service Attacks
- Employee Account Compromise

Potential Business Impact

- Compromised Data
- Compromised Work Devices
- Lost Productivity
- Legal/Information Security Investigations
- Lost Revenue

MOST VULNERABLE HOME NETWORK ASSETS

1. **HOME SECURITY CAMERAS**
2. **HOME ROUTERS /FIREWALL**
3. **AUDIO/VISUAL EQUIPMENT**
4. **CONNECTED HOME STORAGE**

Personal devices often lack the most basic protections

Your executives are increasingly using their personal devices for work. Even before the pandemic, 75% of the U.S. workforce used their personal phones for work, such as accessing corporate resources (Zippia). Moreover, the average employee uses 2.5 devices for work, including laptops, smartphones, tablets, and e-readers.

However secure corporate-owned devices are, personal devices are equally, if not more, insecure. Most personal devices lack basic security software and regularly leak data due to missing or improperly configured device settings – potentially exposing your executives and your company to risk.

Device risks
(Desktop, mobile & tablet)

27% of executives' personal devices contain malware

76% of executives' personal devices are actively leaking data

87% of executives' personal devices have no security installed

Device Risks to the Executive

- Malware & Ransomware
- Account Takeover
- Unpatched Zero Day Exploit
- Data Breach
- Device Takeover
- Financial Fraud

Security Risks to the Company

- Lateral Attacks
- Malware & Ransomware
- Account Takeover
- Breach of Confidentiality
- Reputation Damage

Potential Business Impact

- Lost Revenue
- Disruption of Business Continuity
- Reputation Damage
- Compromised Intellectual Property
- Compromised Data

MOST COMMON DEVICE THREATS

1. **MALWARE (VIRUSES & TROJANS)**
2. **EXPLOITS FROM UNPATCHED DEVICES**
3. **ADWARE**
4. **POTENTIALLY UNWANTED APPLICATIONS**
5. **WI-FI THREATS FROM MALICIOUS NETWORKS**

Executives' online privacy is not very private

According to Pew Research, 79% of Americans are worried about the protection of their personal information. Despite the hard work of security teams, privacy protections on corporate devices, accounts, and home networks cannot transfer into your executives' personal digital lives. Yet, breaches of executive privacy make it significantly easier for cybercriminals to pull off targeted attacks.

BlackCloak research reveals that most personal accounts, such as email, e-commerce, and applications, lack basic privacy protections. In addition, by default, many devices have geo-location enabled, which can make an executive's whereabouts available for anyone to see—putting them at risk of physical harm.

Our data analysis also found that the security credentials of executives — such as bank and social media passwords – are readily available on the dark web, making them susceptible to social engineering attacks, identity theft, and fraud. Further, hundreds of data brokers are selling, or sometimes giving away for free, executives' personal information.

Data Brokers

99% have their personal information available on more than three dozen online data broker websites, with a large percentage listed on more than 100

70% of executive profiles found on data broker websites contained personal social media information, most commonly from LinkedIn and Facebook

40% of online data brokers had the IP address of an executive's home network

95% of executive profiles contained personal and confidential information about their family, relatives, and neighbors

Password Security

8% have multi-factor authentication active across a majority of apps/devices

87% have passwords that are currently leaked on the dark web

53% are not using a secure password manager to protect their login credentials

54% have poor password hygiene. This means they do not use a password manager, they regularly reuse passwords and they store passwords in insecure locations (e.g. Excel)

68% write down their passwords on personal notebooks or store them in their contacts list on their phone

Privacy Risks to Executives

- Identity Theft
- Financial Fraud
- Account Compromise (Email, Software)
- Social Media Compromise
- Credential Theft
- Impersonations & Spoofing
- Communications Hijacking
- SIM Swapping

Security Risks to the Company

- Unauthorized Access (VPN login)
- Phishing/Social Engineering Attacks
- Data Breach
- Credential Theft
- Password Spraying
- Ransomware

Potential Business Impact

- Disruption of Business Continuity
- Reputation Damage
- Compromised Intellectual Property
- Compromised Data
- Lost Revenue

Your security teams lack visibility

Unfortunately, security teams lack visibility into what goes on in an executive's home. They have no insight into the security of the home network, the personal devices used, the personal email accounts, credentials, and password reuse between home and company accounts. Once your high-value employee leaves the confines of the offices, the enterprise can do little to protect them in their personal lives.

5 Reasons Why CISOs Cannot Protect Personal Digital Lives

- Undue Employee Burden
- Potential for Employee Discrimination
- Potential for Reputation Damage
- Ethical Risks
- Reporting Liabilities

Protect your executives, protect your company

Digital executive protection by BlackCloak is the answer to protecting your company by protecting your executives in their personal digital lives. Our award-winning Concierge Cybersecurity and Privacy Platform combines online privacy protection, personal device security, and home network security with 24/7 incident response, a US-based SOC and bespoke client service with concierge support calls being answered by a highly-trained, cybersecurity or privacy analyst. With BlackCloak as your partner, you can rest easy knowing that your high-profile employees are protected 24 hours a day, including when outside of corporate security control.

AWARDS

BLACKCLOAK™

ask@blackcloak.io
1.833.882.5625 Ext 1

www.blackcloak.io

About BlackCloak

BlackCloak protects corporate executives and high-profile individuals from cybersecurity, privacy, financial, and other reputational risks. Used by Fortune 500 companies across all industries, the BlackCloak Concierge Cybersecurity & Privacy™ Platform is a holistic solution including mobile and desktop apps as well as concierge support. Executives and high-profile individuals get peace of mind knowing their family, reputation, and finances are secured. Companies rest assured that their brand, intellectual property, data, and finances are protected against threats coming through executives without having to invade their personal lives. Learn more at **blackcloak.io**