Deepfake Deception:

How AI Harms the Fortunes and Reputations of Executives and Corporations

Ponemon Institute© Research Report

Deepfake Deception: How AI Harms the Fortunes and Reputations of Executives and Corporations

April 2025

Part 1. Introduction

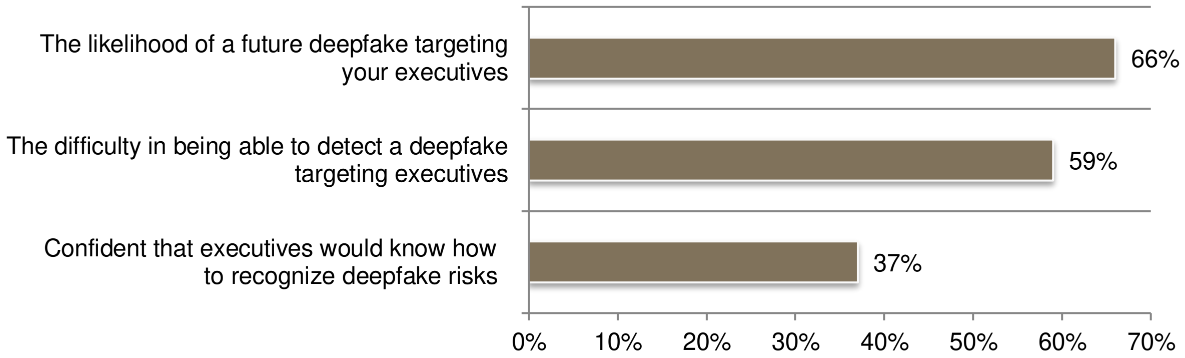
The fortunes and reputations of executives and corporations are at great risk because of the ability of cybercriminals to target vulnerable executives with artificial images or videos for the purposes of extortion and physical harm. As more evidence of the reality and likelihood of deepfake attacks emerges, awareness of the need to take action to prevent these threats is growing. More than half of the IT and IT security practitioners (54 percent) surveyed in this research say deepfake is one of the most worrying uses of artificial intelligence (AI).

The purpose of the research is to learn important information about how organizations view the deepfake risk against board members and executives and how these attacks can be prevented. According to the research, executives were targeted by a fake image or video an average of three times. Another serious threat covered in this research for the second year is the risks to executives' digital assets and their personal safety. In this year's study, attacks by cybercriminals against executives and their families increased from 42 percent to 51 percent of organizations represented in the research.

If and when your executives and board members are the target of a deepfake attack, it is likely they will not even know it. Respondents were asked to rate the likelihood of a deepfake attack, the difficulty in detecting it and the confidence in the executives' ability to know that they are being targeted on a scale from 1 = not likely, not difficult and not confident to 10 = highly likely, highly difficult and highly confident (7+ responses presented). As shown in Figure 1, an attack is highly likely (66 percent), it is very difficult to detect (59 percent) and there is no confidence that executives would recognize an attack (37 percent).

Figure 1. The deepfake threat is real and dangerous

On a scale from 1 = not likely/difficult/confident to 10 = highly likely/difficult/confident 7+ responses presented



The following findings illustrate the severity of deepfake and digital asset attacks:

- **Is the person calling your company's CEO a trusted colleague or a criminal?** Forty-two percent of respondents say their organizations' executives and board members have been targeted an average of three times by a fake image. Or worse, 18 percent are unsure if such an attack occurred. Of those targeted, 28 percent of respondents say it was by impersonating a trusted entity such as a colleague, executive, family member or known organization. Twenty-one percent of respondents say executives and board members received urgent messages such as the requirement of immediate payment or information about a security breach detected.

- **It is difficult to detect imposters seeking to do harm.** Executives must understand that a zero-trust mindset is essential to not becoming a deepfake victim because 56 percent of respondents say It is essential to distinguish between what is authentic and what is fake in messages. For example, imposter accounts are social media profiles engineered for malicious activities, such as a deepfake attacks. The two types of deepfakes of greatest concern are social imposters (53 percent of respondents) and financial fraudsters (37 percent of respondents).

- **Executives need training and a dedicated team to respond to deepfake attacks**. Despite the threat from deepfake cybercriminals, 50 percent of respondents say their organizations do not plan to train executives on how to recognize an attack. Only 11 percent of respondents currently train executives to recognize a deepfake and only 14 percent have an incident response plan with a dedicated team when a deepfake occurs.

- **Threatening activities may go undetected because of a lack of visibility into erroneous activities.** Only 34 percent of respondents say their organizations have high visibility into the erroneous activity happening within their organization to prevent deepfake threats. Fifty-two percent of respondents say it is highly likely that their organization will evaluate technologies that can reduce the risks from deepfakes targeting executives. Fifty-three percent of respondents say technologies that enable executives to verify the identity and authentication of messages they receive are highly important.

- **The financial consequences of deepfake attacks are not often measured and therefore not known.** Only 36 percent of respondents say their organizations measure how much a deepfake attack can cost. If they do, the top two metrics used are the cost to detect, identify and remediate the breach and the cost of staff time to respond to the attack**.**

- **Organizations are in the dark about the severity of the financial consequences from a cyberattack involving digital assets.** Forty-three percent of respondents measure the potential consequences of a cyberattack against their executives and in 2023 only 39 percent of respondents said they had metrics in place. Forty percent of respondents say their organization measure the financial consequences against the business due to a cyberattack against the personal lives of executives and digital assets, a slight decrease from 2023.

- **Metrics used to determine the financial consequences of a digital cyberattack against executives remain the same since 2023.** The top two metrics for cyberattacks against executives are the cost of staff time (62 percent of respondents) and the cost to detect, identify and remediate the breach (51 percent of respondents).

- **Despite the vulnerability of executives' digital assets, most training occurs following an attack.** Most training is done after the damage is done, according to 38 percent of respondents in 2023 and 2024.

- **Attacks on executives and family members have increased.** Organizations need to assess the physical and digital asset risks to executives and their families. In 2023, 42 percent of respondents said there were attacks against executives and family members. This increased to 51 percent in 2025.

- **Online impersonations increased significantly since 2023.** The most prevalent attacks continue to be malware on personal or family devices (58 percent of respondents in 2024 and 56 percent of respondents in 2023), exposure of home address, personal cell and personal email (50 percent of respondents down from 57 percent of respondents in 2023). However, online impersonations increased significantly from 34 percent of respondents in 2023 to 41 percent of respondents in 2024.

- While still a low number, more organizations are increasing budgets and other resources because of the need to protect executives and their digital assets. Since 2023 48 percent of respondents say their organizations incorporate the risk of cyberthreats against executives in their personal lives, especially high-profile individuals in their cyber, IT and physical security strategies and budget, an increase from 42 percent of respondents. More organizations have a team dedicated to preventing and/or responding to cyber or privacy attacks against executives and their families, an increase from 38 percent to 44 percent of respondents.

- **More cybercriminals are targeting IP and executive's home network.** Organizations should be concerned that their company information, including IP and executives' home networks, have become more vulnerable since 2023. The theft of intellectual property and improper access to the executive's home network have increased from 36 percent of respondents to 45 percent of respondents and 35 percent of respondents to 41 percent of respondents, respectively. Significant consequences were the theft of financial data (48 percent of respondents) and loss of important business partners (40 percent of respondents).

- **The likelihood of physical attacks and attacks against executives' digital assets has not decreased in the past year.** Sixty-two percent of respondents in 2023 and 2024 say it is highly likely a cybersecurity attack will be made against executives' digital assets and 50 percent in both years say there will be a physical threat against executives. As discussed previously, organizations are slow to train executives on how to avoid a successful attack against their digital assets. Sixty-eight percent of respondents say it is highly likely that an executive would unknowingly reuse a compromised password from their personal accounts inside the company and 52 percent of respondents say an executive's significant other or child would click on an unsolicited email that takes them to a third-party website.

- **More organizations are providing self-defense training.** Self-defense training has increased since 2023 from 53 percent of respondents to 63 percent of respondents in 2025. Slightly more organizations are assessing the physical risk to executives and their families from 41 percent to 46 percent of respondents. Forty-one percent assess the risk to executives' digital assets when working at home.

- **Why is it difficult to protect executives' digital assets?** The top two challenges are due to remote working and not making protection of digital assets a priority when executives work outside the office, 53 percent and 51 percent of respondents, respectively. As a consequence of not training executives to protect their digital assets, only 38 percent of respondents say their executives and families understand the threat to their personal digital assets and only 32 percent of executives take personal responsibility for the security and safety of their digital assets.

- **Confidence in CEOs' and executives' ability to do the right thing to stop cyberattacks continues to be low.** While there is an increase in confidence in the CEO or executive knowing how to protect their personal computer from viruses (32 percent of respondents, an increase from 26 percent of respondents in 2023), it is still too low. Also, there is a significant decrease in executives knowing how to determine if an email is phishing (23 percent of respondents from 28 percent in 2023). Organizations lack confidence in their executives knowing how to set up their home network security (25 percent of respondents percent of respondents and 26 percent of respondents in 2023) and knowing if their email or social media accounts are protected with dual factor authentication (20 percent of respondents and 16 percent of respondents in 2023).

- **Difficulty in stopping cyberattacks against executives and their digital assets remains high.** It continues to be highly difficult to have sufficient visibility into executives' home networks cyberattacks (63 percent of respondents), to have sufficient visibility into executives' personal devices (66 percent of respondents), sufficient visibility into executives' personal email accounts (67 percent of respondents), sufficient visibility into executives' password hygiene (60 percent of respondents) and sufficient visibility into executives' privacy footprint (65 percent of respondents).

Part 2. Key findings

Ponemon Institute surveyed 586 IT and IT US security practitioners who are knowledgeable about deepfake risks, their organizations' efforts to prevent these attacks and technologies that can be used to reduce the threat. The complete research findings are presented in the Appendix. In the first part of this report, we analyze organizations' ability to address the deepfake risk. The second part is a follow up to the study conducted in 2023 on cybersecurity threats against executives and their digital assets and presents the trends in organizations' approach to digital executive protection. The report is organized according to the following topics.

