BLACKCLOAK® | Ponemon INSTITUTE

Digital Executive Protection Research Report 2025

Contents

Introduction

As security improves within organizations, cybercriminals are increasingly targeting individuals with access to high-value confidential information by attacking their home networks, compromising unsecured devices with malware and ransomware. Over the years, we have seen a number of successful attacks on executives from Microsoft, Dragos, United Healthcare, Twitter, Amazon and Meta, with many more occurring and left unreported in the media.

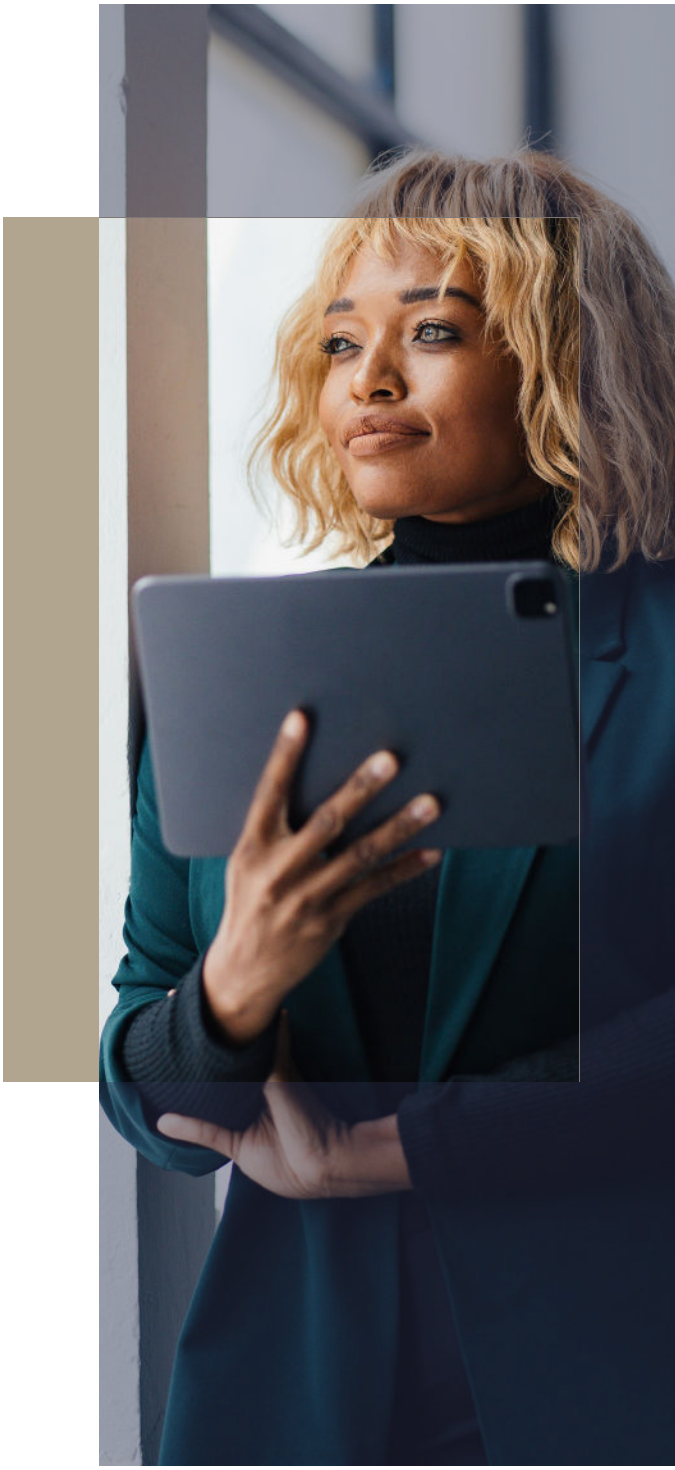
Cybercriminals are exploiting a unique combination of privacy concerns, legal limitations, resource constraints, and information exposure that prevents corporate teams from fully safeguarding executives' personal digital lives. As such, these individuals have become the path of least resistance for a motivated threat actor and an easy stepping stone to their lucrative final target.

Attackers frequently target poorly secured home networks and devices, leveraging reused passwords and advanced tactics like deepfake impersonations. This report, based on an independent survey by the Ponemon Institute of 586 U.S. security professionals, illustrates the depth of the problem and outlines the nature of these targeted attacks.

Key insights include:

- Frequency and nature of attacks on executives and their families
- Tactics, techniques and procedures deployed
- Emergence of deepfake attacks
- Challenges in protecting personal digital assets

The findings reveal a dangerous cycle that organizations unknowingly perpetuate, leaving executives and the organizations they represent vulnerable to cybercriminal exploitation.



Key findings

- 51% of respondents reported the personal digital lives of their executives had been directly targeted by a cybercriminal in the 2 years preceding 2025
- Cybercriminals continue to disrupt the personal lives of the executive targeted as well as the organization following a breach
- 68% of security professionals believe it likely an executive would unknowingly reuse a compromised password from their personal accounts inside the company
- There is low overall confidence that executives and their families understand the threat to their personal digital assets
- Security teams are struggling to obtain the visibility they need into their executives' personal digital lives to protect them

22%

of those targeted

experienced 7 to 10 cyber attacks in the last 2 years

62%

of respondents

anticipate their executives' personal digital lives will be targeted by a cybercriminal in the future

41%

of respondents

reported deepfake incidents targeting their executives

only 43%

of respondents

provided training for executives to secure their personal digital assets

Rising frequency of attacks

Between 2023 and 2025, the percentage reporting targeted attacks on executives increased from 43% to 51%. Of those impacted in 2025, 22% had experienced 7 to 10 cyber attacks, an increase of 32% over 2023. Concern over potential attacks in the future remains consistently high at 62%.

Number of times a cyberattack was experienced by executives against their personal digital lives

(only respondents who reported a cyber attack had occurred answered this question)

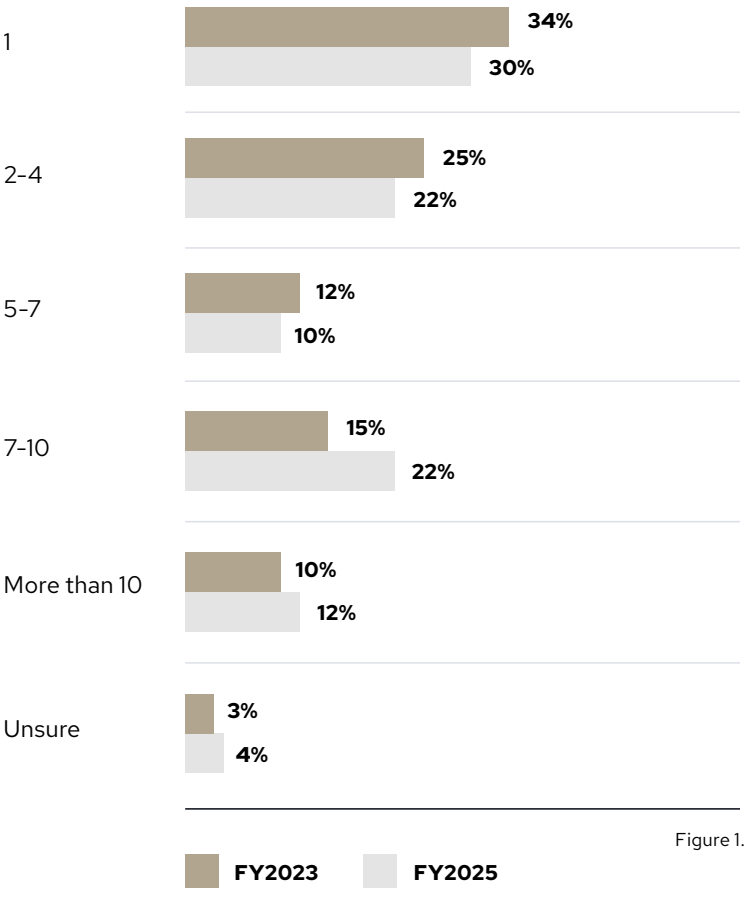


Figure 1.

