BLACKCLOAK™

Ponemon INSTITUTE

Understanding the Serious Risks to Executives' Personal Cybersecurity & Digital Lives

SPONSORED BY BLACKCLOAK

INDEPENDENTLY CONDUCTED BY PONEMON INSTITUTE LLC

PUBLICATION DATE: MAY 2023

Table of Contents

01.

INTRODUCTION

Organizations are allocating millions of dollars to protecting their information assets and employees but are neglecting to take steps to safeguard the very vulnerable digital assets and lives of key executives and board members. Sponsored by BlackCloak, Ponemon Institute surveyed 553 IT and IT security practitioners who are knowledgeable about the programs and policies used to prevent cybersecurity threats against executives and their digital assets.

The purpose of this research is to understand the risks created by the cybersecurity gap between the corporate office and executives' protection at home. According to 42% of respondents, their key executives and family members have already experienced at least one attack by a cybercriminal.

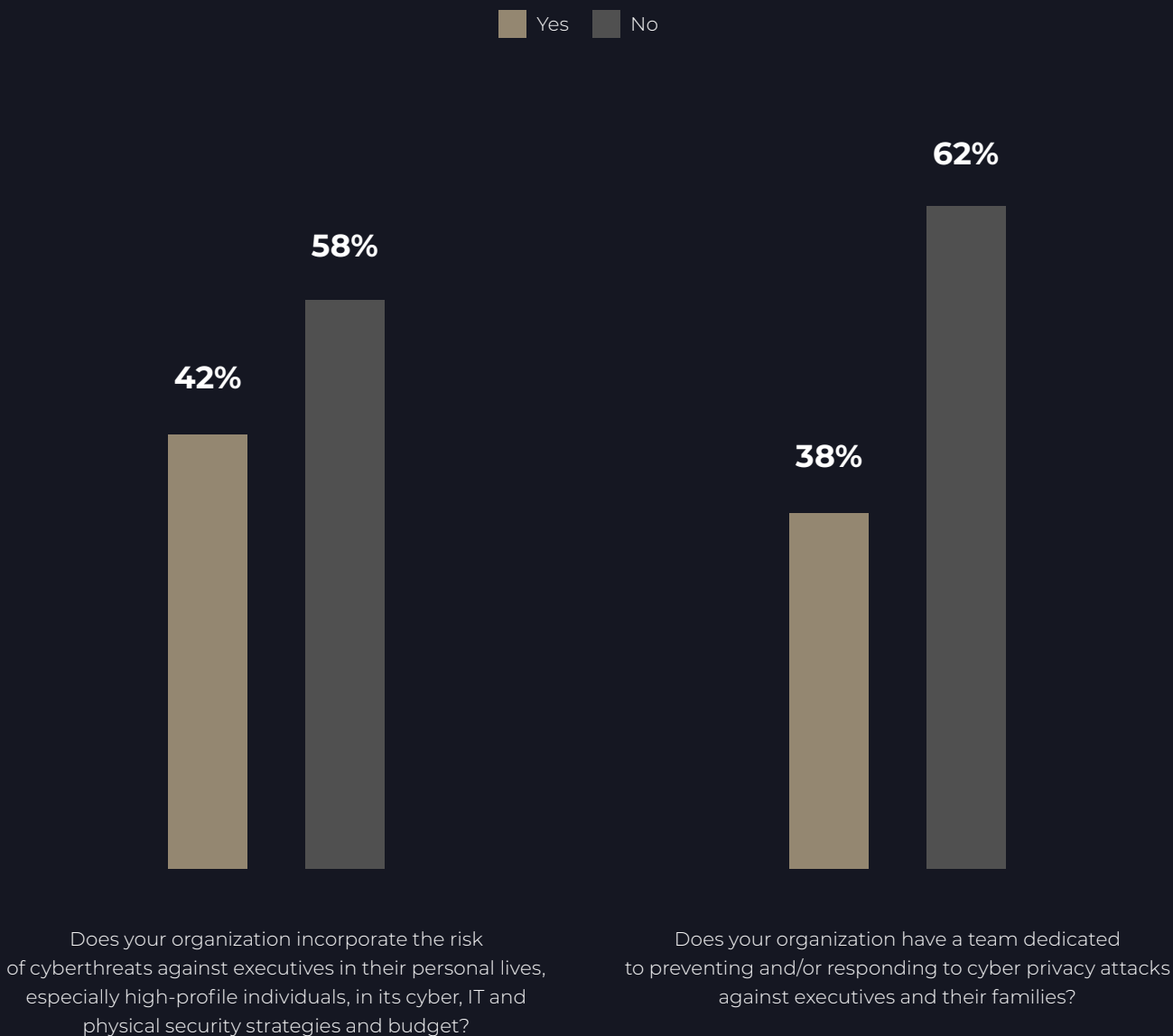
In the context of this research, **Digital Executive Protection** extends cybersecurity to outside the office domain by safeguarding the personal digital lives of company executives, board members and key personnel to mitigate the risks of cybercriminals targeting them for hacking, IP theft, reputational risks, doxxing/swatting and financial attacks.

Digital assets include all aspects of an executive's personal life: address/cell/emails; personal cell, tablet, computer and accounts (email, social etc.), home network and any scams targeting them (doxxing, swatting, personal exposure etc.).

A key takeaway from this research is that while it is likely that executives' digital assets and lives will be targeted by cybercriminals, organizations are not responding with much needed strategies, budget and staff. Specifically, as shown in Figure 1, 58% of respondents say the prevention of cyberthreats against executives and their digital assets is not covered in their cyber, IT and physical security strategies and budget. Moreover, only 38% of respondents say there is a dedicated team to preventing and/or responding to cyber or privacy attacks against executives and their families.

FIGURE 1

The current state of organizations' protection of executives' lives and digital risks



MAJOR THEMES

1. The threat to information security through C-Suite executives' personal digital lives and their assets are a real and constant concern among IT professionals.

2. These attacks often result in the loss of business, theft of sensitive data, and substantial expenses incurred in the process of identifying and remediating the threats.

3. There is little confidence that executives are adequately prepared or equipped to secure their own digital lives and assets.

4. These attacks create very real problems for those tasked with information security as they spend a disproportionate amount of time and concern working to secure key individuals' personal lives.

5. Many CISO's find themselves at an impasse as they try to find practical solutions that provide real security while still allowing executives to seamlessly stay connected to their corporate lives from remote locations.

The threat to information security through C-Suite executives personal digital lives and their assets is a real and constantly occurring issue. As security improves within organizations, cybercriminals are increasingly targeting individuals' private lives by attacking home networks and compromising unsecured devices with malware and ransomware. The attacks are not limited to C-Suite executives. Board members, senior and executive leadership teams and other key personnel are all potential targets. These breaches are not merely hypothetical: 42% of respondents reported that their executives or family members had been attacked by cybercriminals resulting in attacks ranging from malware and doxxing to instances of extortion and even physical attack.

These attacks often result in the loss of business, theft of sensitive data, and substantial expenses incurred in the process of identifying and remediating the threat. The effects of personal attacks are not limited to private consequences — there are also significant professional effects with 45% of respondents reporting a loss of important business partners and 33% reporting reputation damage due to the information exposed. The most common expenses associated with these attacks are incurred by the cost of the staff associated with identifying and responding to the threats.

There is little confidence that executives are adequately prepared or equipped to secure their own digital lives and assets. With remote work becoming more and more common and the expectation that executives are constantly within reach, it has become the norm that executives work from home, as well as other remote locations. However, respondents had very little confidence in the ability of executives to adequately assess threats or in the steps that they take to minimize these threats. On a scale of one to ten, with one being not confident and ten being highly confident, 33% of respondents rated their confidence in their executives' abilities to protect their personal computers as a one or a two, while 20% rated their executives' ability to secure their email account similarly.