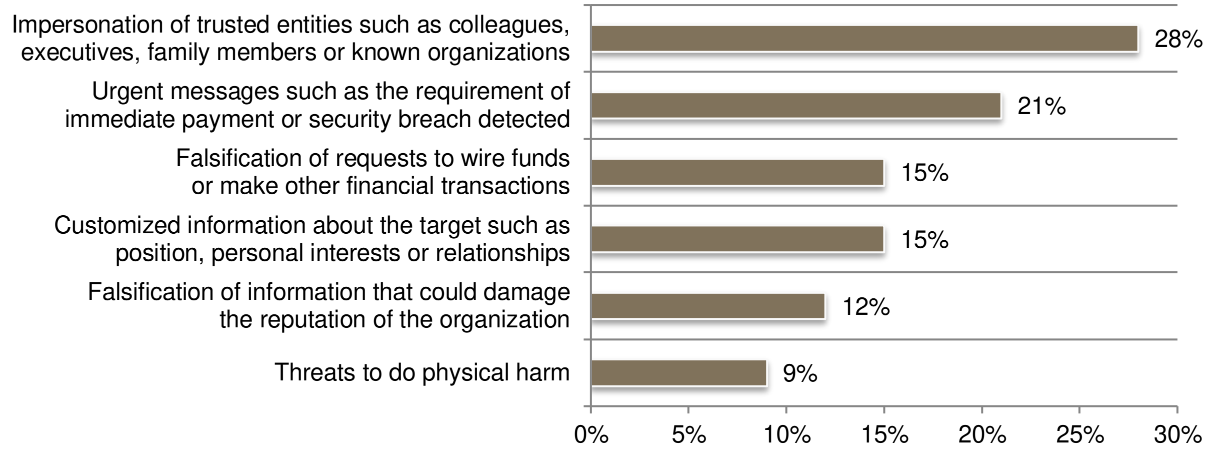
- Deepfakes risks are targeting vulnerable board members and executives.
- The serious consequences from deepfakes and cybersecurity threats.
- Since 2023, cyberattacks against executives continue to be highly likely, but are organizations better able to respond?

Deepfake risks are targeting vulnerable board members and executives.

How it works. A deepfake is an artificial image or video (a series of images) generated by a special kind of machine learning 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.

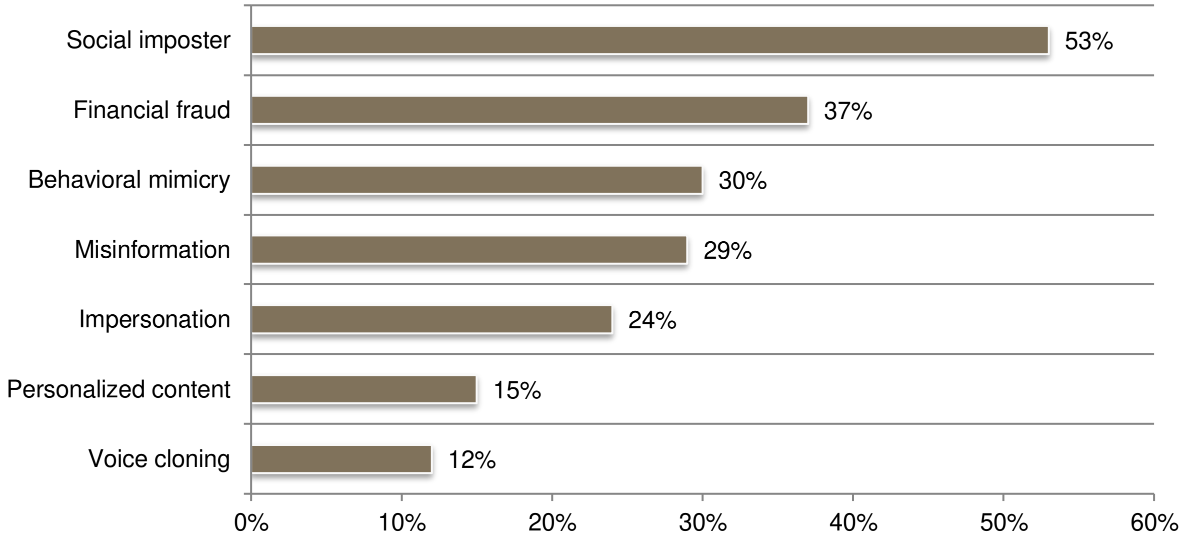
Is the person calling your company's CEO a trusted colleague or a criminal? Sixty percent of respondents say their organizations' executives and board members have been targeted an average of three times by a fake image (42 percent) or worse they are unsure if such an attack occurred (18 percent). As shown in Figure 2, of those targeted, 28 percent of respondents say it was by impersonating a trusted entity such as a colleague, executive, family member or known organization. Twenty-one percent of respondents say executives and board members received urgent messages such as the requirement of immediate payment or information about a security breach detected.

Figure 2. How did the deepfake target the executive?
One choice permitted



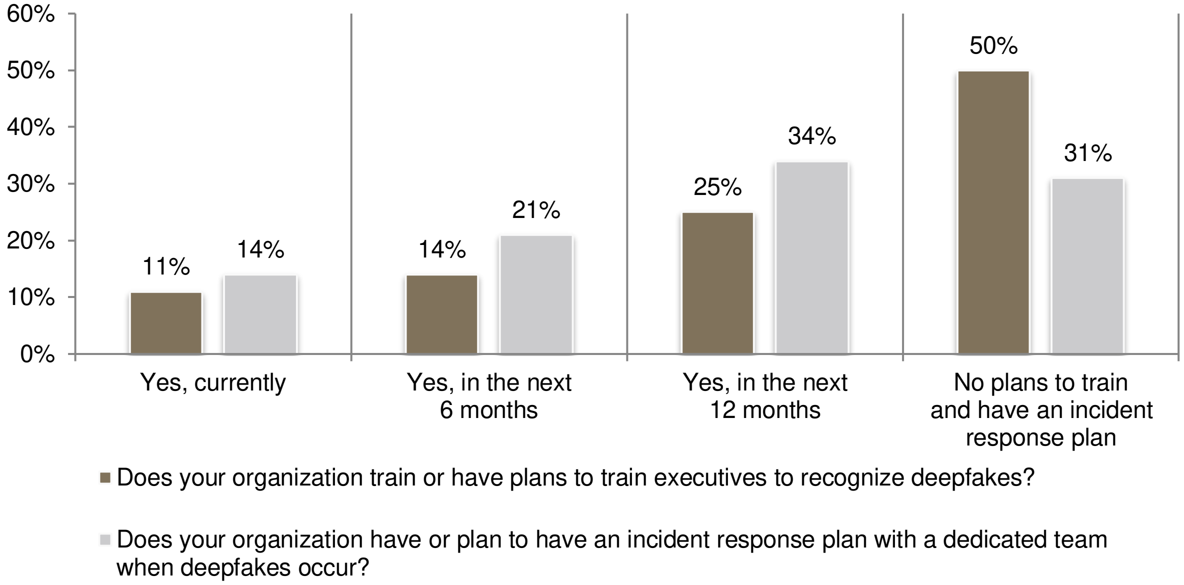
It is difficult to detect imposters seeking to do harm. Executives must understand that a zero-trust mindset is essential to not becoming a deepfake victim. Fifty-six percent of respondents say It is essential to distinguish between what is authentic and what is fake in messages. For example, imposter accounts are social media profiles engineered for malicious activities, such as a deepfake attacks. As shown in Figure 3, the two types of deepfakes of greatest concern are social imposters (53 percent of respondents) and financial fraudsters (37 percent of respondents).

Figure 3. What types of deepfake risks is your organization most concerned about?
Two responses permitted



According to Figure 4, despite the threat from deepfake cybercriminals, 50 percent of respondents say their organizations do not plan to train executives on how to recognize an attack. Only 11 percent of respondents currently train executives to recognize a deepfake and only 14 percent have an incident response plan with a dedicated team when a deepfake occurs.

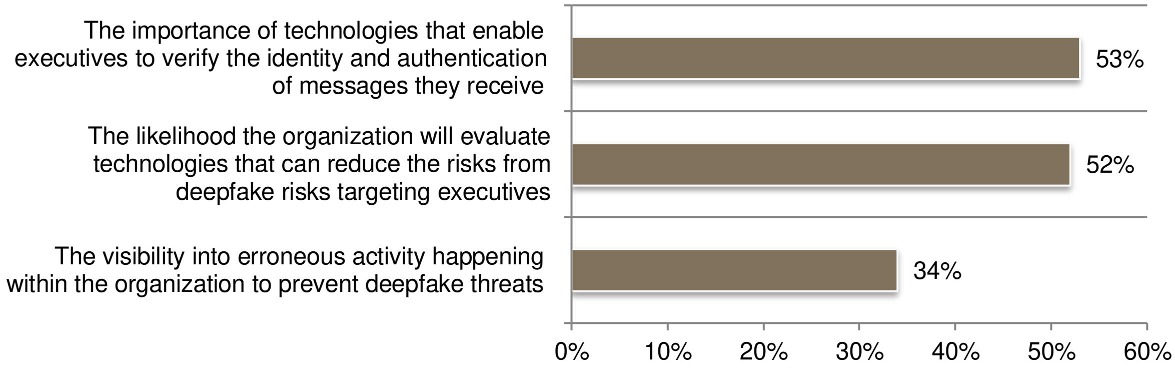
Figure 4. Are executives trained to recognize a deepfake attack and is there a dedicated team to respond to these attacks



Threatening activities may go undetected because of a lack of visibility into erroneous activities. Respondents were asked to rate the **importance** of technologies that enable verification, the authentication of messages, the **likelihood** of evaluating technologies to reduce the risk and the **visibility** into erroneous activity on a scale of 1 = not important/not likely, no visibility to 10 = highly likely/ highly important/high visibility. The 7+ responses are shown in Figure 5.

Only 34 percent of respondents say their organizations have high visibility into the erroneous activity happening within their organization to prevent deepfake threats. Fifty-two percent of respondents say it is highly likely that their organization will evaluate technologies that can reduce the risks from deepfakes targeting executives. Fifty-three percent of respondents say technologies that enable executives to verify the identity and authentication of messages they receive are highly important.