Threat actor tactics, techniques & procedures

The most prevalent attacks continue to be malware on personal or family devices and the exposure of personal information such as their home address, phone number and personal email address.

What types of attacks did your executives experience?

(Three responses permitted)

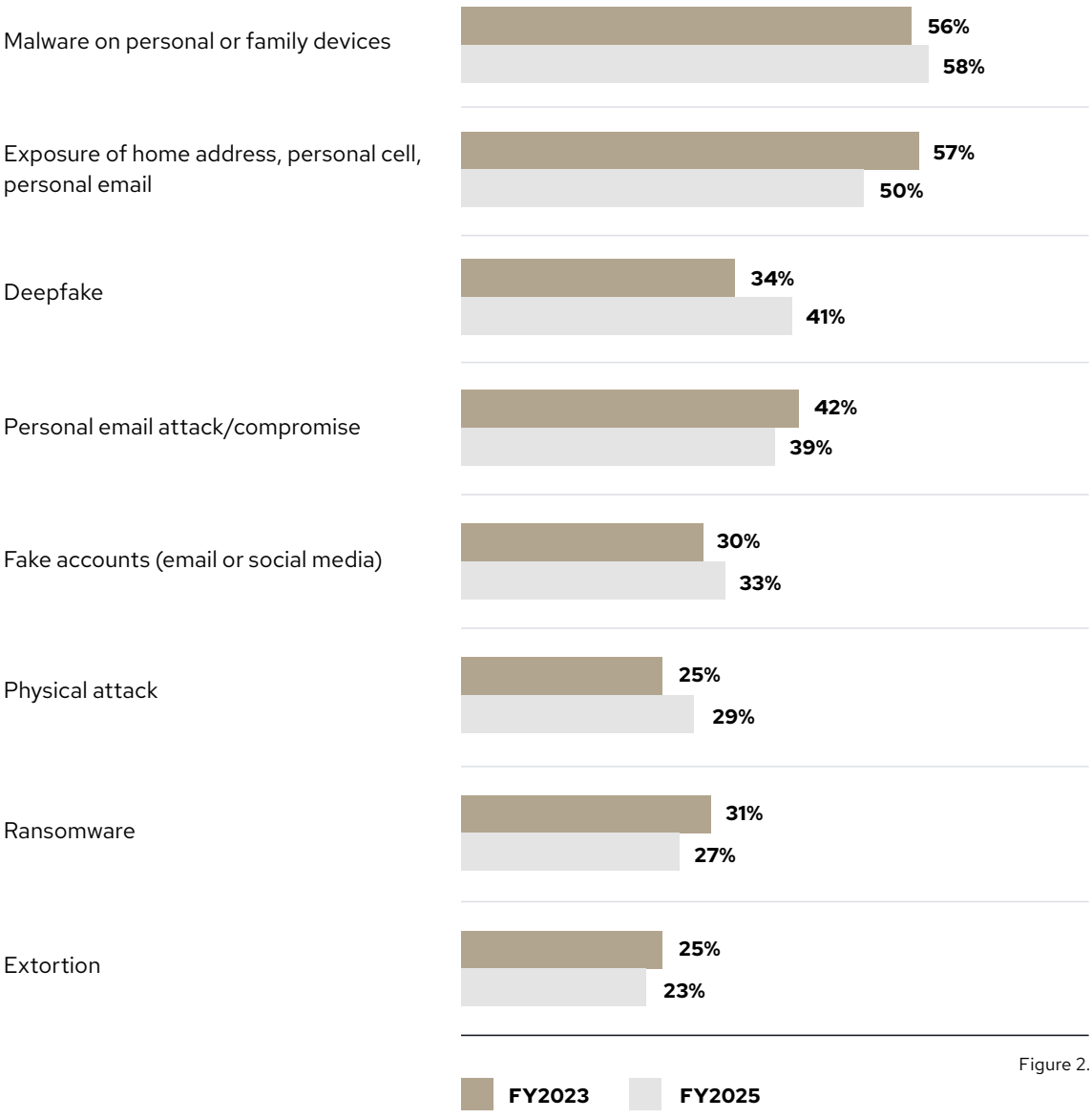


Figure 2.

Deepfake attacks: An emerging threat

Although AI is still in its infancy, threat actors are rapidly exploiting its powerful capabilities to scrape data on their targets from the internet, creating realistic profiles or communications that could fool even the most vigilant of individuals. As such, deepfake attacks targeting executives have increased significantly in the last two years, from 34% of respondents reporting an incident in 2023 to 41% of respondents in 2025.

The impersonation of trusted contacts and urgent demands for payments/information about a detected security breach have been the most commonly deployed tactics.

How have deepfakes targeted your executives?

(One response permitted)

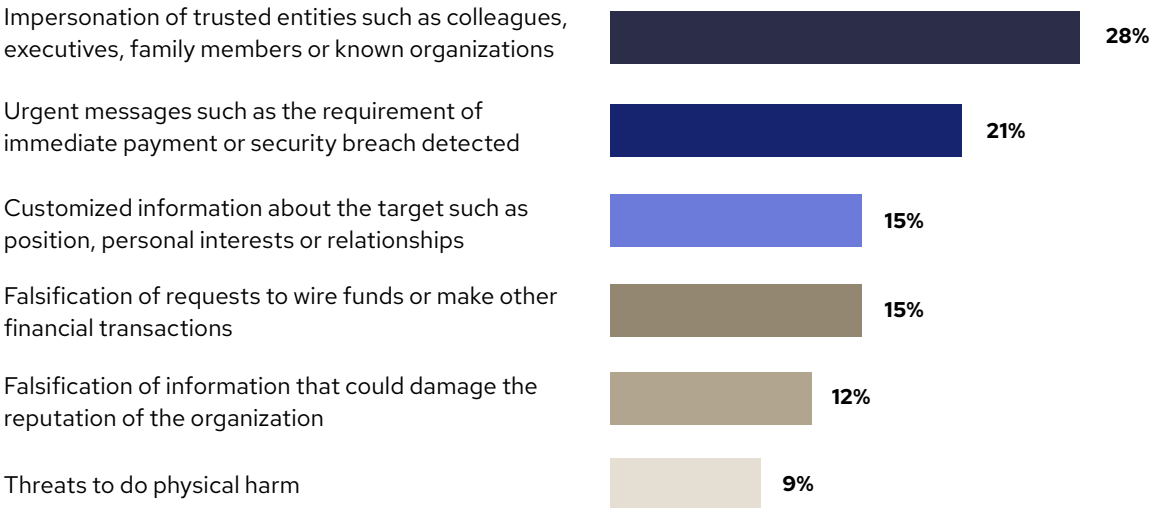


Figure 3.

A deepfake is an artificial image or video generated by a form of artificial intelligence (AI) called deep learning. Typically, the attacker starts by collecting authentic media samples of their target to use as training material for the deep learning model. These samples include still images, videos and audio clips. The more training data the attacker acquires, the more authentic the resulting deepfake will appear.

The deepfake tactics of greatest ongoing concern are social imposters (53% of respondents) and financial fraudsters (37% of respondents). The impersonation of trusted contacts and urgent demands for payments/information about a detected security breach have been the most commonly deployed tactics.

What are the top two deepfake risks concerning your organization?