These attacks create very real problems for security teams as they spend a disproportionate amount of time and concern working to secure individuals' personal lives. Security teams have worked diligently and successfully to harden the security measures within their corporations. They have been so successful that cybercriminals have been forced to search for softer targets; thus choosing an attack surface outside the control and oversight of IT. Even so, the lengths that these teams go to to prevent cybercriminals from attacking the digital assets of executives outside the organization represents an undue burden with 35% of respondents rating the amount of time they spend on this particular issue as a nine or ten on a scale where ten represents highly time-consuming.

> Perhaps even more telling, 63% of respondents reported that they had lost sleep over concerns regarding protecting executives on their personal devices or accounts.

Many CISO's find themselves at an impasse as they try to find practical solutions that provide real security while still allowing 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, most respondents reported overwhelming difficulties with acquiring adequate access to assess possible vulnerabilities. When asked to rate the difficulty involved in areas such as gaining sufficient visibility into executives' personal devices to prevent cyberattacks, 41% of respondents rated the difficulty as a nine or ten on a scale where ten represented highly difficult. On that same scale, 41% of respondents rated the difficulty in getting sufficient visibility into home networks to prevent cyberattacks as a seven or an eight. With insufficient access, the complicated job of providing protection to an executive's personal digital life becomes even more difficult.

SURVEY EVIDENCE

THE FOLLOWING FINDINGS ARE EVIDENCE OF THE RISK TO EXECUTIVES' PHYSICAL SECURITY & DIGITAL ASSETS

Executives are experiencing multiple cyberattacks. According to the research, 42% of respondents say their executives and family members were attacked by cybercriminals and 25% of respondents say in the past two years executives experienced an average of seven or more than 10. In addition to doxxing and malware infections, other attacks include personal email attacks or compromises (42%) and online impersonation (34%).

Attacks against executives have the same serious consequences as a data breach. Cyberattacks against executives resulted in the theft of sensitive financial data (47% of respondents), loss of important business partners (45% of respondents) and theft of intellectual property/company information (36% of respondents). More than one-third of respondents (35% of respondents) say the consequence was improper access to the executive's home network, which is not secured or patched to the level an organization would require in its offices and facilities.

The finance and marketing departments are most likely to send sensitive data to executives' personal emails, according to 23% and 22% of respondents respectively. However, the executive suite (21% of respondents) and board members (19% of respondents) are also guilty of sending sensitive information to personal emails to one another.

Staff time and the steps taken to detect, identify and remediate the breach are the most costly following an incident. 39% of respondents say their organization measures the potential financial consequences from such an attack. 59% of these respondents say their organizations measure the cost of staff time involved in responding to the attack and 55% of respondents say they measure the cost to detect, identify and remediate the breach.

It's not if but when key executives will be targeted by organized criminals. 62% of respondents say attacks against digital assets are highly likely and 50% of respondents say future physical threats against executives is highly likely.

Criminals are sophisticated and stealthy when targeting executives and other high-profile individuals. Executives are most likely to unknowingly reuse a compromised password from their personal accounts inside their company (71% of respondents) and 67% say it is highly likely that an imposter would send a text message to another employee at their company. 51% of respondents say it is highly likely that an executive's significant other or child receives an unsolicited email and clicks on a link taking them to a third-party website.

Organizations are not determining the extent of the threat to executives' physical safety and security of personal digital devices. Only 41% of respondents say their organizations are assessing the physical risk to executives and their families and only 38% of respondents say organizations assess the risk to executives' digital assets.

39%

OF RESPONDENTS SAY THEIR ORGANIZATION MEASURES THE POTENTIAL FINANCIAL CONSEQUENCES FROM AN ATTACK

62%

OF RESPONDENTS SAY ATTACKS AGAINST DIGITAL ASSETS ARE HIGHLY LIKELY

51%

OF RESPONDENTS SAY IT IS HIGHLY LIKELY THAT AN EXECUTIVE'S SIGNIFICANT OTHER OR CHILD RECEIVES AN UNSOLICITED EMAIL

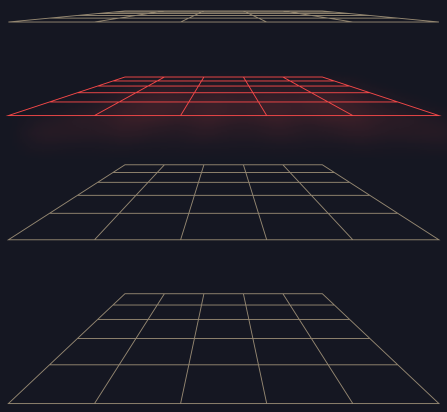
Executives are the weakest link in the ability to protect their lives and digital assets. Only 16% of respondents say their organizations are highly confident that a CEO or executives' personal email or social media accounts are protected with dual-factor authentication. The most confidence (48% of respondents) is that CEOs and other executives would know how to secure their personal email. 28% of respondents are highly confident that executives would know how to determine if an email is phishing and 26% of respondents say they are highly confident that executives would know how to set up their home network securely.

Only 32% of respondents say executives take some personal responsibility for the security of their digital assets and safety and only **38%** of respondents say executives understand the threat to their personal digital assets.

As executives switch to their home networks and personal devices, visibility critical to detecting attacks is diminished. According to the research the following areas lack visibility: personal devices (74% of respondents), executives' personal email accounts (66% of respondents), the executive's home network to prevent cyberattacks (64% of respondents), executives' privacy footprint (61% of respondents) and password hygiene (57% of respondents).

59%

OF RESPONDENTS SAY ENSURING EXECUTIVE PROTECTION IS MORE DIFFICULT DUE TO THE INCREASING ATTACK SURFACE



Executives working outside the office increase the attack surface significantly. 59% of respondents say ensuring executive protection is more difficult due to the increasing attack surface. However, only about half of respondents (53%) say attacks against the digital assets of executives outside the office domain is as much a priority as preventing such attacks when they are in the office. Only 50% of respondents say their organizations track potential attacks against executives, such as doxxing, phishing and malware attempts.

To reduce the risk, executives should be trained to secure their devices and physical safety. Almost all organizations are not doing the basics in enabling executives to protect themselves and their personal digital devices. Training executives to secure devices in and outside the workplace is only conducted by 37% and 36% of respondents, respectively. More organizations (53% of respondents) are providing self-defense training but only 42% of respondents say their organizations conduct tabletop exercises specific to the threats against executives.

Steps taken to protect executives' lives and digital devices are ineffective. According to 56% respondents, organizations are mainly focused on updating executives' personal devices. 52% of respondents say their organizations patch vulnerabilities and 51% of respondents say they use password managers. Only 45% of respondents say they are using dual factor authentication, 39% of respondents say they use botnet scanning and 36% of respondents say they analyze network connectivity on personal devices to detect malicious WiFi hotspots.

02.

WHAT IS DIGITAL EXECUTIVE PROTECTION?

Digital executive protection is a system for securing executives' and other high-access individuals' information and assets outside of their professional lives. Cybercriminals search for any weakness to exploit an organization's defenses, and the individuals that work for that organization become the path of least resistance – an easy stepping stone to the primary and lucrative final target.

Attackers find vulnerabilities in poorly secured home networks, frequently reused passwords for social media and personal email accounts, and attack inadequately defended personal devices. Effective digital executive protection minimizes these weaknesses without a disproportionate expenditure of time from IT security and with as little disruption as possible to the executives that it is meant to protect.

For digital executive protection to be truly effective, it is not enough to defend against any one list of possible attacks or malicious approaches. It must be holistic: addressing all of the possible factors and circumstances of a cyberattack and treat them as an interconnected whole.

03. EXECUTIVE SUMMARY

BY DR. CHRIS PIERSON

> Cyber attacks on the personal digital lives of executives are a growing threat, but most companies are unprepared to prevent them or to mitigate the potential damage to their organizations.

42% of companies have already experienced cybercriminal attacks on their executives or their executives' families which had serious negative consequences for the organization. 78% experienced theft of corporate intellectual property, research and development data, or business strategy information;

66% **experienced loss of customers or business partners**

27% **experienced theft of customer or employee data**

The results of this study confirm what the BlackCloak team has been seeing day in and day out and in our discussions with senior cybersecurity leaders - corporations are not well prepared to mitigate cyber threats against their executives in their private lives. With only 9% of cybersecurity professionals highly confident that their CEO or executives would know how to protect their personal computer from viruses, and only 22% when it comes to securing personal emails, it paints a picture in need of improvement.