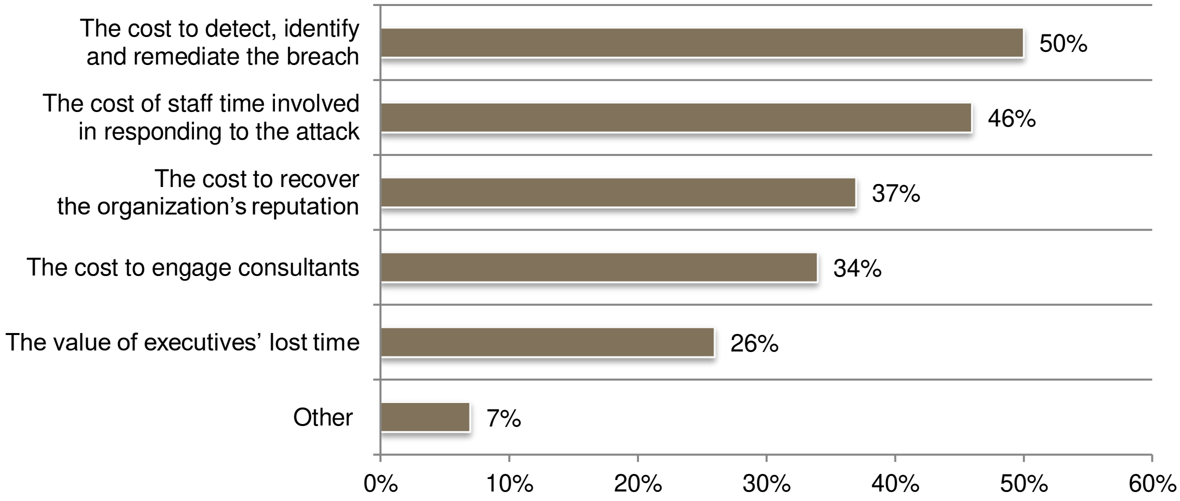
Figure 5. The importance of technologies to reduce deepfake risks
On a scale from 1 = not important/ likely/visible to 10 = highly important/ likely/visible
7+ responses shown



The serious consequences from deepfakes and cybersecurity threats

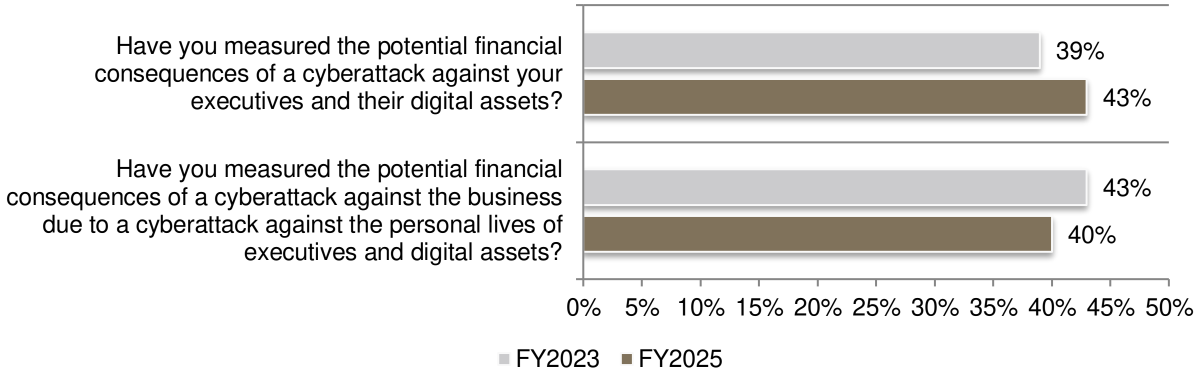
The financial consequences of deepfake attacks are not often measured and therefore not known. Only 36 percent of respondents say their organizations measure how much a deepfake attack can cost. If they do, the metrics used are shown in Figure 6. The top two are the cost to detect, identify and remediate the breach (50 percent of respondents) and the cost of staff time to respond to the attack (46 percent of respondents)**.**

Figure 6. How does your organization measure the potential financial consequences of a deepfake attack?
Two choices permitted.



Organizations are in the dark about the severity of the financial consequences from a cyberattack involving digital assets. As shown in Figure 7, 43 percent of respondents measure the potential consequences of a cyberattack against their executives and in 2023 only 39 percent of respondents said they had metrics in place. Forty percent of respondents say their organization measures the financial consequences against the business due to a cyberattack against the personal lives of executives and digital assets, a slight decrease from 2023.

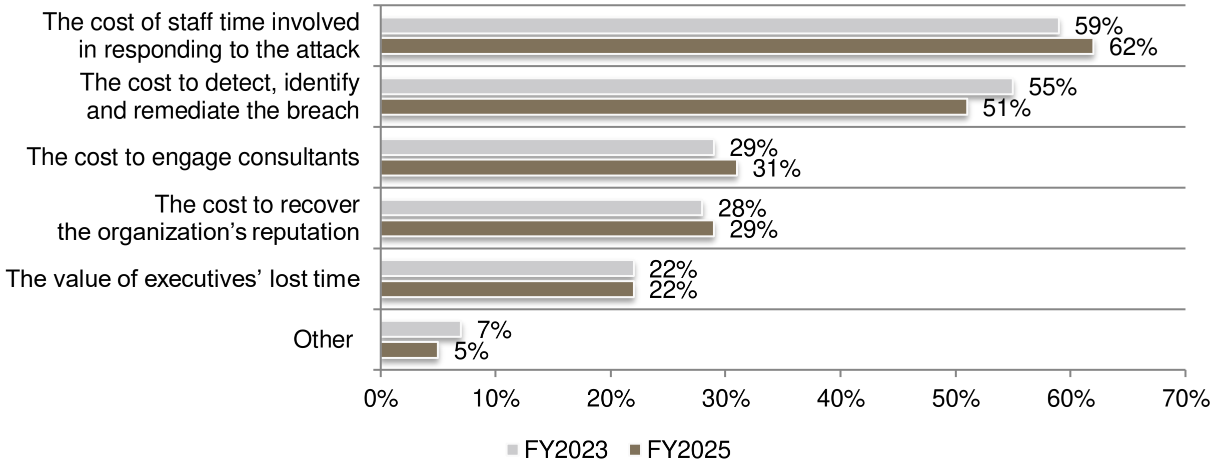
Figure 7. Do organizations measure the potential financial consequences of attacks against executives and the business' digital assets?
Yes responses presented.



Metrics used to determine the financial consequences of a digital cyberattack against executives remain the same since 2023. As shown in Figure 8, the top two metrics for cyberattacks against executives are the cost of staff time (62 percent of respondents) and the cost to detect, identify and remediate the breach (51 percent of respondents).

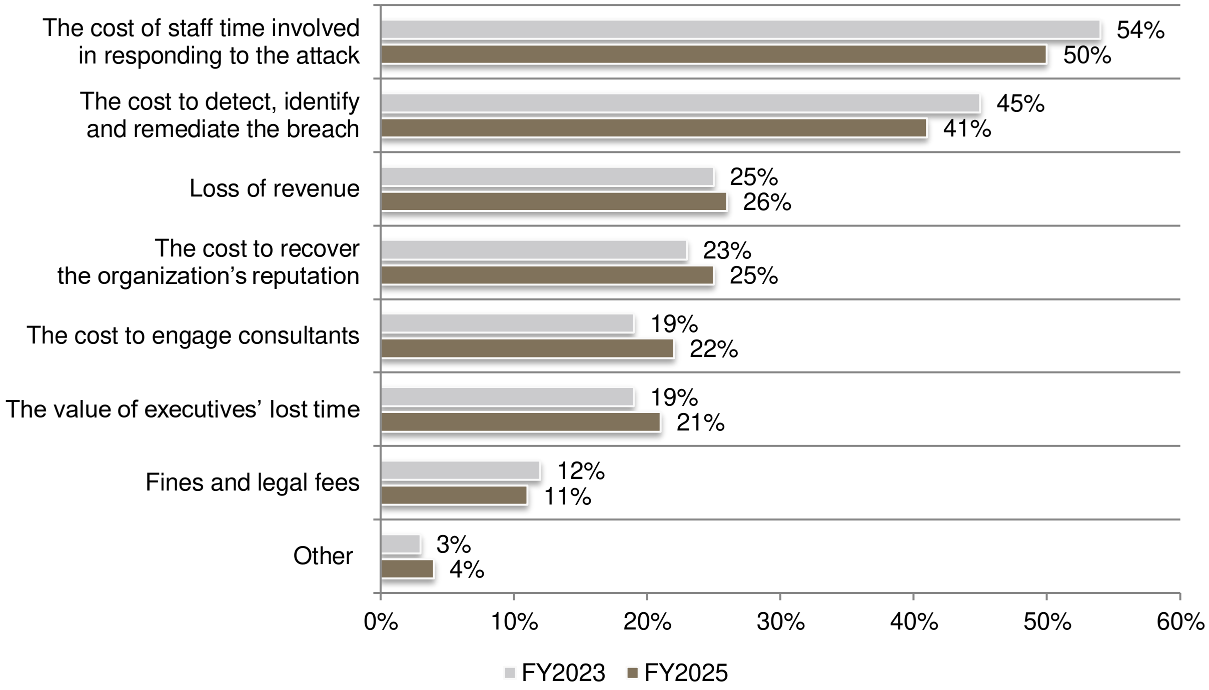
Figure 8. Metrics used to measure the potential financial consequences of a cyberattack against your executives and their digital assets.

Two responses permitted.