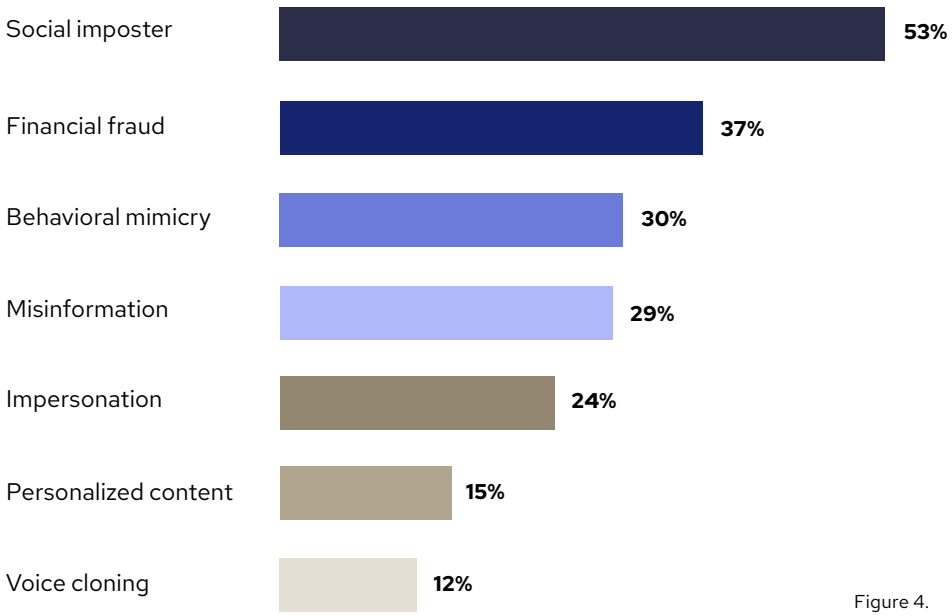


Figure 4.

Physical and digital threat convergence

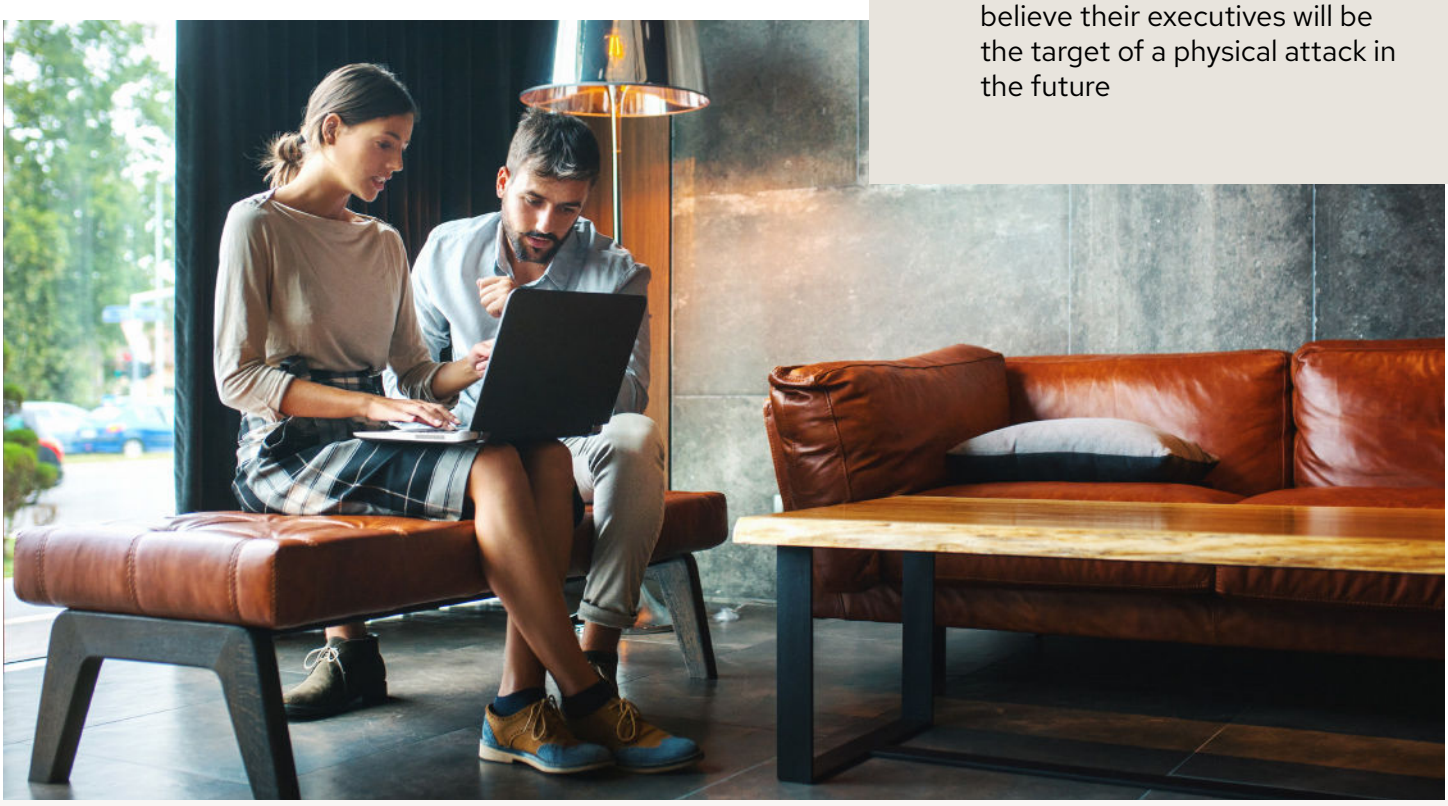
One of the most severe consequences of a digital attack on an executive is the ability to use their personal information to cause physical harm. Fifty percent of security professionals believe their executives will be the target of a physical attack in the future. To combat this threat, 63% of respondents say their organization currently provides self-defense training for executives, an increase of 15% from 2023's report.

In stark contrast, despite 62% of security professionals believing their executives are highly likely to be the target of a cybercriminal attack in the future, only 43% have provided training on how to secure their personal digital assets, 38% of which took place following an attack. Notably, 50% of respondents had no plans to train their executives to recognize a deepfake attack.

50%

of security professionals

believe their executives will be the target of a physical attack in the future



A breach is both business and personal

A cyber attack on the personal digital assets of a corporate executive can have far-reaching consequences. Not only can the individual suffer personal financial loss or reputational damage, but the broader implications can also significantly affect the organization they represent.

Personal devices used for work-related activities or open home networks could give cybercriminals a 'free pass' into the corporate environment if breached. From there, the company's operations, intellectual property, finances, business relationships and reputation are at risk. There may also be legal and compliance consequences, as data breaches often result in regulatory fines for failing to protect sensitive information.

Since 2023, there has been a noteworthy increase in the theft of intellectual property and improper access to the executive's home network as a result of a targeted attack. Although financial loss continues to be the main impact of a breach, intellectual property theft and access to home networks have taken the 2nd and 3rd slots respectively in 2025. This marks an interesting shift from 2023's research, which reported a loss of business partners and non-compliance with regulations in positions 2 and 3 respectively.

The inclusion of improper access to the executive's home network in the top 3 consequences of a successful breach suggests how indiscriminate threat actors are once they gain access – they are increasingly likely to continue disrupting the individual's personal life as well as the corporation.

Organizations are largely in the dark about the severity of the financial consequences of a personal cyberattack. Only 43% of respondents measure the potential impact of a cyberattack against their executives.

Digital assets include all aspects of an executive's personal life including phones, tablets, laptops, gaming equipment, home security cameras, IoT devices, online accounts (email, financial, retail, social, etc.) and home networks.

What were the consequences of a cyberattack against the lives and/or digital assets of executives?