BlackCloak has observed a wide range of cybercriminal threats which are actively targeting the personal digital lives of executives. These include email compromise, ransomware, malware infection, doxxing, extortion, online impersonation, swatting, and even attacks to move into the physical realm.

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 www.blackcloak.io, follow them on LinkedIn and Twitter.

04.

KEY FINDINGS

In this section, we present an analysis of the research. The complete audited findings are shown in the Appendix of this report. The report is organized according to the following topics.

- The risk is real: criminals are attacking the digital assets and lives of executives and their families
- It's not if but when key executives will be targeted by criminals and hackers
- The attack surface is expanding from the office to the home making it easier for the criminal to steal valuable data

The risk is real: criminals are attacking the digital assets and lives of executives and their families.

The two most common cyberattacks are doxxing (57% of respondents) and malware infections on personal or family devices (56% of respondents), as shown in Figure 2. According to the research, 42% of respondents say their executives and family members were attacked by cybercriminals and 25% of respondents say in the past two years executives experienced an average of seven or more than 10. In addition to doxxing and malware infections, other attacks include personal email attacks or compromises (42%) and online impersonation (34%).

FIGURE 2

What types of attacks did your executives experience?

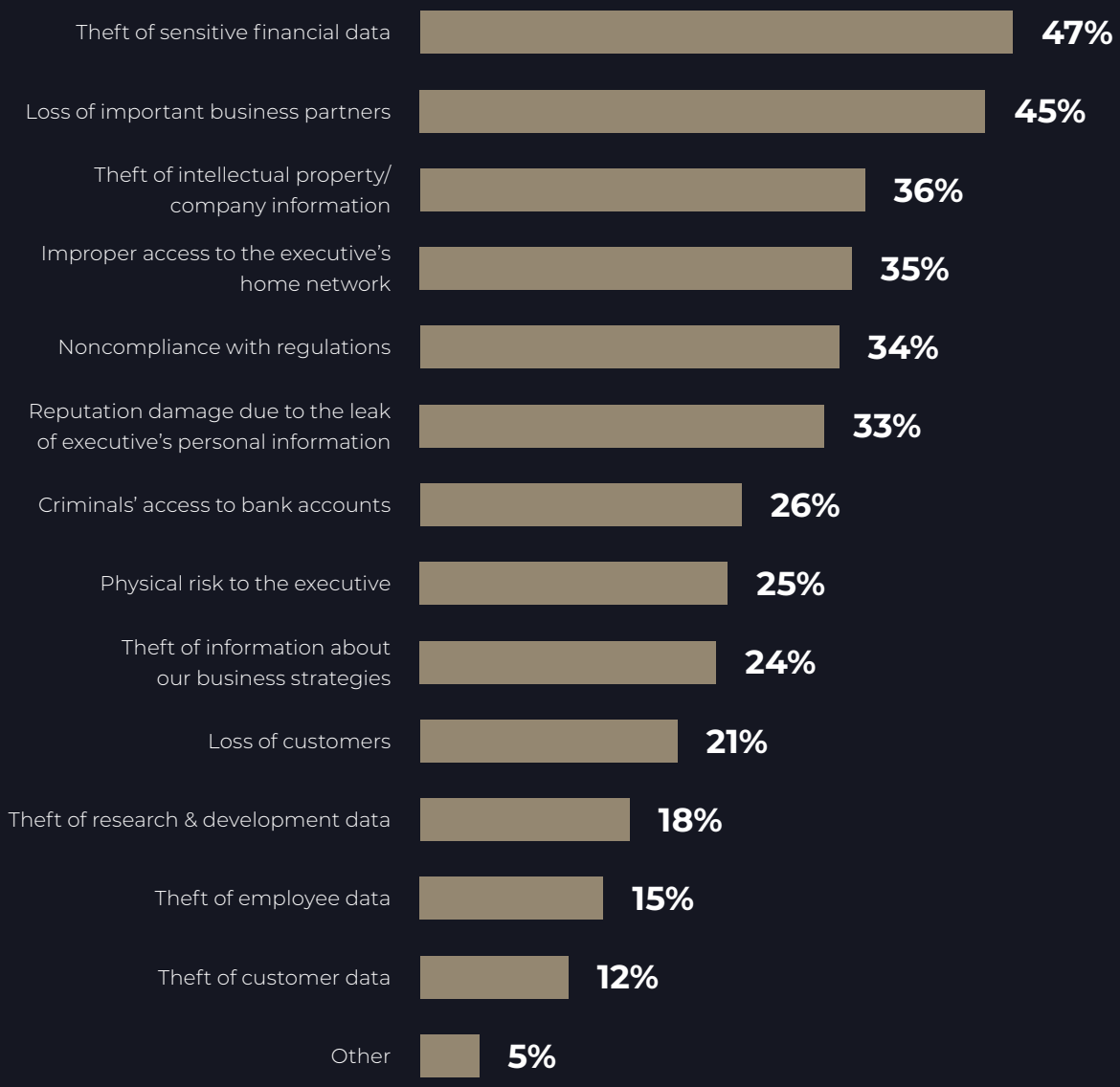
Three responses permitted

Attacks against executives have the same serious consequences as a data breach. As shown in Figure 3, the cyberattacks against executives resulted in the theft of sensitive financial data (47% of respondents), loss of important business partners (45% of respondents) and theft of intellectual property/company information (36% of respondents). More than one-third of respondents (35% of respondents) say the consequence was improper access to the executive's home network, which is not secured or patched to the level an organization would require in its offices and facilities.

FIGURE 3

What were the consequences of the attack?