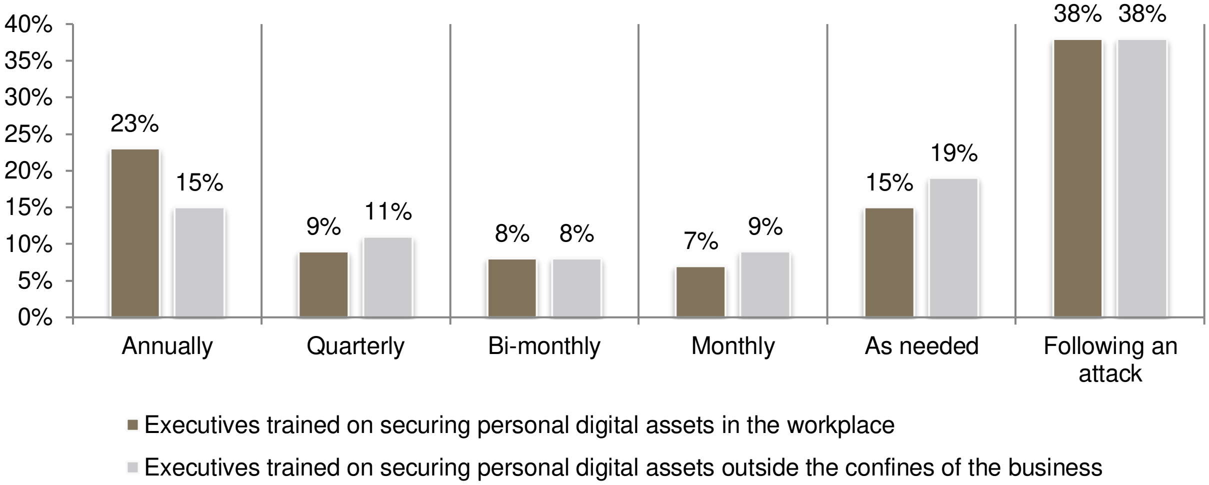
Metrics used to determine the financial consequences of attacks against the business are also the cost of staff time and the cost to detect, identify and remediate the breach, 50 percent and 41 percent of respondents respectively. There were slight decreases from 2023.

Figure 9. Metrics used to measure the potential financial consequences of a cyberattack against the business due to a cyberattack against the personal lives of executives and digital assets.
Two responses permitted.



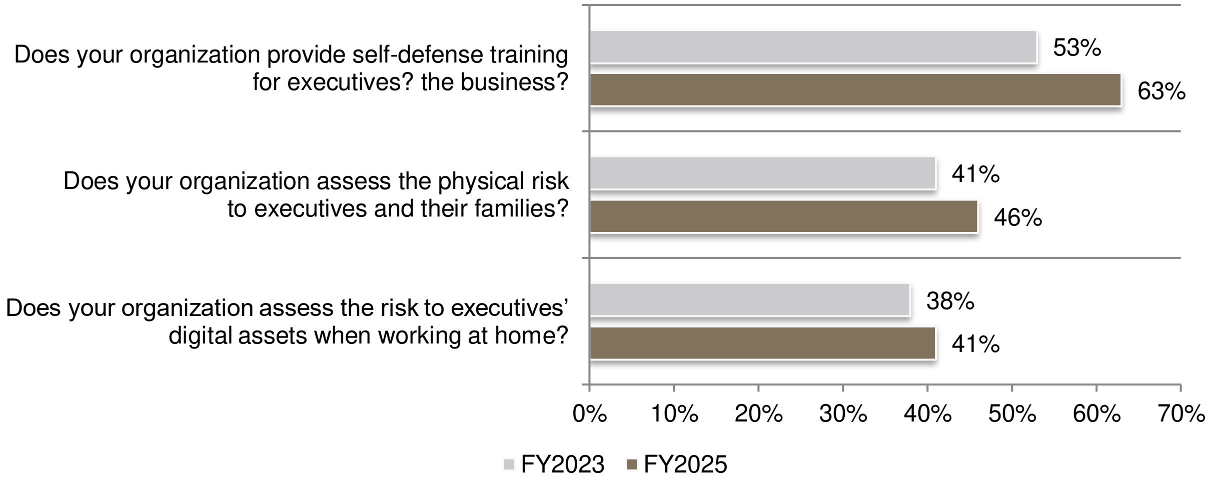
Despite the vulnerability of executives' digital assets, most training occurs following an attack. As shown in Figure 10, most training is done after the damage is done, according to 38 percent of respondents in 2023 and 2024.

Figure 10. How often are executives trained to secure personal digital assets in the workplace and outside the workplace?



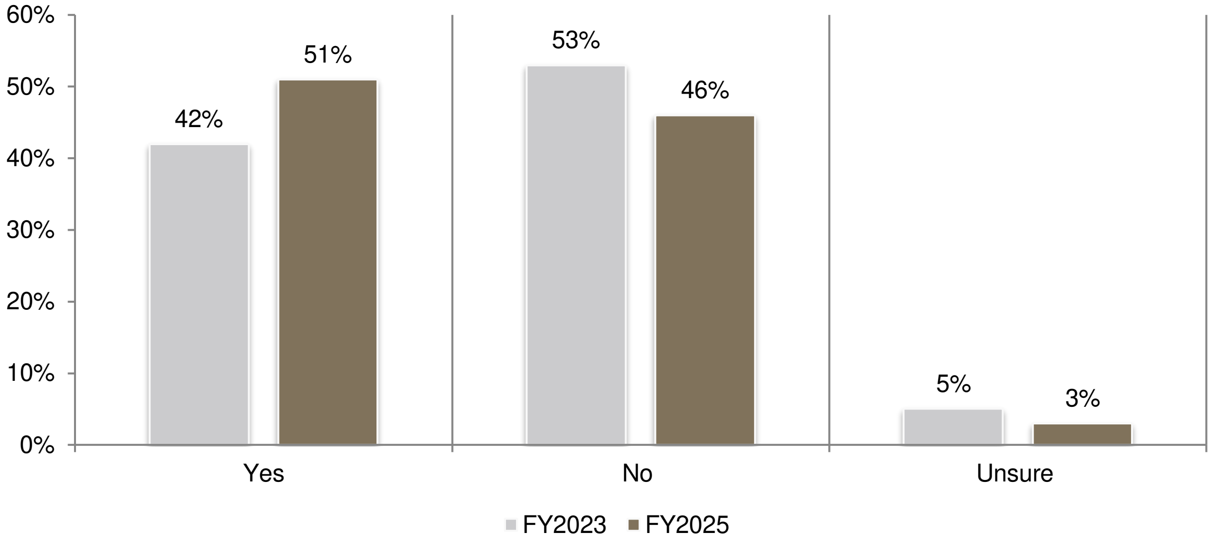
More organizations are providing self-defense training. According to Figure 11, self-defense training has increased since 2023 from 53 percent of respondents to 63 percent of respondents in 2025. Slightly more organizations are assessing the physical risk to executives and their families from 41 percent to 46 percent of respondents. Forty-one percent assess the risk to executives' digital assets when working at home.

Figure 11. The assessment of risk to executives and the increase in self-defense training
Yes responses presented.



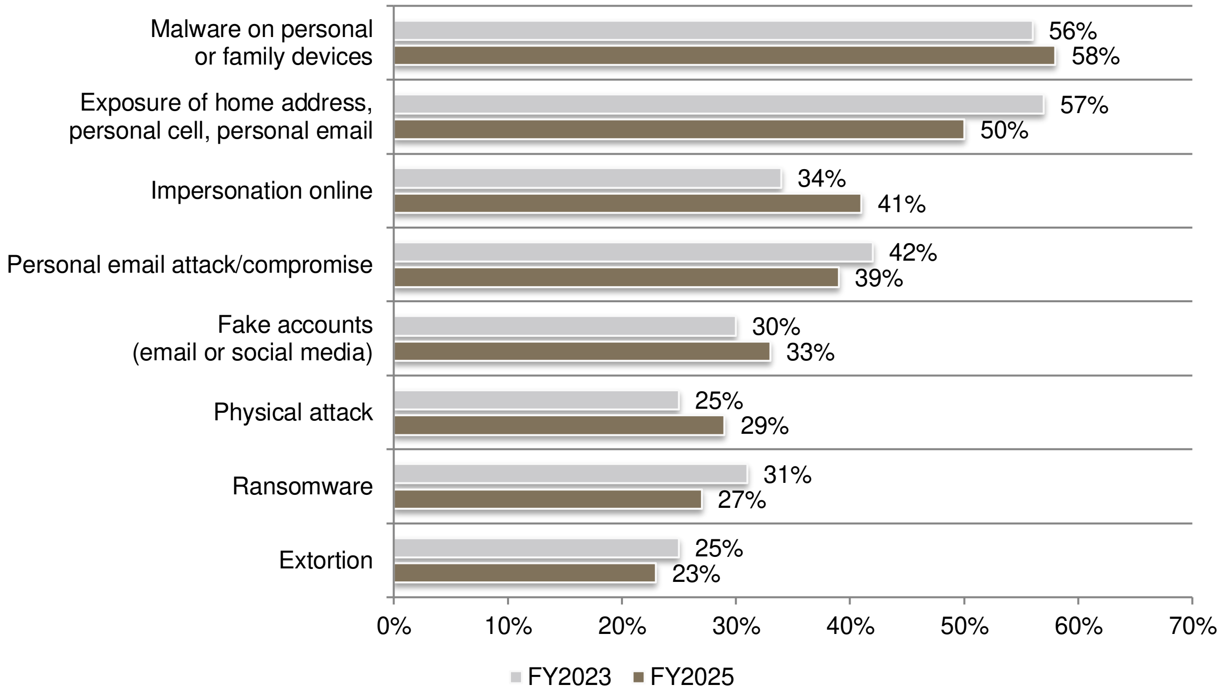
Attacks against executives and family members increase. Organizations need to assess the physical and digital asset risks to executives and their families. In 2023, 42 percent of respondents said there were attacks against executives and family members. This increased to 51 percent in 2025, as shown in Figure 12.

Figure 12. Have any of your executives or family members experienced an attack by a cybercriminal?