(More than one response permitted)

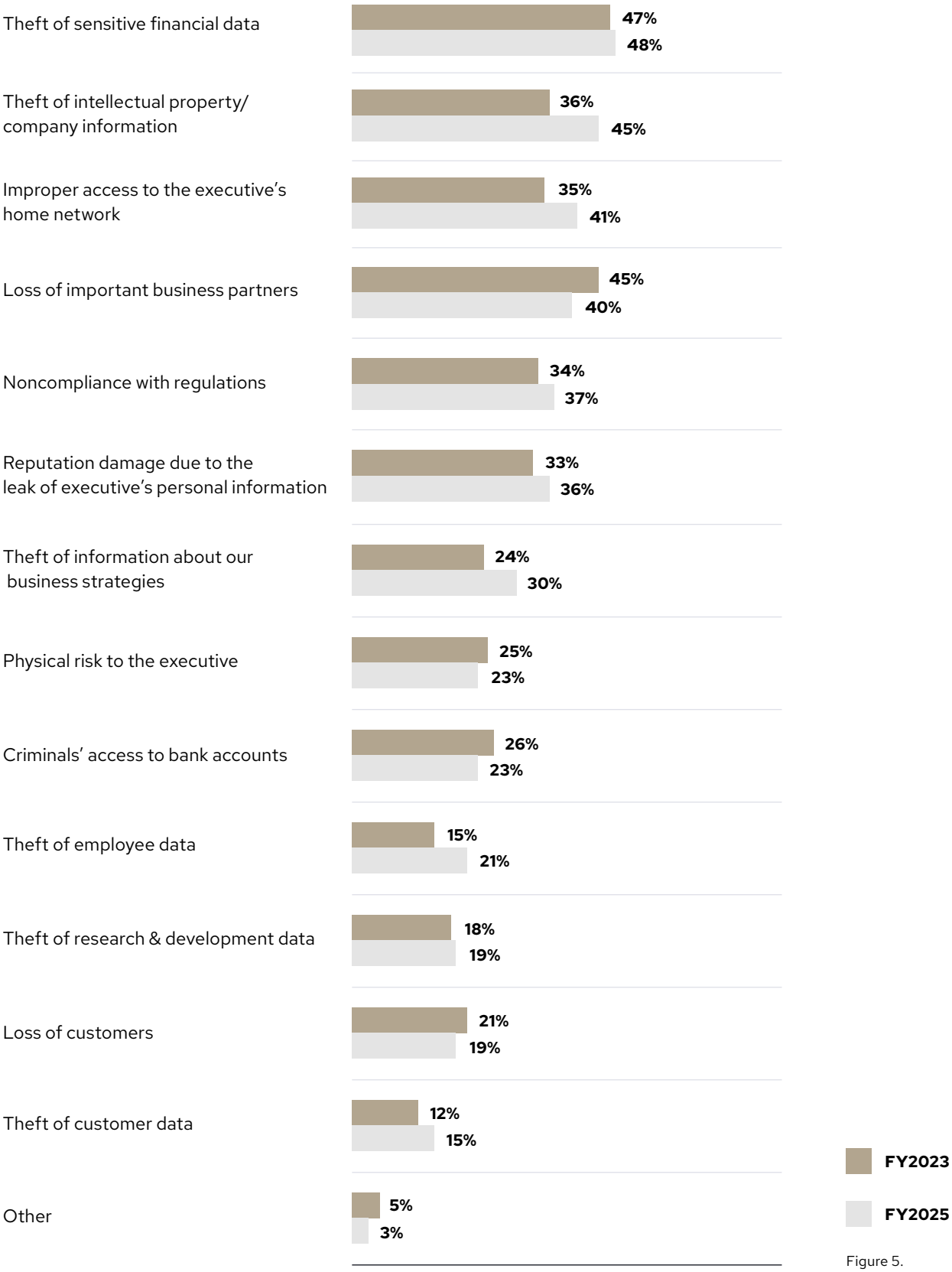


Figure 5.

The challenge of protecting executives' digital lives

Over the last 5 years, corporate cybersecurity teams have raced to overcome the increased security challenges caused by remote working. Solutions such as security service edge and cloud-native application protection platforms have boomed during this period, however, executives often transition from their homes to the office environment using personal devices that are not covered by corporate security.

Compounding the problem, security teams are clearly struggling to track threat actors targeting their executives and there is little confidence that the executives themselves understand the threat their personal digital lives pose to the organization they work for. This perhaps is a consequence of a lack of training and awareness – respondents reported low commitment levels to regular cybersecurity training overall.

The challenges of protecting executives' digital assets

(Strongly agree and Agree responses combined)

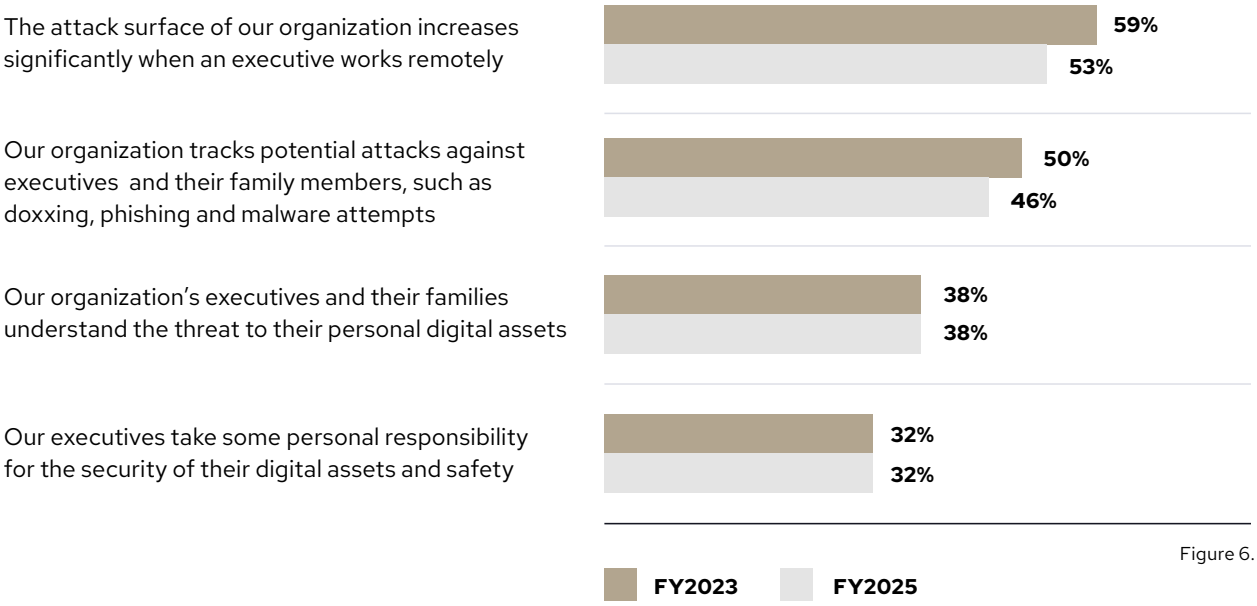


Figure 6.

68%

of security professionals

believe it is likely an executive would unknowingly reuse a compromised password from their personal accounts inside the company.

Difficulty stopping cyberattacks against executives and their digital assets remains high.

Many security professionals find themselves at an impasse as they try to find practical solutions that provide real security while enabling executives to seamlessly stay connected to their corporate lives from remote locations. Despite bearing the responsibility for securing the digital lives and assets of C-Suite executives, it continues to be highly difficult for security professionals to have sufficient visibility into executives' home networks, personal devices, personal email accounts, password hygiene and privacy footprint to assess possible vulnerabilities and prevent fast-growing threats such as deepfake attacks.

Difficulty in reducing risks

(One a scale from 1 = not difficult to 10 = highly difficult. Responses with scores of 7+ are presented)