More than one response permitted

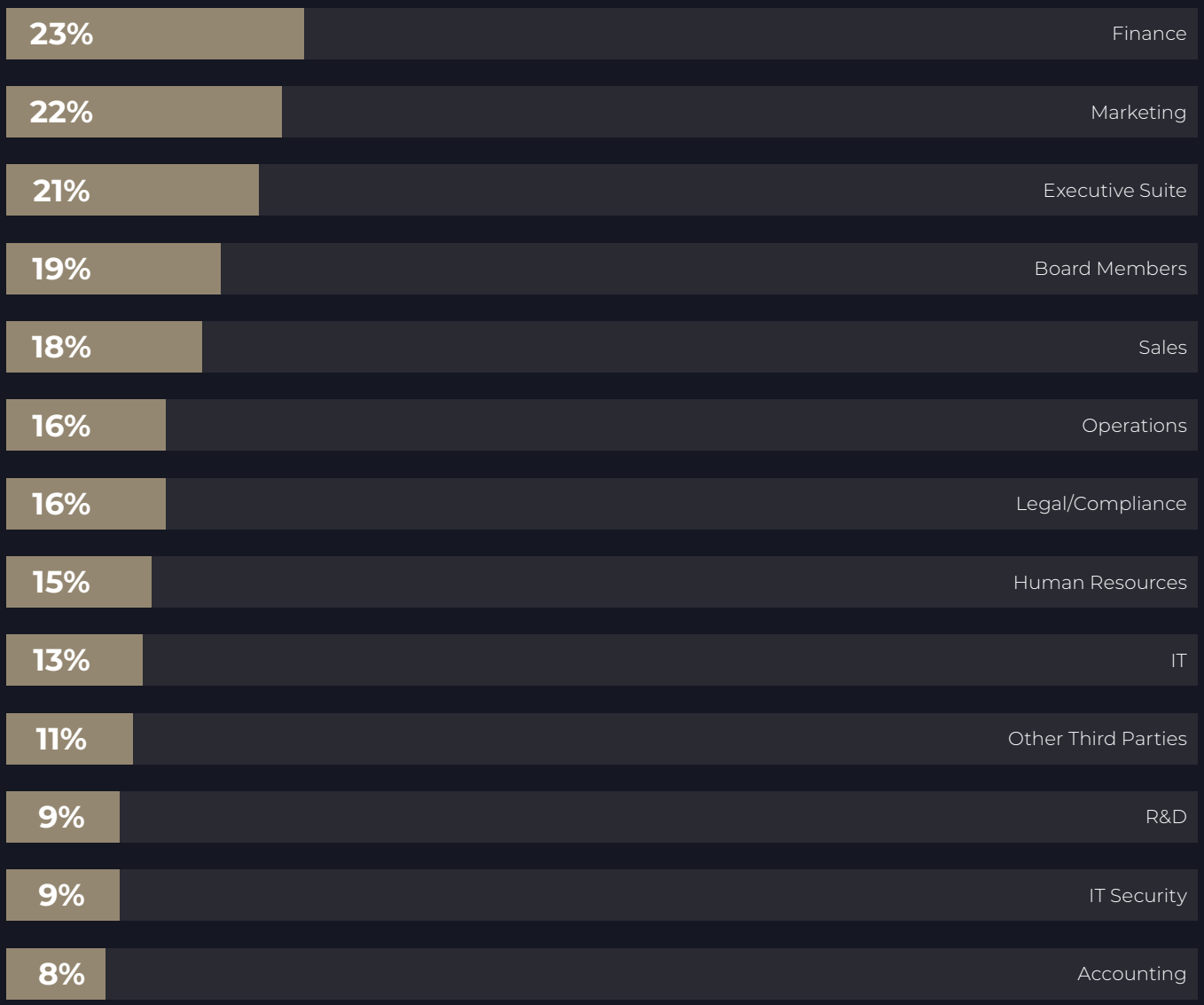


The finance and marketing departments are most likely to send sensitive data to executives' personal emails. Figure 4 presents a list of corporate functions and respondents' perceptions of whom would be sending sensitive data to executives' personal email. The finance function is most likely to send sensitive and confidential documents to executives' personal emails (23% of respondents) followed by marketing (22% of respondents). The executive suite (21% of respondents) and board members (19% of respondents) are also guilty of sending sensitive information to personal emails to one another.

FIGURE 4

The departments/functions most likely to send sensitive & confidential documents to executives' personal emails

Two responses permitted

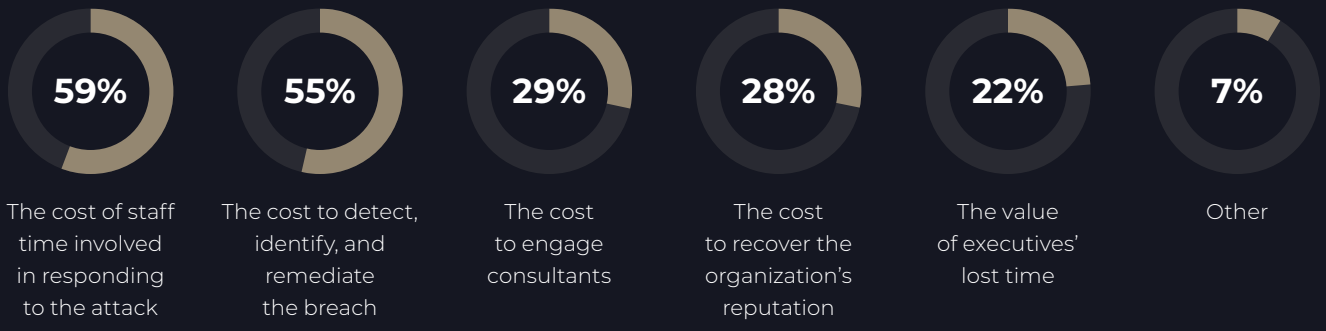


The highest costs when executives are attacked are related to the cost of staff time and the steps taken to detect, identify and remediate the breach. 39% of respondents say their organizations measure the potential financial consequences from such an attack. According to Figure 5, 59% of these respondents say their organizations measure the cost of staff time involved in responding to the attack and 55% of respondents say they measure the cost to detect, identify and remediate the breach.

FIGURE 5

What metrics do you use to determine the potential consequences of a cyberattack against your executives and their digital assets?

Two responses permitted

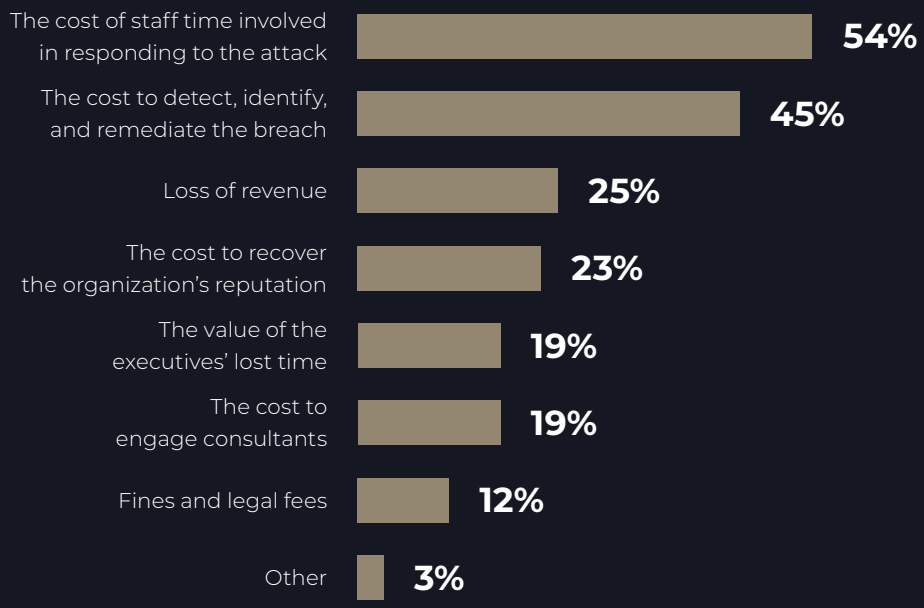


Organizations are using the same cost metrics to understand the potential financial consequences to organizations. As shown in Figure 6, 54% of respondents say the financial impact is measured by the cost of staff time involved in responding to the attack and 45% of respondents say it is the cost to detect, identify and remediate the breach.

FIGURE 6

What metrics do you use to measure the potential financial consequences of a cyber attack against business?

Two responses permitted



It's not if but when key executives will be targeted by organized criminals and hackers.

Attacks against executives' digital assets and physical threats are highly likely. Respondents were asked to rate the likelihood of cyberattacks on a scale from 1 = not likely to 10 = highly likely. Figure 7 presents the highly likely responses (7+ on the ten=point scale). As shown, 62% of respondents say attacks against digital assets are highly likely and 50% of respondents say future physical threats against executives is highly likely.

FIGURE 7

An attack against digital assets and physical threats is highly likely

On a scale from 1 = not likely to 10 = highly likely, 7+ responses presented

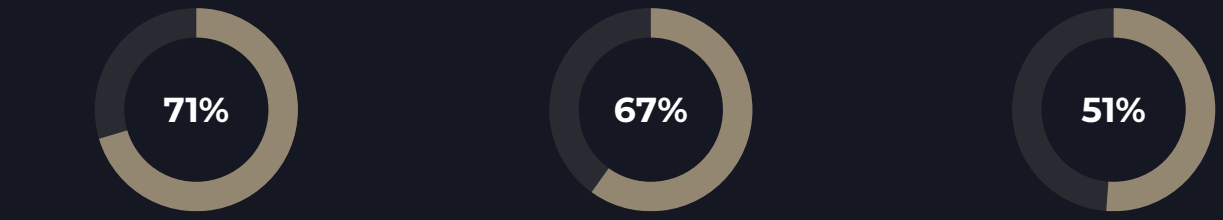
Criminals are sophisticated and stealthy when targeting executives and other high-profile individuals. Respondents were asked to rate the likelihood that executives would not be aware of how they are being targeted on a scale from 1 = not likely to 10 = highly likely.