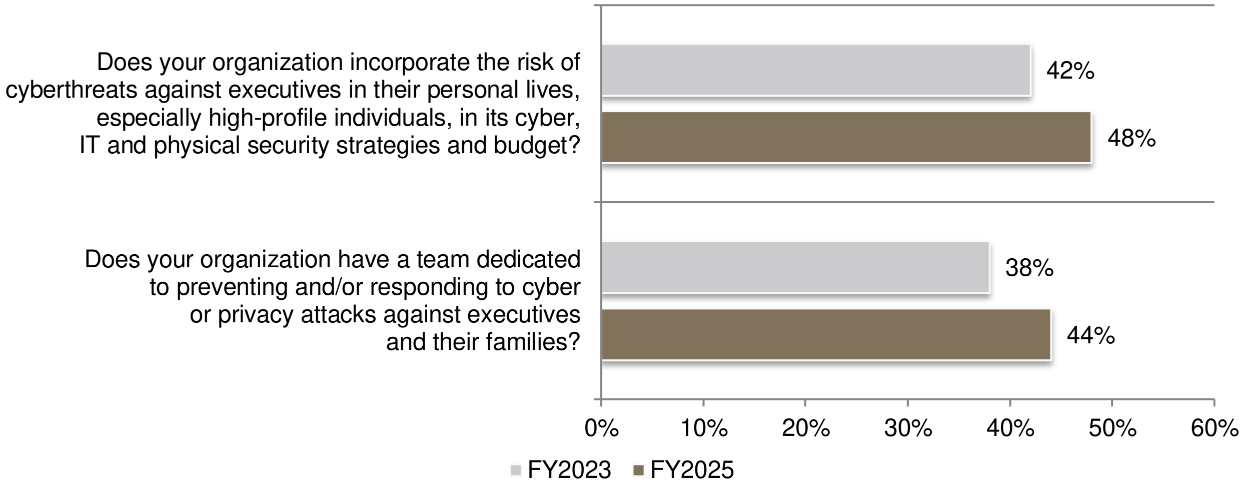
Online impersonations increased significantly since 2023. As shown in Figure 13, the most prevalent attacks continue to be malware on personal or family devices (58 percent of respondents in 2024 and 56 percent of respondents in 2023), exposure of home address, personal cell and personal email (50 percent of respondents down from 57 percent of respondents in 2023). However, online impersonations increased significantly from 34 percent of respondents in 2023 to 41 percent of respondents in 2024.

Figure 13. What types of attacks did your executives experience?
Three responses permitted.



While still a low number, more organizations are increasing budgets and other resources because of the need to protect executives and their digital assets. According to Figure 14, since 2023 48 percent of respondents say their organizations incorporate the risk of cyberthreats against executives in their personal lives, especially high-profile individuals in their cyber, IT and physical security strategies and budget, an increase from 42 percent of respondents. More organizations have a team dedicated to preventing and/or responding to cyber or privacy attacks against executives and their families, an increase from 38 percent to 44 percent of respondents.

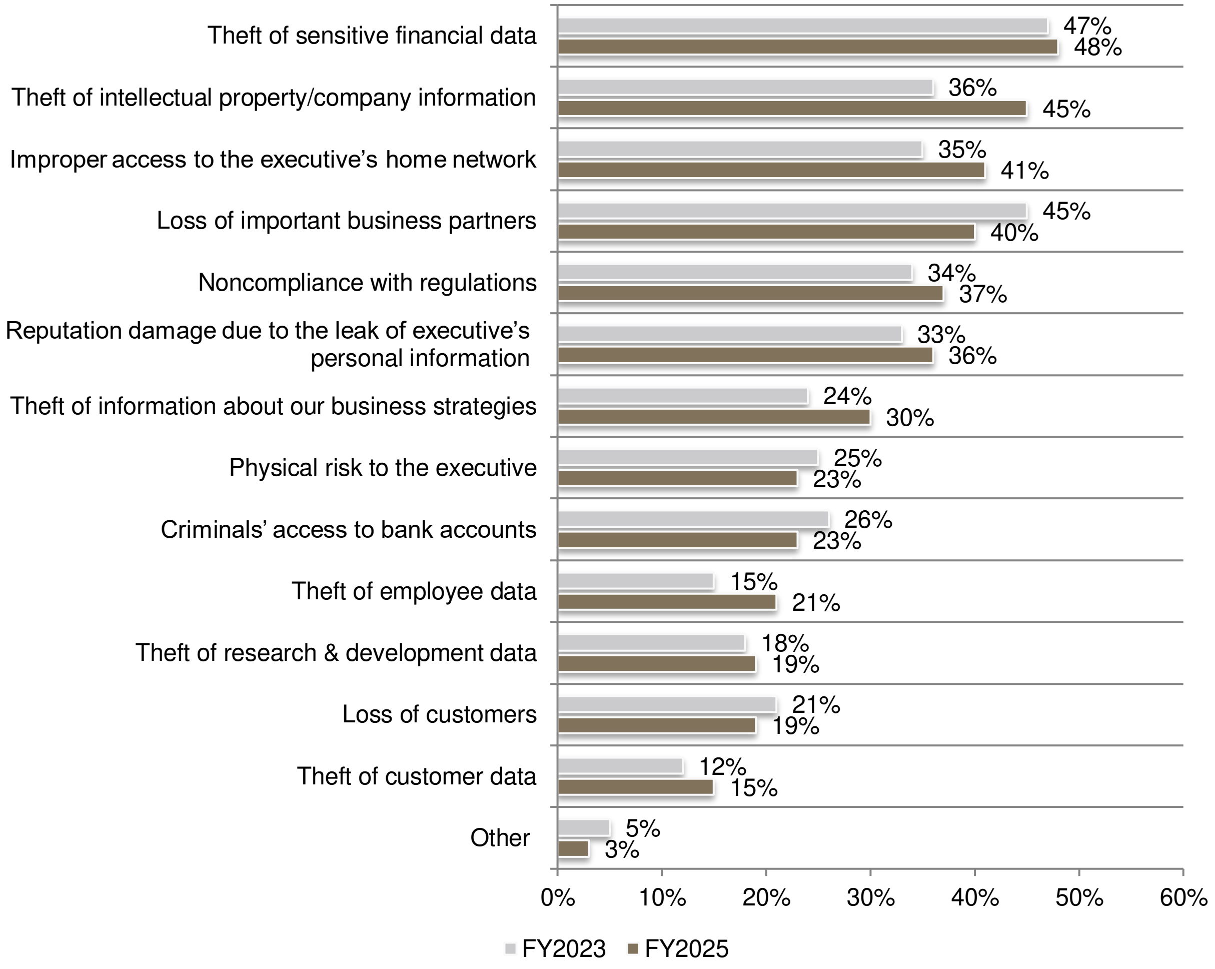
Figure 14. Steps to protect executives from cyber risks.
Yes responses presented.



More cybercriminals are targeting IP and executive's home network. Organizations should be concerned that their company information, including IP and executives' home networks, have become more vulnerable since 2023.

According to Figure 15, the theft of intellectual property and improper access to the executive's home network have increased from 36 percent of respondents to 45 percent of respondents and 35 percent of respondents to 41 percent of respondents, respectively. Other significant consequences were the theft of financial data (48 percent of respondents) and loss of important business partners (40 percent of respondents).

Figure 15. What were the consequences of a cyberattack against the lives and/or digital assets of executives?
More than one response permitted.

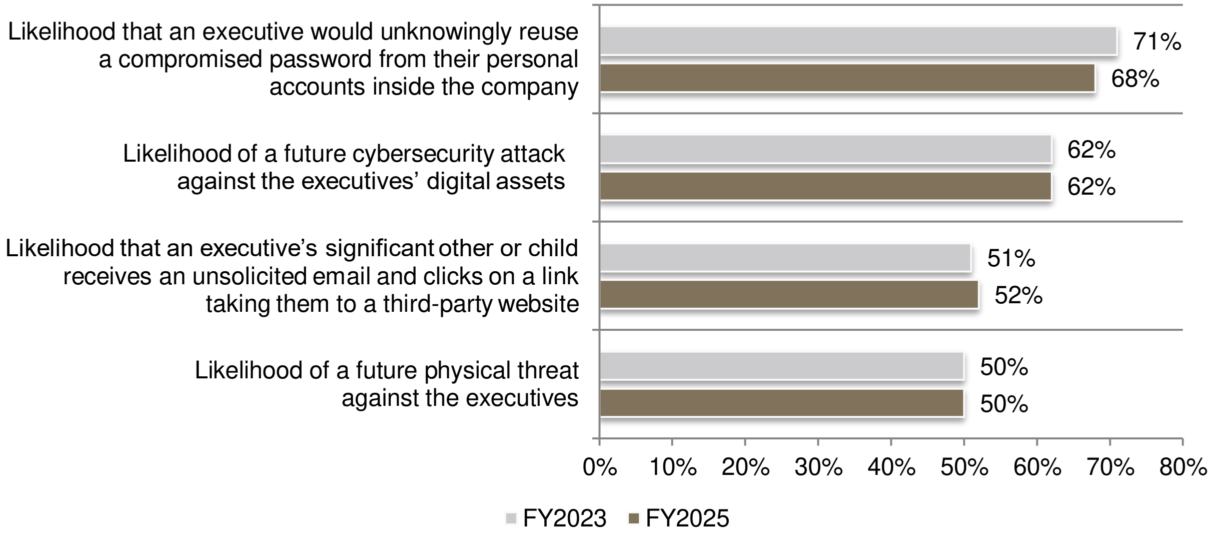


Since 2023, cyberattacks against executives continue to be highly likely, but are organizations better able to respond?

The likelihood of physical attacks and attacks against executives' digital assets has not decreased in the past year. Respondents were asked to rate the likelihood of attacks and threats on a scale of 1 = not likely to 10 = highly likely. Figure 16 shows the highly likely responses (7+ on the 10-point scale).

Sixty-two percent of respondents in 2023 and 2024 say it is highly likely a cybersecurity attack will be made against executives' digital assets and 50 percent in both years say there will be a physical threat against executives. As discussed previously, organizations are slow to train executives on how to avoid a successful attack against their digital assets. Sixty-eight percent of respondents say it is highly likely that an executive would unknowingly reuse a compromised password from their personal accounts inside the company and 52 percent of respondents say an executive's significant other or child would click on an unsolicited email that takes them to a third-party website.