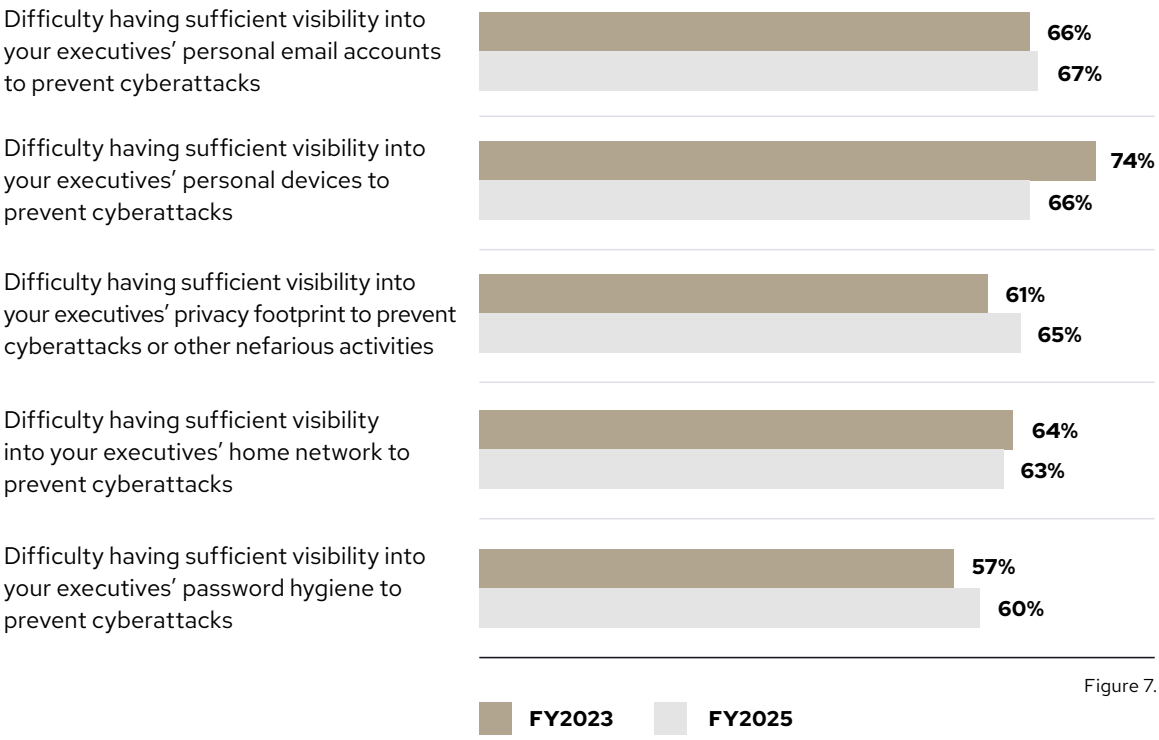


Figure 7.

Visibility issues affect response to emerging attack TTPs

When exploring the impact of these visibility challenges on a specific attack tactic such as deepfakes, 50% of respondents say their team did not have the insight required to prevent a breach. It is therefore not surprising that the majority of respondents rated detecting a deepfake attack as difficult.

Rate the difficulty to detect a deepfake targeting your executives

(1 = not difficult to 10 = highly difficult)

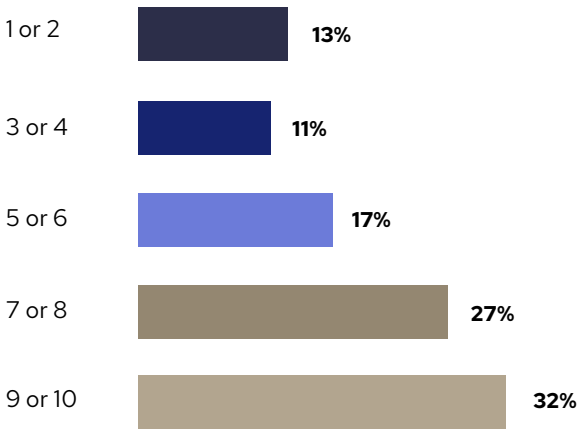
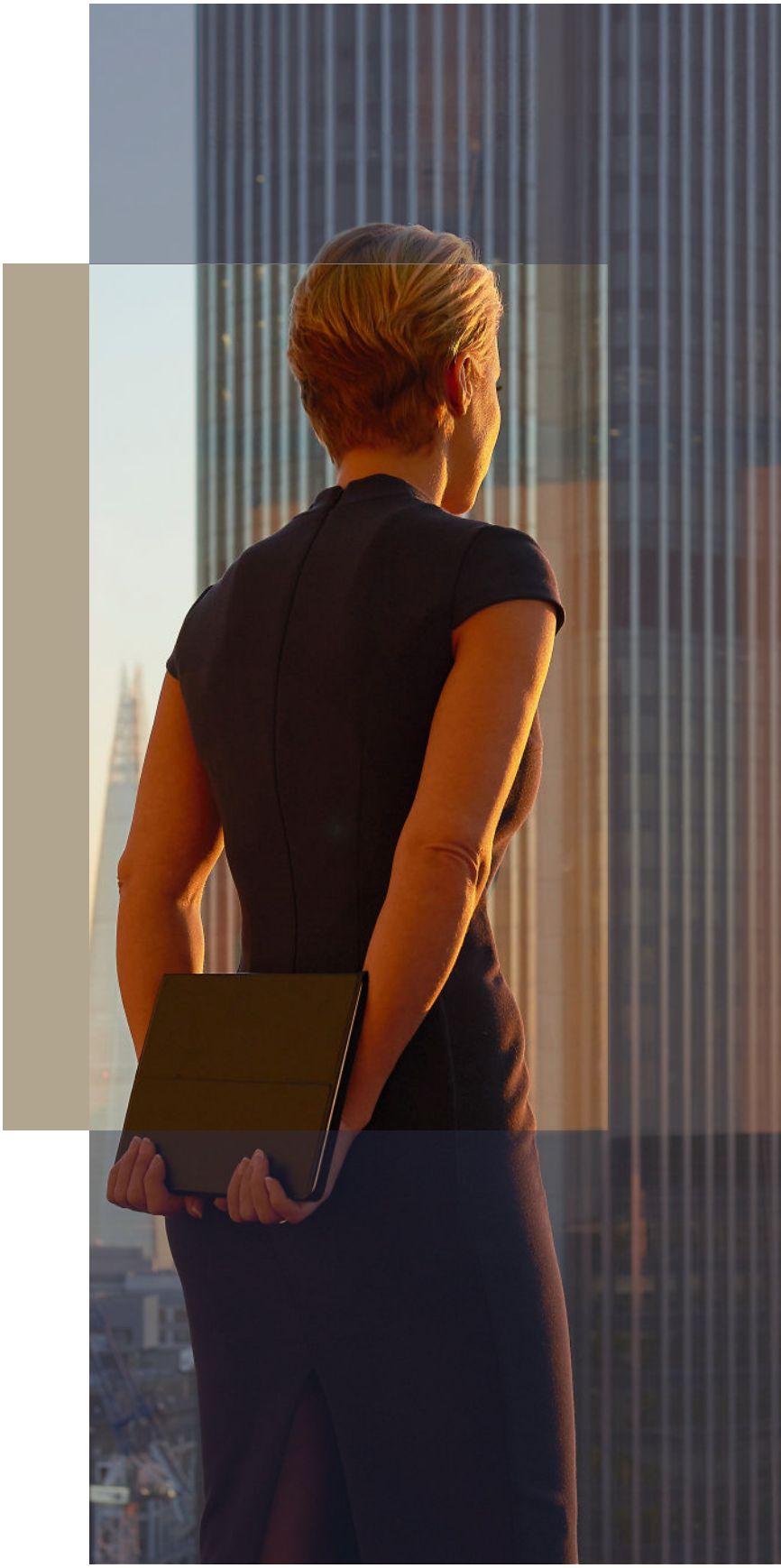


Figure 8.



This creates a very real problem for security teams. The lengths they now must take to prevent cybercriminals from attacking the digital assets of executives outside the organization represent an undue burden.

Security professionals are left with no option but to rely on executives to know how to protect their devices, and there is evidently little confidence in their capabilities to do so.