According to Figure 8, which presents the highly likely responses, executives are most likely to unknowingly reuse a compromised password from their personal accounts inside their company (71% of respondents) and 67% say it is highly likely that an imposter would send a text message to another employee at their company. 51% of respondents say it is highly likely that an executive's significant other or child receives an unsolicited email and clicks on a link taking them to a third-party website.

FIGURE 8

How criminals are targeting executives

On a scale from 1 = not likely to 10 = highly likely, 7+ responses presented



Organizations are not determining the extent of the threat to executives' physical safety and security of personal digital devices. As shown In Figure 9, only 41% of respondents say their organizations are assessing the physical risk to executives and their families and only 38% of respondents say organizations assess the risk to executives' digital assets.

FIGURE 9

Does your organization assess physical and digital threats?

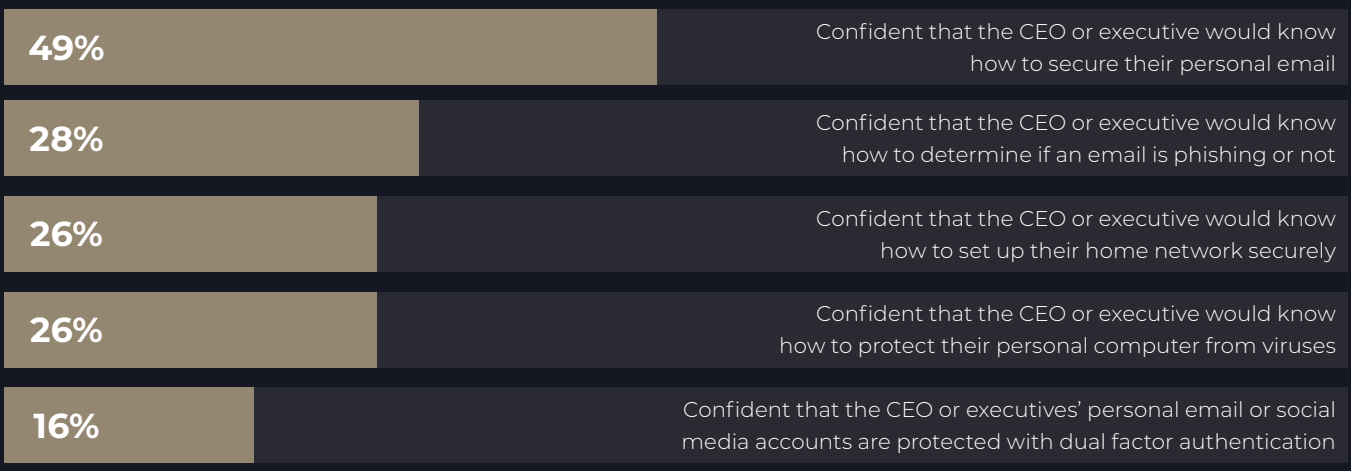
Executives need training to understand the seriousness of being targeted by cybercriminals. Respondents were asked to rate their organizations' confidence in executives' ability to reduce the threats against their digital assets on a scale from 1 = not confident to 10 = highly confident.

As shown in Figure 10, only 16% of respondents say their organizations are highly confident that CEO or executives' personal email or social media accounts are protected with dual factor authentication. The most confidence (49% of respondents) is that CEOs and other executives would know how to secure their personal email. 28% of respondents are highly confident that executives would know how to determine if an email is phishing and 26% of respondents say they are highly confident that executives would know how to set up their home network securely.

FIGURE 10

IT security teams lack confidence in the ability of executives to prevent attacks

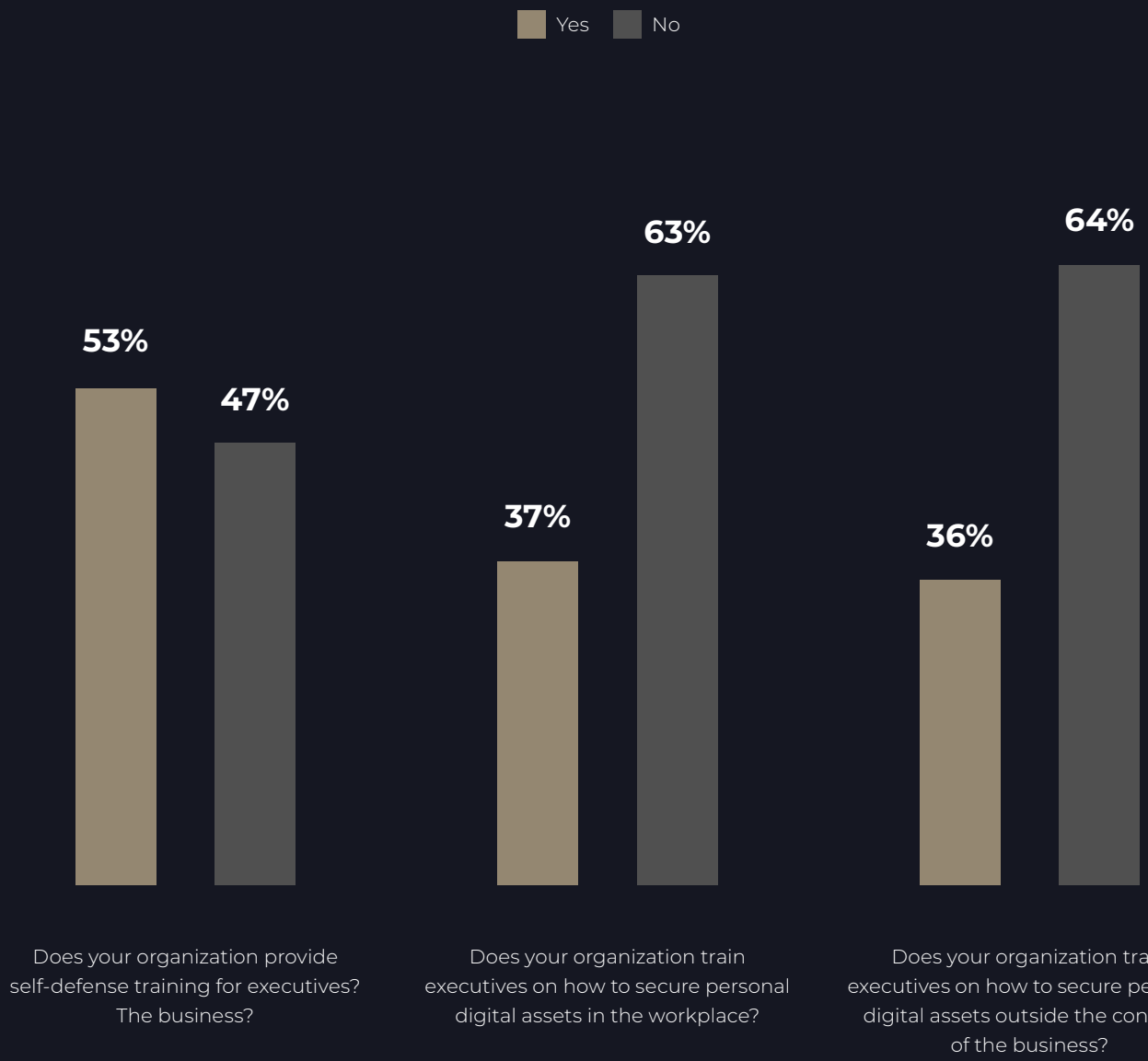
On a scale from 1 = not confident to 10 = highly confident, 7+ responses presented



Executives are the weakest link in preventing attacks against their digital assets. This can be remedied by training. As shown in Figure 11, almost all organizations are not doing the basics in enabling executives to protect themselves and their personal digital devices. Training executives to secure devices in and outside the workplace is only conducted by 37% and 36% of respondents, respectively. More organizations (53% of respondents) are providing self-defense training but only 42% of respondents say their organizations conduct tabletop exercises specific to the threats against executives.

FIGURE 11

Does your organization train executives to protect themselves and their digital assets?



According to Figure 12, only 32% of respondents say executives take some personal responsibility for the security of their digital assets and safety and only 38% of respondents understand the threat to their personal digital assets.