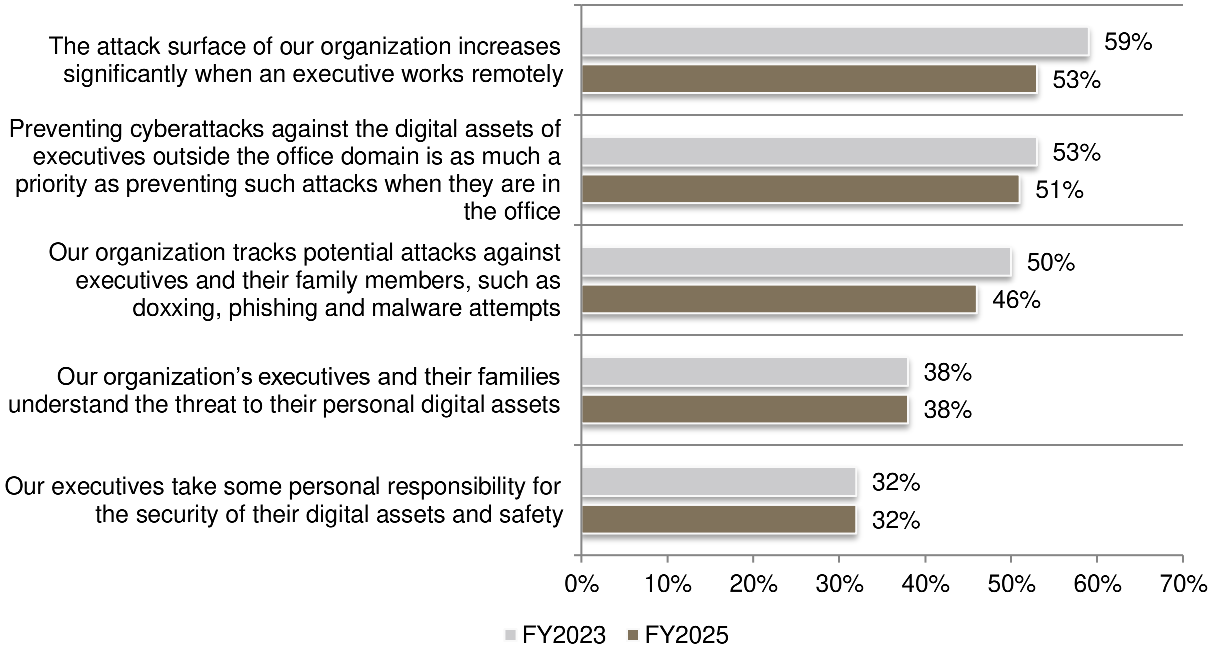
Figure 16. The likelihood of cyberattacks involving digital assets and physical threats.
On a scale from 1 = not likely to 10 = highly likely, 7+ responses presented



Why is it difficult to protect executives' digital assets? Figure 17 lists the challenges organizations face in protecting executives' digital assets. The top two challenges are due to remote working and not making protection of digital assets a priority when executives work outside the office, 53 percent and 51 percent of respondents, respectively.

As a consequence of not training executives to protect their digital assets, only 38 percent of respondents say their executives and families understand the threat to their personal digital assets and only 32 percent of executives take personal responsibility for the security and safety of their digital assets.

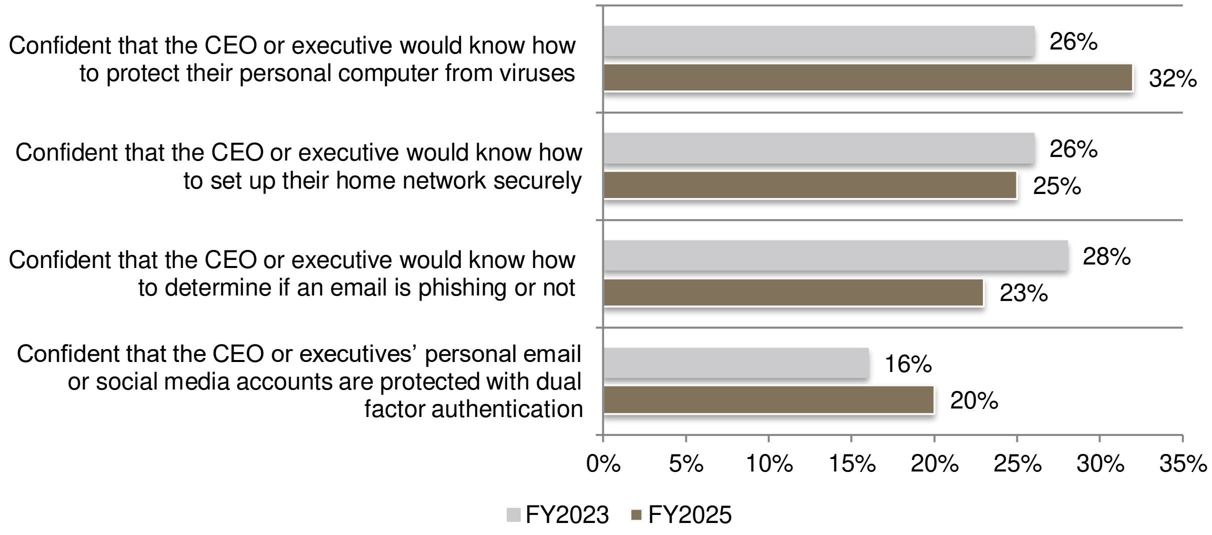
Figure 17. The challenges of protecting executives' digital assets
Strongly agree and Agree responses combined



Confidence in CEOs' and executives' ability to do the right thing to stop cyberattacks continues to be low. Respondents were asked to rate their level of confidence in their executives' ability to protect their digital assets on a scale from 1 = not confident to 10 = highly confident. Figure 18 presents the highly confident responses, (7+ on the 10-point scale).

While there is an increase in confidence in the CEO or executive knowing how to protect their personal computer from viruses (32 percent of respondents, an increase from 26 percent of respondents in 2023), it is still too low. Also, there is a decrease in executives knowing how to determine if an email is phishing (23 percent of respondents from 28 percent in 2023). Organizations also lack confidence in their executives knowing how to set up their home network security (25 percent of respondents percent of respondents and 26 percent of respondents in 2023) and knowing if their email or social media accounts are protected with dual factor authentication (20 percent of respondents and 16 percent of respondents in 2023).

Figure 18. Confidence in reducing the risk of cyberattacks.
One a scale from 1 = not confident to 10 = highly confident, 7+ responses presented

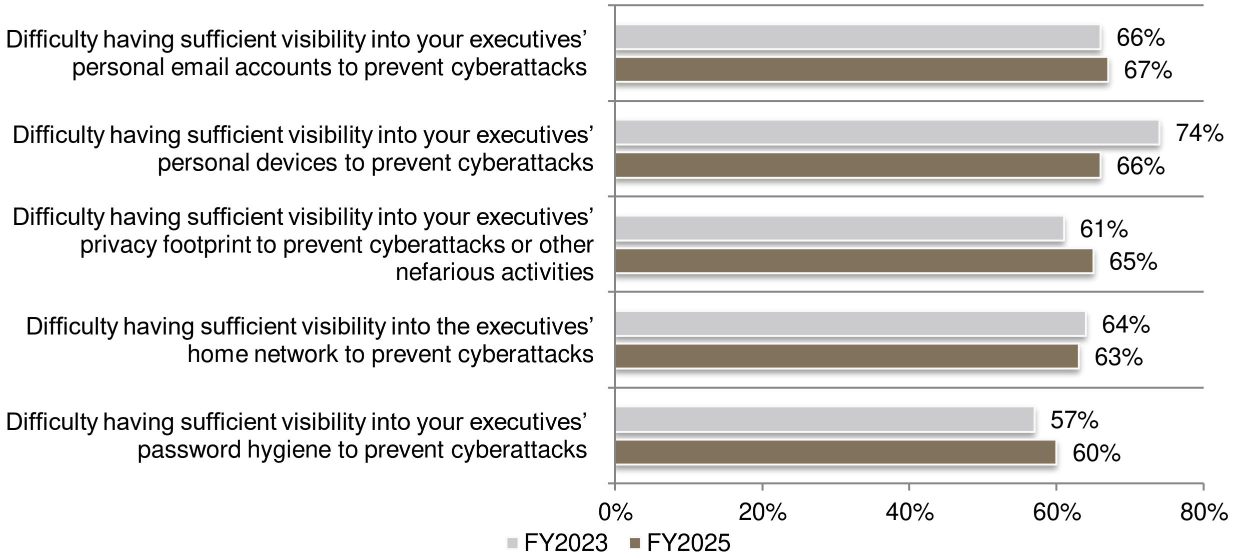


Difficulty in stopping cyberattacks against executives and their digital assets remains high.

Respondents were asked to rate the difficulty in stopping cyberattacks against executives and their digital assets as 1 = not difficult to 10 = highly difficult. Figure 18 presents the highly difficult responses, 7+ on the 10-point scale.

As shown, It continues to be highly difficult to have sufficient visibility into executives' home networks cyberattacks (63 percent of respondents), to have sufficient visibility into executives' personal devices (66 percent of respondents), sufficient visibility into executives' personal email accounts (67 percent of respondents), sufficient visibility into executives' password hygiene (60 percent of respondents) and sufficient visibility into executives' privacy footprint (65 percent of respondents).