Confidence level of security professionals in the capabilities of executives to secure their personal digital lives

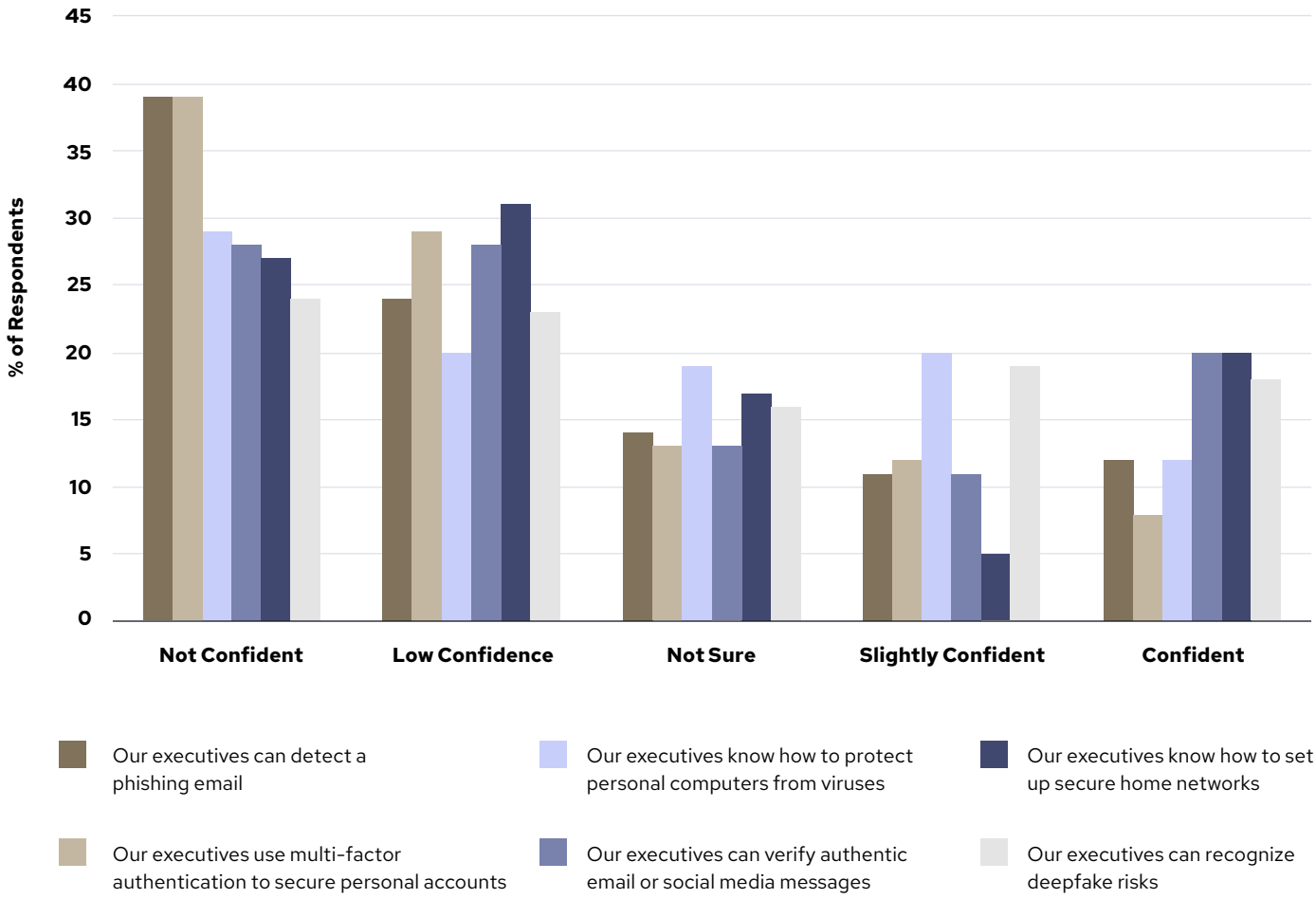


Figure 9.

Despite recognizing the risks executives and their families pose to their organization, only 48% incorporate Digital Executive Protection into their security strategies or budgets—marginally up from 42% in 2023. This oversight, combined with inadequate training, low levels of targeted threat tracking and limited visibility into their executives' digital lives leaves organizations at an impasse, with an open door for cybercriminals.

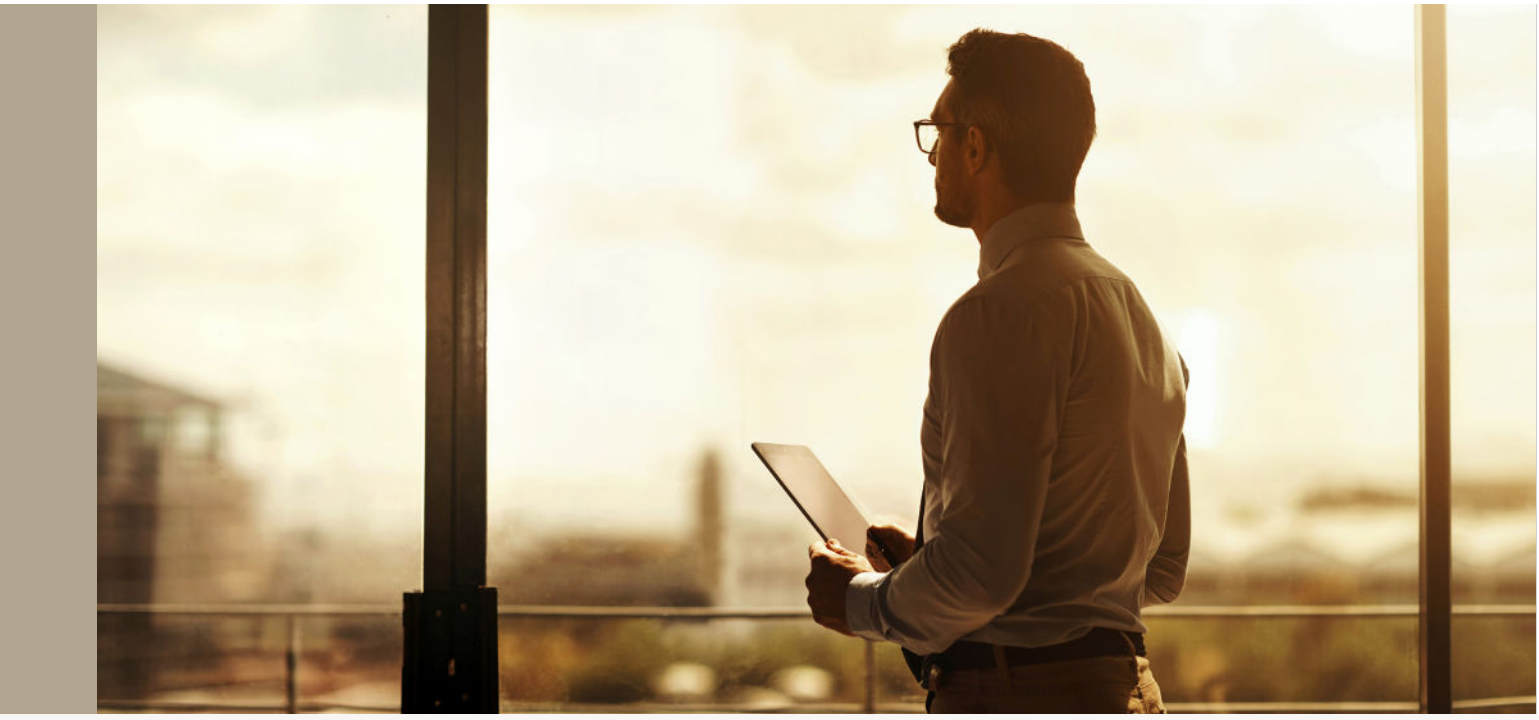
Overstretched security teams, a lack of understanding of DEP and (until recently), the absence of a proven framework have perpetuated this cycle.

What is Digital Executive Protection?

Digital Executive Protection extends cybersecurity beyond the corporate perimeter by safeguarding the personal digital lives of company executives, board members and key personnel. It minimizes their attack surface exposure without overburdening internal security teams and with minimal disruption to the lives of those it protects.

Digital Executive Protection is more than privacy protection. Cybercriminals target family members too. Over 50% of organizations surveyed believe it is highly likely an executive's partner or child will click on a link in a phishing email as part of a targeted campaign.

For Digital Executive Protection to be truly effective, it must be holistic and protect the entire family - not just the executive from cyber attacks - addressing all possible factors and circumstances of a cyberattack, treating them as an interconnected whole.



A new framework for Digital Executive Protection

To help organizations protect themselves and their executives from resourceful threat actors, BlackCloak has released the first-ever DEP framework, the culmination of years of experience providing the highest level of cybersecurity protection for executives in their personal digital lives.