FIGURE 12

Executives underestimate the threat and the need to take personal responsibility for the protection of their digital assets

Strongly agree and Agree responses combined

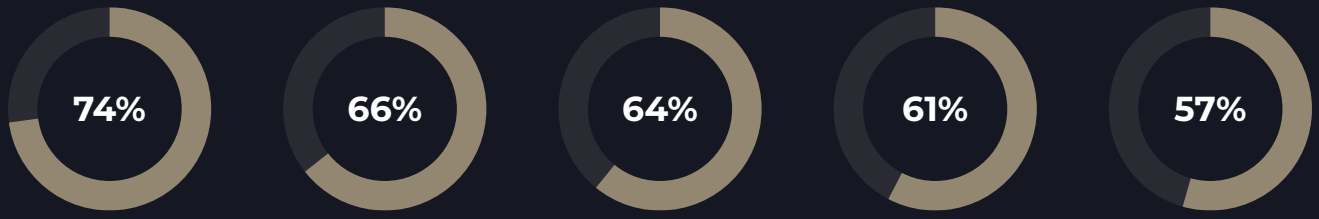
The attack surface is expanding from the office to the home making it easier for the criminal to steal valuable data.

As executives switch to their home networks and personal devices, visibility critical to detecting attacks is diminished. Respondents were asked to rate the difficulty in the ability to stop cyberattacks against executives on a scale of 1 = not difficult to 10 = highly difficult. Figure 13 presents the highly difficult responses. According to the research the following areas lack visibility: personal devices (74% of respondents), executives' personal email accounts (66% of respondents), the executive's home network to prevent cyberattacks (64% of respondents), executives' privacy footprint (61% of respondents) and password hygiene (57% of respondents).

FIGURE 13

The lack of visibility into devices puts organizations and executives at risk

On a scale from 1 = not difficult to 10 = highly difficult, 7+ responses presented



Difficulty having sufficient visibility into your executives' personal devices to prevent cyberattacks

Difficulty having sufficient visibility into your executives' personal email accounts to prevent cyberattacks

Difficulty having sufficient visibility into the executives' home network to prevent cyberattacks

Difficulty having sufficient visibility into your executives' privacy footprint to prevent cyberattacks or other nefarious activities

Difficulty having sufficient visibility into your executives' password hygiene to prevent cyberattacks

Executives working outside the office increase the attack surface significantly. According to Figure 14, 59% of respondents say ensuring executive protection is more difficult due to the increasing attack surface. However, only about half of respondents (53%) say attacks against the digital assets of executives outside the office domain is as much a priority as preventing such attacks when they are in the office. Only 50% of respondents say their organizations track potential attacks against executives, such as doxxing, phishing and malware attempts.

FIGURE 14

Perceptions about the threats

Strongly agree and Agree responses combined

59%

The attack surface of our organization increases significantly when an executive works remotely

53%

Preventing cyberattacks against the digital assets of executives outside the office domain is as much a priority as preventing such attacks when they are in the office

50%

Our organization tracks potential attacks against executives and their family members, such as doxxing, phishing and malware attempts

FIGURE 15

Who is most responsible for digital executive protection

Only one choice permitted

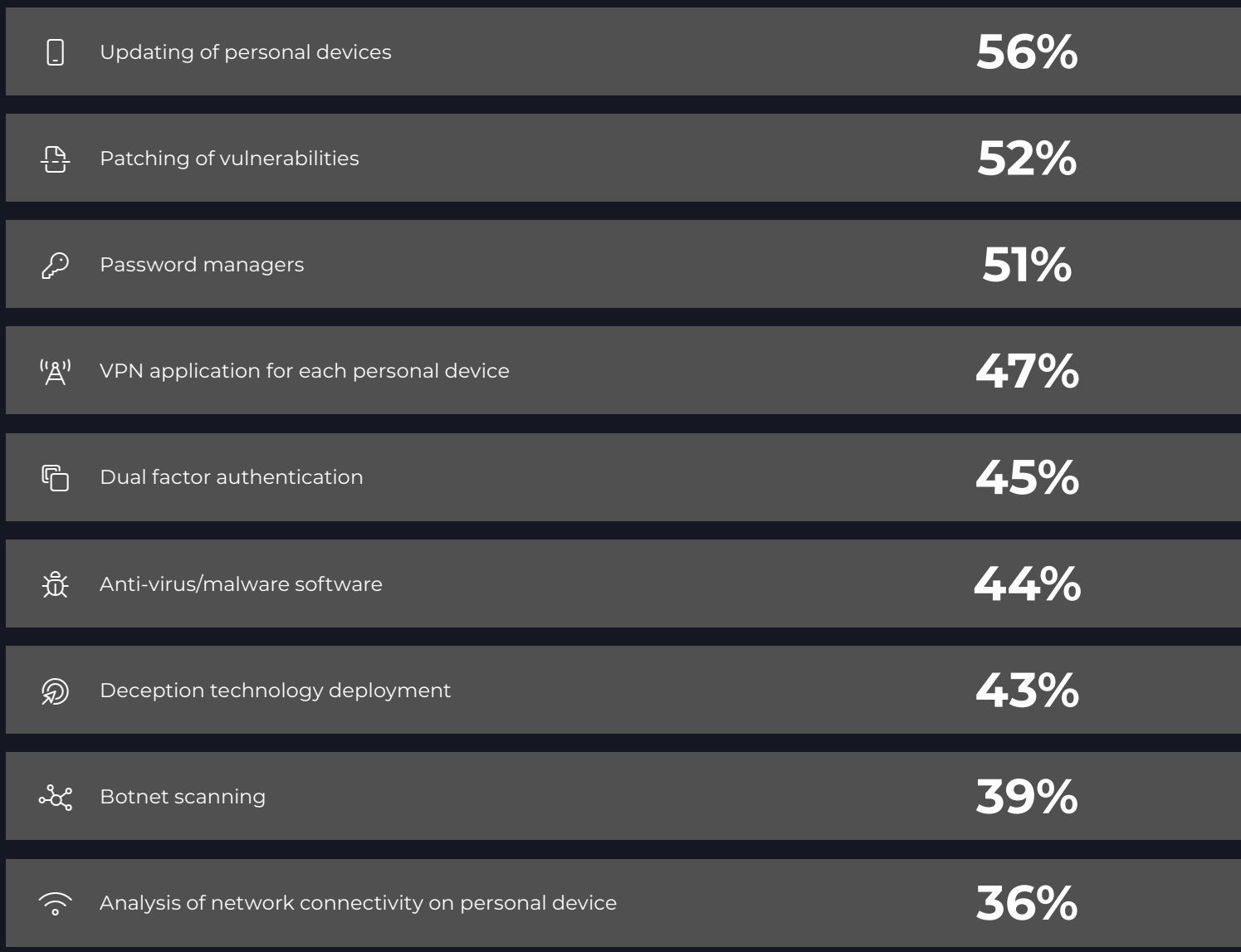
IT and IT security are most responsible for digital executive protection. However, as shown in Figure 15, 15% of respondents say no one is most responsible.

Steps taken to protect executives' lives and digital devices are ineffective. Updating personal devices is the number one step taken to secure personal home networks and devices. Figure 16 presents a list of steps taken to protect executives' digital assets. According to 56% respondents, organizations are mainly focused on updating executives' personal devices. 52% of respondents say their organizations patch vulnerabilities and 51% of respondents say they use password managers. Only 45% of respondents say they are using dual factor authentication, 39% of respondents say they use botnet scanning and 36% of respondents say they analyze network connectivity on personal devices to detect malicious WiFi hotspots.

FIGURE 16

Steps taken to secure personal home networks and devices

More than one response permitted



05.

DIGITAL EXECUTIVE PROTECTION FROM BLACKCLOAK

Digital executive protection from BlackCloak is a powerful, holistic approach to securing the private digital lives and assets of C-Suite executives and other high profile individuals such as board members, senior and executive leadership teams and other key personnel and their families from threats such as cyberattack, impersonation, harassment, and identity theft.