Figure 19. Difficulty in reducing risks.
One a scale from 1 = not difficult to 10 = highly difficult, 7+ responses presented



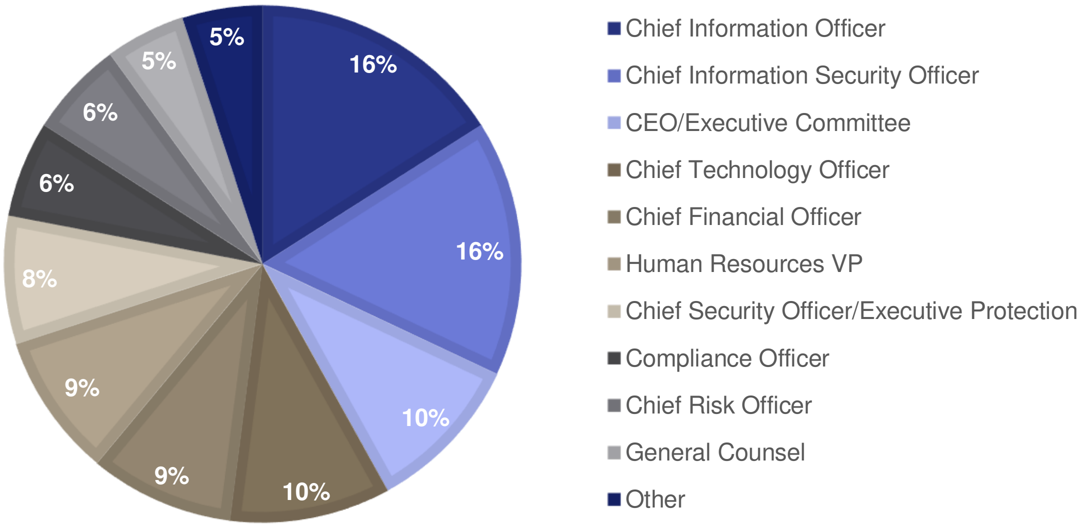
Part 3. Methodology

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.

Table 1. Sample response	Freq	Pct%
Sampling frame	17,100	100.0%
Total returns	633	3.7%
Rejected or screened surveys	47	0.3%
Final sample	586	3.4%

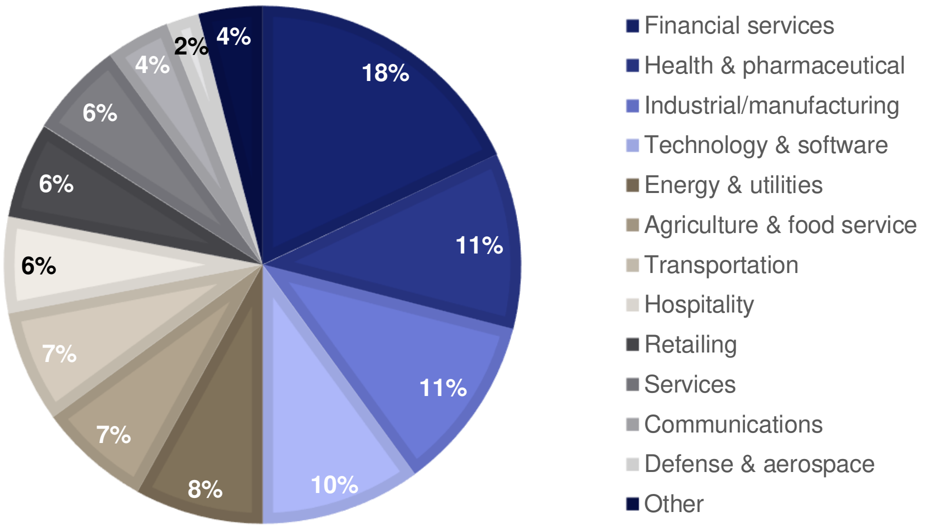
Pie Chart 1 reports the primary person the respondent reports to within the organization. Sixteen percent of respondents report to the chief information officer, 16 percent of respondents report to the chief information security officer, 10 percent report to the CEO/Executive Committee, 10 percent of respondents report to the chief technology officer, 9 percent of respondents report to the chief compliance officer, and 9 percent of respondents report to the human resources VP as shown in Pie Chart 1.

Pie Chart 1. Primary person respondent reports to within the organization



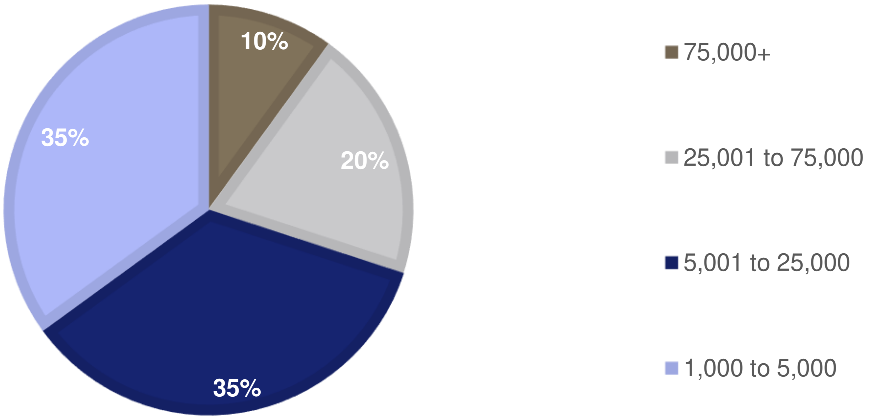
Pie Chart 2 reports the industry focus of respondents' organizations. This chart identifies financial services (18 percent) as the largest industry focus, which includes banking, investment management, insurance, brokerage, payments and credit cards. This is followed by healthcare and pharmaceuticals (11 percent of respondents), industrial manufacturing (11 percent of respondents), technology and software (10 percent of respondents), and energy and utilities (8 percent of respondents).

Pie Chart 2. Primary industry focus



As shown in Pie Chart 3, 35 percent of respondents are from organizations with a global headcount between 5,000 and 25,000 employees, 35 percent of respondents are from organizations with a global headcount between 1,000 and 5,000 and 20 percent of respondents are from organizations with a global headcount between 25,000 and 75,000 employees.

Pie Chart 3. Global full-time headcount



Part 4. 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.

Part 5. Appendix with the detailed audited findings

The following tables provide the frequency or percentage frequency of responses to all survey questions contained in this study. All survey responses were captured in February 2025.

Survey Response	FY2025	FY2023
Total sampling frame	17100	16,450
Total survey returns	633	605
Rejected surveys	47	52
Final survey	586	553
Response rate	3.4%	3.4%

Screening Questions

S1. What best describes your primary organizational role or area of focus? Please select one choice only.	FY2025
Cybersecurity C-level executive	12%
Cybersecurity VP	14%
Cybersecurity director/manager	15%
Security compliance and privacy management	11%
Cybersecurity staff/operations	9%
IT C-level executive	10%
IT VP	7%
IT director/manager	8%
IT operations	9%
None of the above (stop)	5%
Total	100%

S2. How knowledgeable are you about deepfake risks?	FY2025
Significant knowledge	41%
Knowledgeable	39%
Somewhat knowledgeable	20%
Total	100%

S3. How knowledgeable and involved are you in your organization’s programs and policies to prevent deepfake risks?	FY2025
Very knowledgeable and involved	28%
Knowledgeable and involved	38%
Somewhat knowledgeable	34%
Total	100%

S4. How knowledgeable are you about your organization’s technologies that can be used to mitigate deepfake risks against executives and their digital assets?	FY2025
Significant knowledge	21%
Knowledgeable	39%
Somewhat knowledgeable	40%
Total	100%

Part 1. The ability to address the deepfake risk.

Q1. What types of deepfake risks is your organization most concerned about? Please select the top two deepfake risks	FY2025
Social imposter	53%
Financial fraud	37%
Misinformation	29%
Impersonation	24%
Behavioral mimicry	30%
Personalized content	15%
Voice cloning	12%
Total	200%

Q2. Have your executives been targeted by a fake image or video?	FY2025
Yes	42%
No (please skip to Q5)	40%
Unsure (please skip to Q5)	18%
Total	100%

Q3. If yes, how did the deepfake target the executive?	FY2025
Impersonation of trusted entities such as colleagues, executives, family members or known organizations	28%
Urgent messages such as the requirement of immediate payment or security breach detected	21%
Customized information about the target such as position, personal interests or relationships	15%
Falsification of information that could damage the reputation of the organization	12%
Falsification of requests to wire funds or make other financial transactions	15%
Threats to do physical harm	9%
Total	100%

Q4. If yes, how often were executives targeted in the past year?	FY2025
1	35%
2 to 4	36%
More than 4	18%
Unsure	11%
Total	100%

Q5. Does your organization train or have plans to train executives to recognize deepfakes?	FY2025
Yes, currently	11%
Yes, in the next 6 months	14%
Yes, in the next 12 months	25%
No plans to train executives	50%
Total	100%

Q6. Does your organization have or plan to have an incident response plan with a dedicated team when deepfakes occur?	FY2025
Yes, currently	14%
Yes, in the next 6 months	21%
Yes, in the next 12 months	34%
No plans to have an incident response plan	31%
Total	100%

Q7a. Have you measured the potential financial consequences of a deepfake targeting your executives?	FY2025
Yes	36%
No	64%
Total	100%

Q7b. If yes, what metrics do you use? Please select your top two (2) choices.	FY2025
The cost of staff time involved in responding to the attack	46%
The cost to detect, identify and remediate the breach	50%
The cost to engage consultants	34%
The cost to recover the organization's reputation	37%
The value of executives' lost time	26%
Other (please specify)	7%
Total	200%

Q8. Using the following 10-point scale, please rate the likelihood of a future deepfake targeting your executives from 1 = not likely to 10 = highly likely.	FY2025
1 or 2	10%
3 or 4	13%
5 or 6	11%
7 or 8	35%
9 or 10	31%
Total	100%

Q9. Using the following 10-point scale, please rate the likelihood your organization will evaluate technologies that can reduce the risks from deepfake risks targeting executives from 1 = not likely to 10 = highly likely.	FY2025
1 or 2	16%
3 or 4	12%
5 or 6	20%
7 or 8	22%
9 or 10	30%
Total	100%

Q10. Using the following 10-point scale, please rate the importance of technologies that enable executives to verify the identity and authentication of messages they receive from 1 = not important to 10 = highly important.	FY2025
1 or 2	15%
3 or 4	21%
5 or 6	11%
7 or 8	27%
9 or 10	26%
Total	100%

Q11. Using the following 10-point scale, please rate the difficulty in being able to detect a deepfake targeting executives from 1 = not difficult to 10 = highly difficult.	FY2025
1 or 2	13%
3 or 4	11%
5 or 6	17%
7 or 8	27%
9 or 10	32%
Total	100%

Q12. Using the following 10-point scale, please rate the visibility into erroneous activity happening within your organization to prevent deepfake threats from 1 = not visible to 10 = high visibility	FY2025
1 or 2	23%
3 or 4	27%
5 or 6	16%
7 or 8	13%
9 or 10	21%
Total	100%