Consisting of 14 key tenets, the DEP framework encompasses a range of services and technologies designed to:

- **Reduce the digital footprint of executives and their families:** Minimizing the amount of personal information exposed online.
- **Monitor personal devices and home networks for threats:** Proactively identifying and mitigating potential cyber risks.
- **Educate and train:** Empowering executives and their families to make informed decisions about their online activities.
- **Perform incident response:** Rapidly addressing threats before they escalate into breaches of the enterprise.

The framework is available from BlackCloak and is free for all security teams to download.

Get your copy

Key Components of Digital Executive Protection

Privacy:
Protecting personal information from unauthorized access and exposure.

Identity Theft Protection:
Monitoring for and mitigating identity theft risks.

Deepfake Protection:
Detecting and preventing the malicious use of AI-generated synthetic media.

Financial Protection:
Safeguarding personal finances from cyberattacks and fraud.

Personal Device Hardening:
Reducing vulnerabilities and minimizing the risk of unauthorized access.

Cybersecurity/Personal Device Protection:
Securing personal devices from malware.

Home Network Hardening:
Protecting home networks from intrusion.

Home Network IoT Monitoring & Protection:
Securing all connected devices within the home.

Social Media Hardening:
Hardening social media accounts and managing online reputations.

Family Protection:
Extending protection to family members who may be targeted through association.

Physical Protection:
Integrating physical security measures with digital protection strategies.

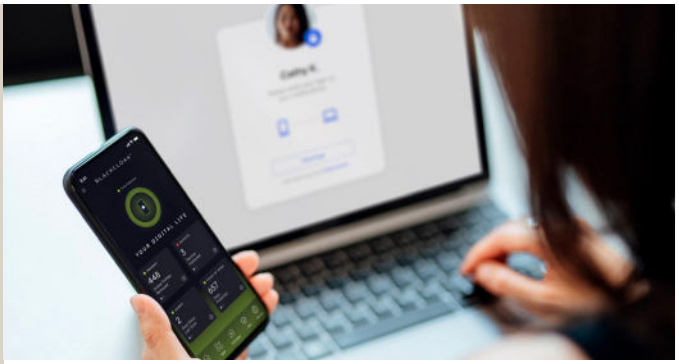
Personal Cyber & Identity Theft Insurance:
Conducting detailed risk assessments and offering expert recommendations.

Education and Training:
Providing ongoing education and training to executives and their families on cybersecurity best practices.

Incident Response:
Providing coordinated strategies to quickly identify, contain, and mitigate personal security incidents that impact the company.

BlackCloak Digital Executive Protection

BlackCloak's tailored technology, paired with expert concierge support, proactively shrinks executives' digital footprints, monitors and secures home networks, and provides comprehensive device protection. Our holistic solution aligns with your corporate security strategy without burdening internal resources.



Protect your executives' privacy

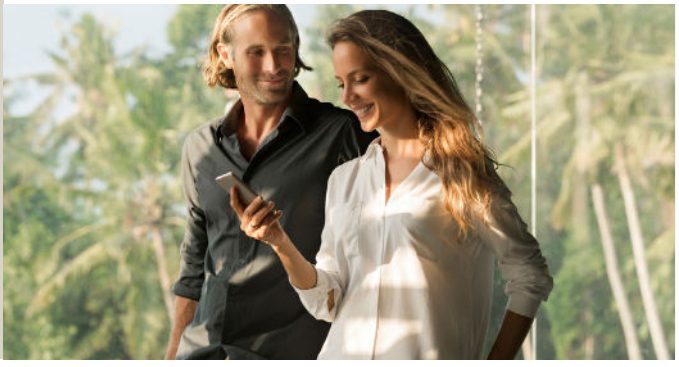
We remove sensitive personal information from the internet, perform dark web searches for exposed personal credentials and implement privacy settings to protect the identities of key employees and their families. We also provide the tools to protect everyone online, including a VPN and identity verification to prevent deepfake video calls.

Protect your executives' homes

We perform penetration testing and regular scans of home networks to detect compromised networks, weak cybersecurity, BotNets and to prevent decisions children and family make online from resulting in a compromise. We also work with home security and smart technology providers to identify and resolve system vulnerabilities.

Protect your executives' devices

We monitor, detect, prevent, and block threats to your executives' personal devices, such as malware and ransomware, that occur when someone accidentally clicks on a malicious link or opens malware from a phishing scam. Our US-based security operations center remediates any attacks that are detected.



Protect everyone's peace of mind

We provide the high-touch, on-demand and meticulously transparent service experiences your executives are accustomed to in both their work and personal lives. Our concierge team is available around-the-clock to answer queries, provide support and deliver ongoing cybersecurity training to prevent a breach.

Methodology

A sampling frame of 17,100 IT and IT security practitioners who are knowledgeable about the programs and policies used to prevent cybersecurity threats against executives and their digital assets were selected as participants to this survey. Table 1 shows 633 total returns. Screening and reliability checks required the removal of 47 surveys. Our final sample consisted of 586 surveys, or a 3.4 percent response.

Sample Response	Freq	Pct%
Sampling Frame	17,100	100%
Total Returns	633	3.7%
Rejected or Screened Surveys	47	0.3%
Final Sample	586	3.4%

Table 1.

Primary person respondents report to within their organization

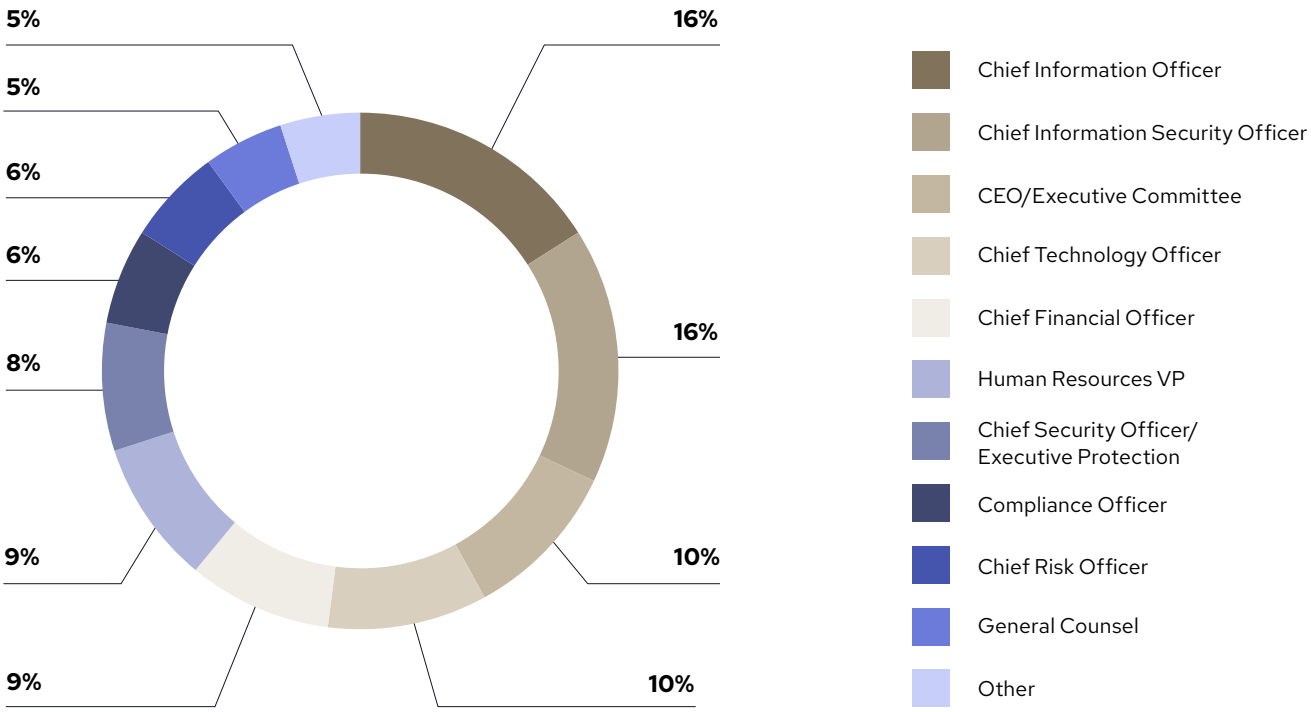


Figure 10.