BlackCloak's award-winning Concierge Cybersecurity & Privacy™ Platform combines sleek mobile and desktop applications with white glove concierge service. This unique approach allows executives and their families to maintain privacy and peace of mind, while benefiting from the same level of protection that they would experience inside the traditional perimeter of an organization's network. The end goal is to provide users with secure, seamless protection that allows for the frictionless transition between private and professional digital lives.

WHY DO YOU NEED DIGITAL EXECUTIVE PROTECTION FROM BLACKCLOAK?

IT security professionals know that the vast majority of all data breaches begin with the human element and that executives are more likely to be the targets of these attacks. CISOs and their security teams have worked tirelessly to prevent cybercriminals from leveraging these attack vectors within the walls of their corporations. As a result, bad actors looking to penetrate organizations have shifted their focus to softer targets–digital private lives – because it's easier to gain access through weak home networks, where family members more frequently use weak passwords.

The consequences for improperly securing the digital devices and assets of employees can easily be recognized in such high-profile incidents as the 2022 data breaches at Twilio and Uber. Cybercriminals were able to gain access to sensitive company information at Twilio through a sophisticated social engineering approach that involved phishing texts designed to bypass the two-factor authentication (2FA) they used to protect their system. Similarly, bad actors were able to breach Uber's systems with a social engineering text attack in 2022.

However, it is not enough to defend against social engineering attacks — two months ago, criminals were able to enter Lastpass's secure servers by remotely accessing an engineer's home computer through exploiting a weakness in a third-party software package.

Cybercriminals are actively working to find weaknesses and exploit the personal digital lives of executives and other high-access individuals because they represent the softest points of entry into organizations, making it more important than ever for IT security to find practical solutions to protecting their organizations and their executives' personal digital well-being. BlackCloak has created a service that provides the solution. Its award-winning Concierge Cybersecurity & Privacy™ Platform allows IT departments to return their focus on protecting the work that takes place within the organization's extended network, while allowing executives to work securely and seamlessly from anywhere.

06.

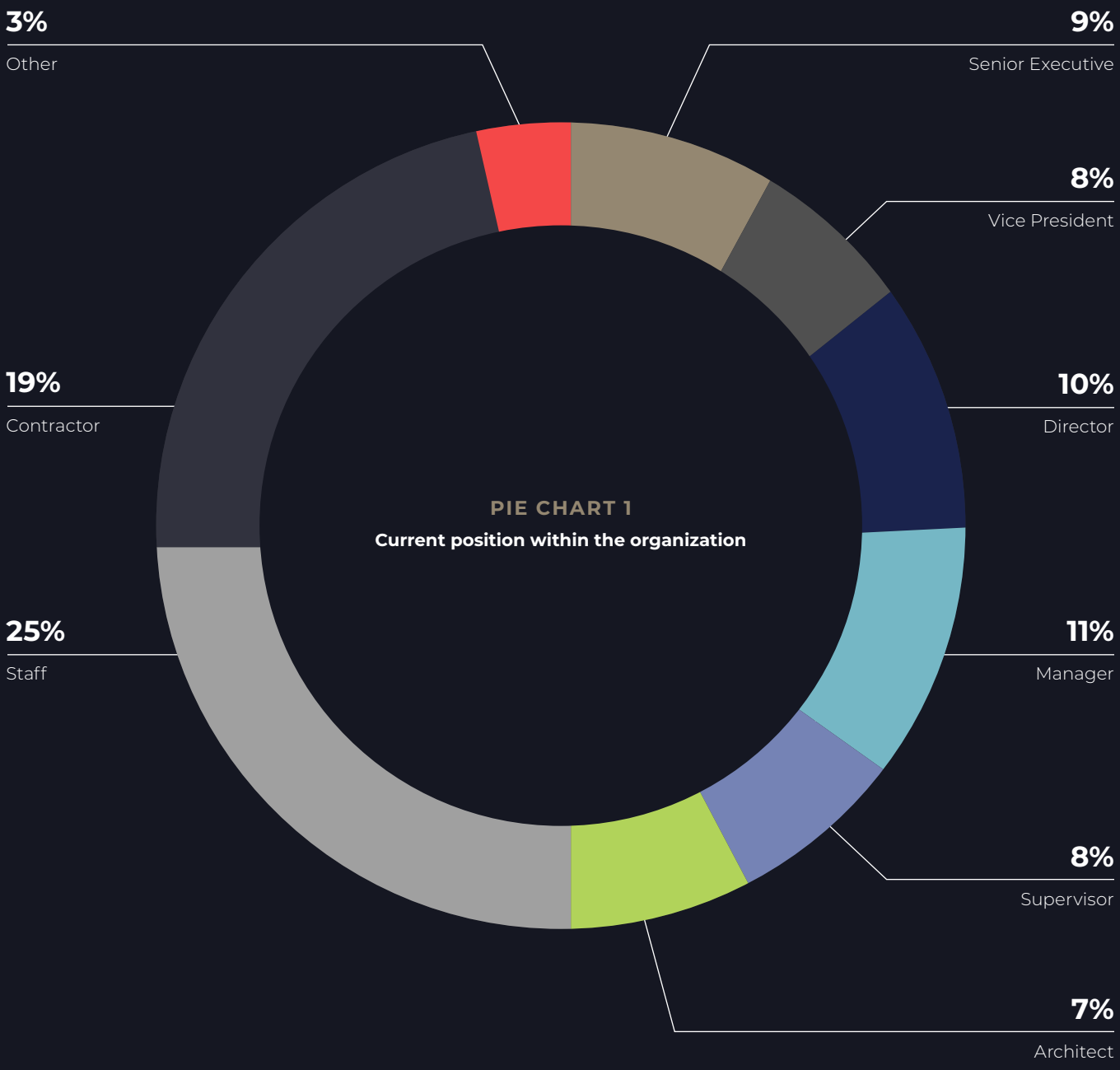
METHODOLOGY

A sampling frame of 16,400 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 605 total returns. Screening and reliability checks required the removal of 52 surveys. Our final sample consisted of 553 surveys or a 3.4% response.