The pie chart below reports the industry within which each respondent's organization operates.

Primary industry focus

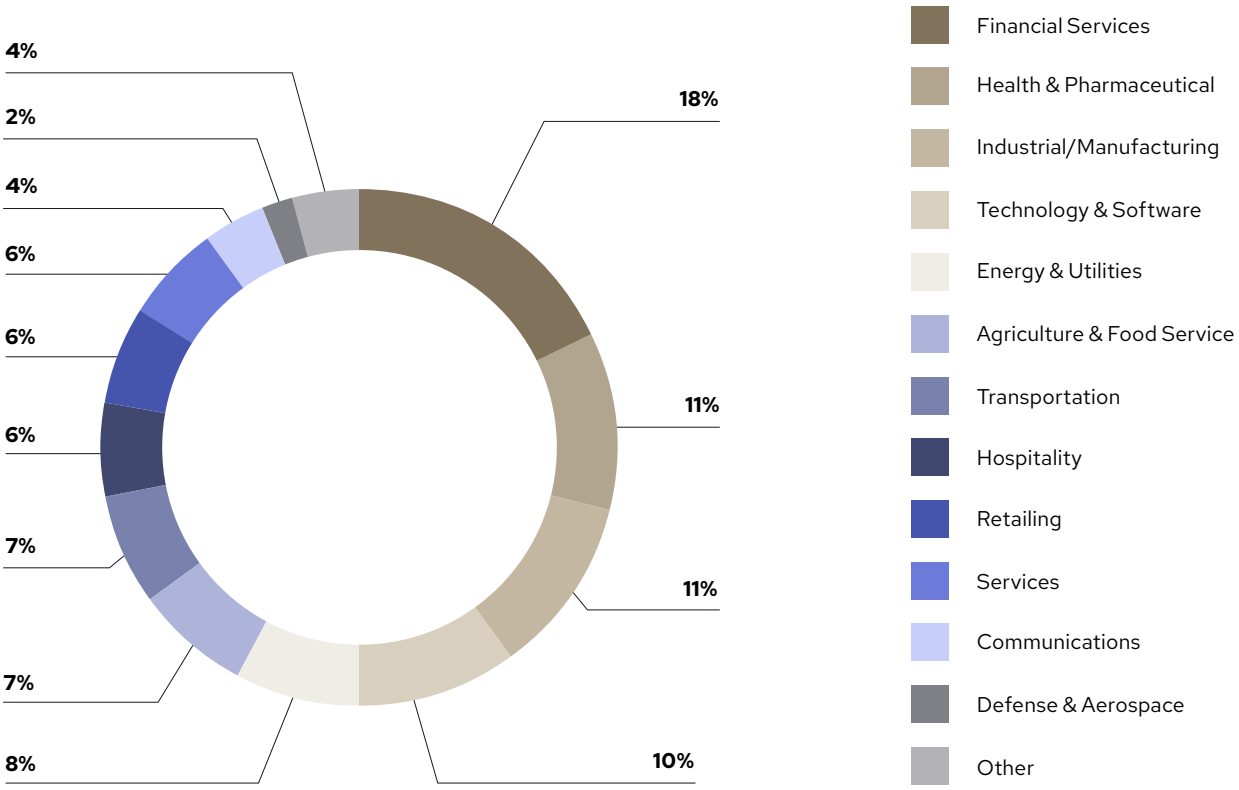


Figure 11.

As shown in the following pie chart, all respondents work for organizations with a global headcount of +1,000 employees.

Global full-time headcount

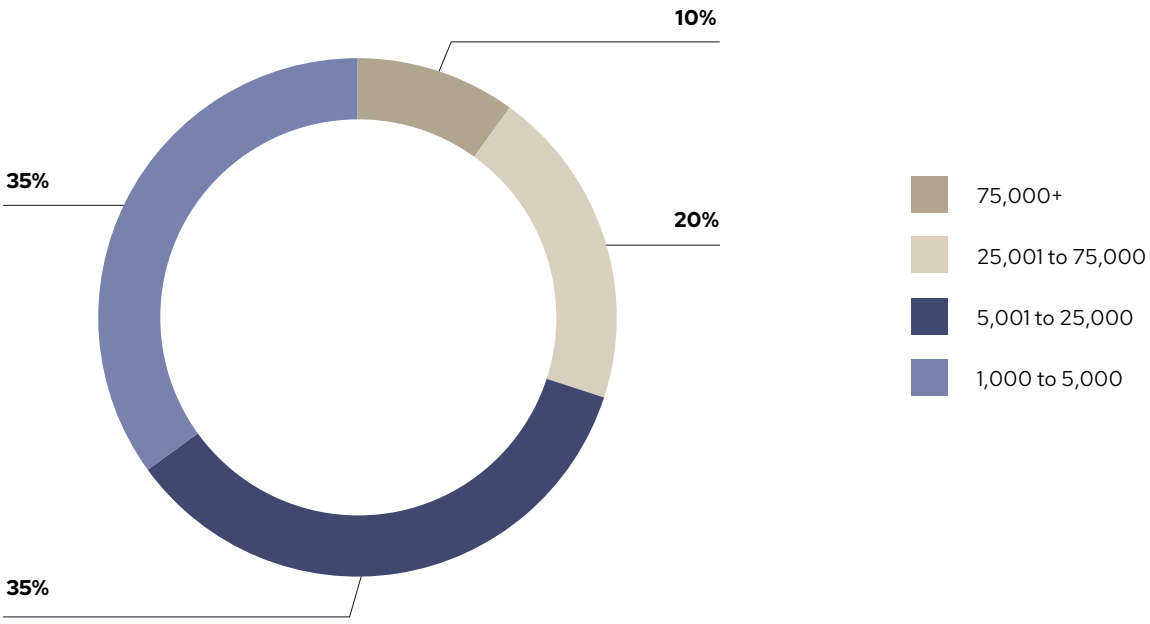


Figure 12.

Caveats to the study

There are inherent limitations to survey research that need to be carefully considered before drawing inferences from findings. The following items are specific limitations that are germane to most web-based surveys.

Non-response bias

The current findings are based on a sample of survey returns. We sent surveys to a representative sample of individuals, resulting in a large number of usable returned responses. Despite non-response tests, it is always possible that individuals who did not participate are substantially different in terms of underlying beliefs from those who completed the instrument.

Sampling-frame bias

The accuracy is based on contact information and the degree to which the list is representative of IT decision-makers and security professionals. We also acknowledge that the results may be biased by external events such as media coverage. Finally, because we used a web-based collection method, it is possible that non-web responses by mailed survey or telephone call would result in a different pattern of findings.

Self-reported bias

The quality of survey research is based on the integrity of confidential responses received from subjects. While certain checks and balances can be incorporated into the survey process, there is always the possibility that a subject did not provide accurate responses.

BlackCloak's experts come from intelligence agencies, banking and finance, aerospace and defense, hospitality, legal and compliance, as well as cybersecurity and anti-fraud companies. Some of our experts even hold Top Secret security clearances. We know cybersecurity & privacy because that is all we do.

In the media

The New York Times · FT Financial Times · The Washington Post · Forbes · Bloomberg

VentureBeat · the cyberwire · DARKREADING · SECUREWORLD · CSO

Read our media mentions

Our latest awards

Global Infosec Awards Winner Cyber Defense Magazine 2025 · 2025 Cyber 150 IT-Harvest · 2025 Globee Awards Silver Winner Cybersecurity · 2025 Winner Cyber Security Excellence Awards · Best Places to Work 2025 · Top Infosec Innovator Winner Cyber Defense Magazine 2024 · Black Unicorn Awards 2024 Finalist

See all our awards

BLACKCLOAK®

Get in touch for more information

info@blackcloak.io | www.blackcloak.io