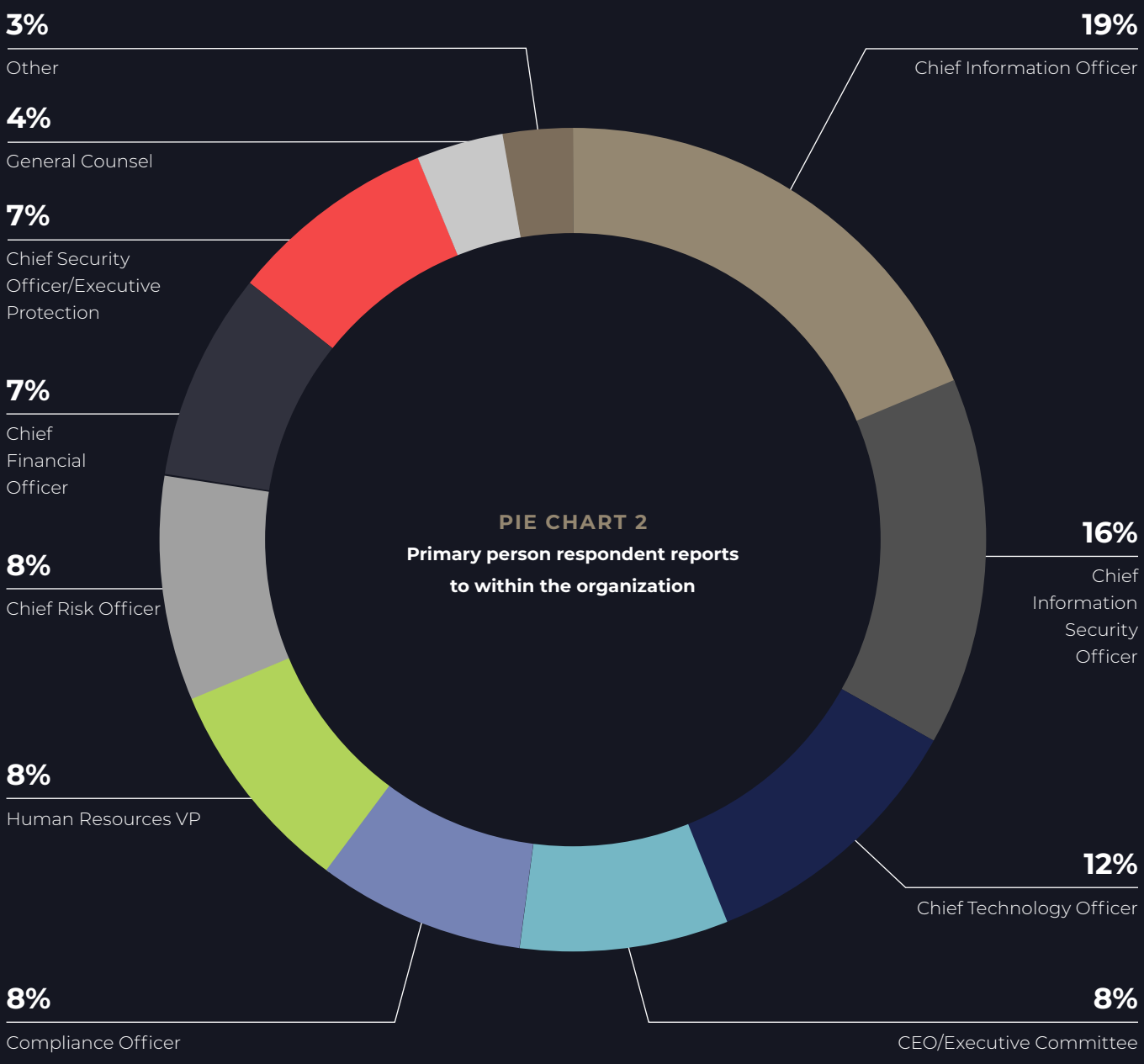
TABLE 1

SAMPLE RESPONSE	FREQ	PCT%
Sampling frame	16,400	100.0%
Total returns	605	3.7%
Rejected or screened surveys	52	0.3%
Final sample	553	3.4%

Pie Chart 1 reports the respondent's organizational level within participating organizations. By design, almost half (46%) of respondents are at or above the supervisory levels. The largest category at 25% of respondents is classified as staff.



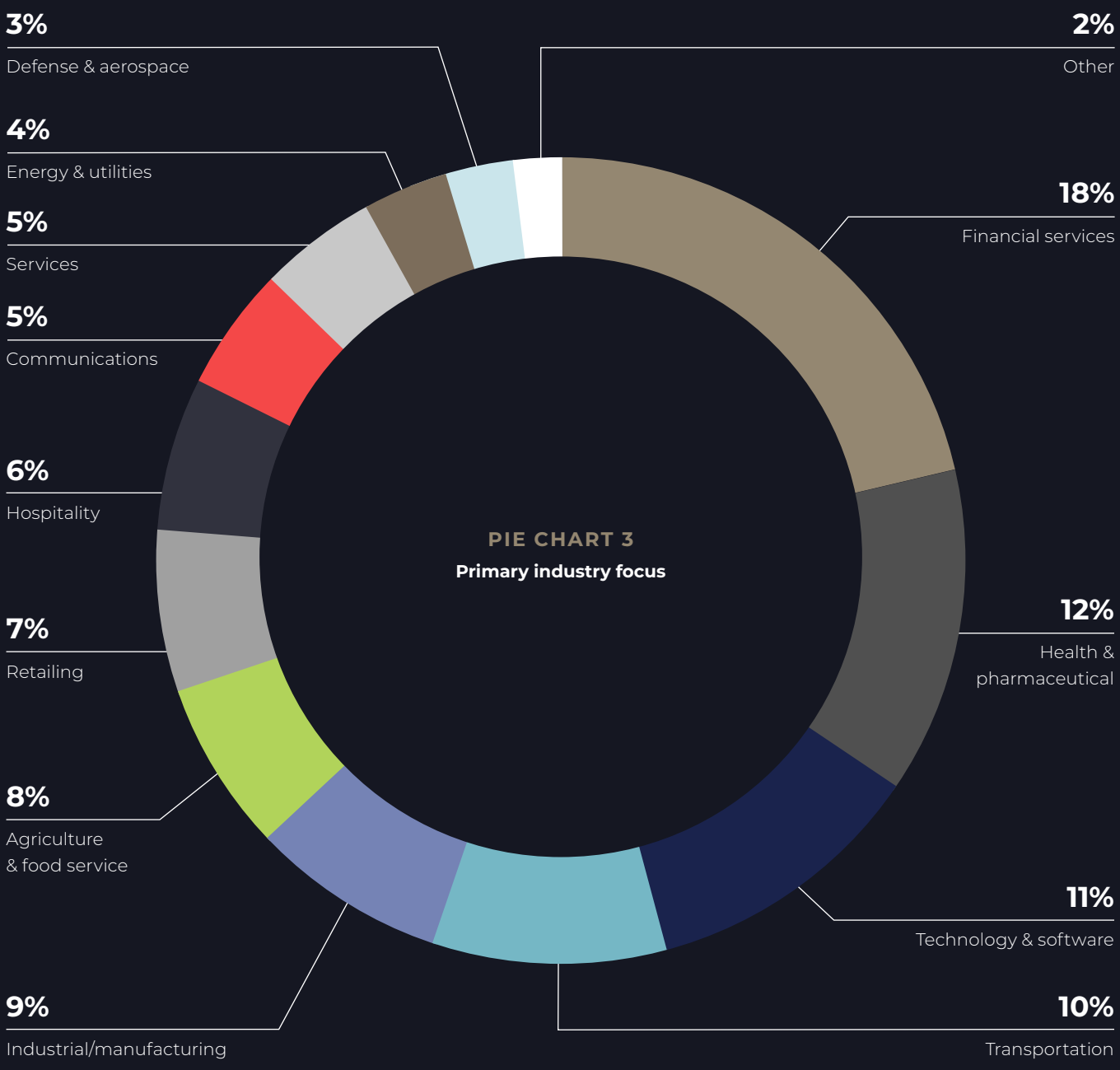
Pie Chart 2 reports the primary person the respondent reports to within the organization. 19% of respondents report to the chief information officer, 16% of respondents report to the chief information security officer, 12% report to the chief technology officer, 8% of respondents report to the CEO/executive committee, 8% of respondents report to the compliance officer, and 8% of respondents report to the human resources VP as shown in Pie Chart 2.



PIE CHART 2

Primary person respondent reports to within the organization

Pie Chart 3 reports the industry focus of respondents' organizations. This chart identifies financial services (18%) as the largest industry focus, which includes banking, investment management, insurance, brokerage, payments and credit cards. This is followed by healthcare and pharmaceuticals (12% of respondents), technology and software (11% of respondents), transportation (10% of respondents), and industrial manufacturing (9% of respondents).



PIE CHART 3

Primary industry focus

As shown in Pie Chart 4, 37% of respondents are from organizations with a global headcount between 25,000 and 75,000 employees, 31% of respondents are from organizations with a global headcount between 1,000 and 25,000 and 32% of respondents are from organizations with a global headcount between 1,000 and 5,000 employees.

PIE CHART 4

Global full-time headcount

07.

CAVEATS TO THIS 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 RESULTS

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.

Ponemon INSTITUTE

For more information about this study, please contact Ponemon Institute by sending an email to research@ponemon.org or call at 1.800.887.3118.

PONEMON INSTITUTE

ADVANCING RESPONSIBLE INFORMATION MANAGEMENT

Ponemon Institute is dedicated to independent research and education that advances responsible information and privacy management practices within business and government. Our mission is to conduct high-quality, empirical studies on critical issues affecting the management and security of sensitive information about people and organizations.

We uphold strict data confidentiality, privacy and ethical research standards. We do not collect any personally identifiable information from individuals (or company identifiable information in our business research). Furthermore, we have strict quality standards to ensure that subjects are not asked extraneous, irrelevant or improper questions.