Q13. Using the following 10-point scale, please rate how confident you are that executives would know how to recognize deepfake risks from 1 = not confident to 10 = highly confident.	FY2025
1 or 2	24%
3 or 4	23%
5 or 6	16%
7 or 8	19%
9 or 10	18%
Total	100%

Q14. Deepfake is one of the most worrying uses of artificial intelligence (AI).	FY2025
Strongly agree	28%
Agree	26%
Unsure	13%
Disagree	15%
Strongly disagree	18%
Total	100%

Q15. A zero-trust mindset is essential to being able to distinguish between what is authentic and what is fake in messages.	FY2025
Strongly agree	26%
Agree	30%
Unsure	15%
Disagree	14%
Strongly disagree	15%
Total	100%

Part 2. Cybersecurity threats against executives and their digital assets

Q16. Does your organization incorporate the risk of cyber threats against executives in their personal lives, especially high-profile individuals, in its cyber, IT and physical security strategies and budget?	FY2025	FY2023
Yes	48%	42%
No	52%	58%
Total	100%	100%

Q17. Does your organization have a team dedicated to preventing and/or responding to cyber or privacy attacks against executives and their families?	FY2025	FY2023
Yes	44%	38%
No	56%	62%
Total	100%	100%

Q18. Have any of your executives or family members experienced an attack by a cybercriminal?	FY2025	FY2023
Yes	51%	42%
No (please skip to Q21a)	46%	53%
Unsure (please skip to Q21a)	3%	5%
Total	100%	100%

Q19. If yes, what types of attacks did your executives experience? Please check the top 3 choices.	FY2025	FY2023
Personal email attack/compromise	39%	42%
Exposure of home address, personal cell, personal email	50%	57%
Extortion	23%	25%
Fake accounts (email or social media)	33%	30%
Impersonation online	41%	34%
Malware on personal or family devices	58%	56%
Ransomware	27%	31%
Physical attack	29%	25%
Total	300%	300%

Q20a. If yes, in the past two years how many times has a cyberattack against the lives and/or digital assets of your executives occurred?	FY2025	FY2023
One	30%	34%
2 to 4	22%	26%
5 to 7	10%	12%
7 to 10	22%	15%
More than 10	12%	10%
Unsure	4%	3%
Total	100%	100%

Q20b. If yes, what were the consequences of the attack? Please select all that apply.	FY2025	FY2023
Criminals' access to bank accounts	23%	26%
Loss of customers	19%	21%
Loss of important business partners	40%	45%
Noncompliance with regulations	37%	34%
Physical risk to the executive	23%	25%
Reputation damage due to the leak of executive's personal information	36%	33%
Improper access to the executive's home network	41%	35%
Theft of customer data	15%	12%
Theft of employee data	21%	15%
Theft of intellectual property/company information	45%	36%
Theft of research & development data	19%	18%
Theft of sensitive financial data	48%	47%
Theft of information about our business strategies	30%	24%
Other (please specify)	3%	5%
Total	400%	376%

Q21a. Have you measured the potential financial consequences of a cyberattack against your executives and their digital assets?	FY2025	FY2023
Yes	43%	39%
No	57%	61%
Total	100%	100%

Q21b. If yes, what metrics do you use? Top two choices only.	FY2025	FY2023
The cost of staff time involved in responding to the attack	62%	59%
The cost to detect, identify and remediate the breach	51%	55%
The cost to engage consultants	31%	29%
The cost to recover the organization's reputation	29%	28%
The value of executives' lost time	22%	22%
Other (please specify)	5%	7%
Total	200%	200%

Q22a. Have you measured the potential financial consequences of a cyberattack against the business due to a cyberattack against the personal lives of executives and digital assets?	FY2025	FY2023
Yes	40%	43%
No	60%	57%
Total	100%	100%

Q22b. If yes, what metrics do you use? Top two choices only.	FY2025	FY2023
The cost of staff time involved in responding to the attack	50%	54%
The cost to detect, identify and remediate the breach	41%	45%
The cost to engage consultants	22%	19%
The cost to recover the organization's reputation	25%	23%
The value of executives' lost time	21%	19%
Fines and legal fees	11%	12%
Loss of revenue	26%	25%
Other (please specify)	4%	3%
Total	200%	200%

Likelihood scale

Q23. Using the following 10-point scale, please rate the likelihood of a future cybersecurity attack against your executives' digital assets from 1 = not likely to 10 = highly likely.	FY2025	FY2023
1 or 2	8%	9%
3 or 4	11%	12%
5 or 6	19%	17%
7 or 8	24%	20%
9 or 10	38%	42%
Total	100%	100%

Q24. Using the following 10-point scale, please rate the likelihood of a future physical threat against your executives from 1 = not likely to 10 = highly likely.	FY2025	FY2023
1 or 2	17%	18%
3 or 4	23%	20%
5 or 6	10%	12%
7 or 8	23%	22%
9 or 10	27%	28%
Total	100%	100%

Q25. Using the following 10-point scale, please rate the likelihood that an executive's significant other or child receives an unsolicited email and clicks on a link taking them to a third-party website? from 1 = not likely to 10 = highly likely.	FY2025	FY2023
1 or 2	15%	12%
3 or 4	13%	17%
5 or 6	20%	20%
7 or 8	26%	25%
9 or 10	26%	26%
Total	100%	100%

Q26. Using the following 10-point scale, please rate the likelihood that an executive would unknowingly reuse a compromised password from their personal accounts inside the company? from 1 = not likely to 10 = highly likely.	FY2025	FY2023
1 or 2	8%	7%
3 or 4	9%	10%
5 or 6	15%	12%
7 or 8	33%	37%
9 or 10	35%	34%
Total	100%	100%

Confidence scale

Confidence scale		
Q27. Using the following 10-point scale, please rate how confident you are that the CEO or executive would know how to protect their personal computer from viruses from 1 = not confident to 10 = highly confident.	FY2025	FY2023
1 or 2	29%	33%
3 or 4	20%	21%
5 or 6	19%	20%
7 or 8	20%	17%
9 or 10	12%	9%
Total	100%	100%

Q28. Using the following 10-point scale, please rate how confident you are that the CEO or executive would know how to determine if an email is phishing or not from 1 = not confident to 10 = highly confident.	FY2025	FY2023
1 or 2	39%	33%
3 or 4	24%	22%
5 or 6	14%	17%
7 or 8	11%	16%
9 or 10	12%	12%
Total	100%	100%

Q29. Using the following 10-point scale, please rate how confident you are that the CEO or executive would know how to set up their home network securely from 1 = not confident to 10 = highly confident.	FY2025	FY2023
1 or 2	27%	33%
3 or 4	31%	26%
5 or 6	17%	15%
7 or 8	5%	8%
9 or 10	20%	18%
Total	100%	100%

Q30. Using the following 10-point scale, please rate how confident you are that the CEO or executives' personal email or social media accounts are protected with dual factor authentication from 1 = not confident to 10 = highly confident.	FY2025	FY2023
1 or 2	38%	39%
3 or 4	29%	32%
5 or 6	13%	13%
7 or 8	12%	9%
9 or 10	8%	7%
Total	100%	100%

Q31. Using the following 10-point scale, please rate the effectiveness of verifying the authenticity of messages sent to CEO or executives' personal email or social media accounts from 1 = not effective to 10 = highly effective.	FY2025	FY2023
1 or 2	28%	33%
3 or 4	28%	26%
5 or 6	13%	15%
7 or 8	11%	8%
9 or 10	20%	18%
Total	100%	100%

Difficult scale

Q32. How difficult is it to have sufficient visibility into your executives' home network to prevent cyberattacks from 1 = not difficult to 10 = highly difficult.	FY2025	FY2023
1 or 2	5%	2%
3 or 4	8%	9%
5 or 6	24%	25%
7 or 8	45%	42%
9 or 10	18%	22%
Total	100%	100%

Q33. How difficult is it to have sufficient visibility into your executives' personal devices to prevent cyberattacks from 1 = not difficult to 10 = highly difficult.	FY2025	FY2023
1 or 2	6%	2%
3 or 4	15%	6%
5 or 6	13%	18%
7 or 8	33%	33%
9 or 10	33%	41%
Total	100%	100%

Q34. How difficult is it to have sufficient visibility into your executives' personal email accounts to prevent cyberattacks from 1 = not difficult to 10 = highly difficult.	FY2025	FY2023
1 or 2	6%	3%
3 or 4	11%	9%
5 or 6	16%	22%
7 or 8	33%	37%
9 or 10	34%	29%
Total	100%	100%

Q35. How difficult is it to have sufficient visibility into your executives’ password hygiene to prevent cyberattacks from 1 = not difficult to 10 = highly difficult.	FY2025	FY2023
1 or 2	11%	14%
3 or 4	10%	12%
5 or 6	19%	17%
7 or 8	30%	30%
9 or 10	30%	27%
Total	100%	100%

Q36. How difficult is it to have sufficient visibility into your executives’ privacy footprint to prevent cyberattacks or other nefarious activities from 1 = not difficult to 10 = highly difficult.	FY2025	FY2023
1 or 2	7%	8%
3 or 4	7%	9%
5 or 6	21%	22%
7 or 8	35%	33%
9 or 10	30%	28%
Total	100%	100%

Part 3. Attributions

Please rate each statement and questions using the scale provided below each item.

Q37a. 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.	FY2025	FY2023
Strongly agree	16%	19%
Agree	35%	34%
Unsure	16%	13%
Disagree	21%	21%
Strongly disagree	12%	13%
Total	100%	100%

Q37b. The attack surface of our organization increases significantly when an executive works remotely.	FY2025	FY2023
Strongly agree	32%	35%
Agree	21%	24%
Unsure	16%	15%
Disagree	17%	15%
Strongly disagree	14%	11%
Total	100%	100%

Q37c. Our organization tracks potential attacks against executives and their family members, such as doxxing, phishing and malware attempts.	FY2025	FY2023
Strongly agree	22%	27%
Agree	24%	23%
Unsure	24%	20%
Disagree	19%	16%
Strongly disagree	11%	14%
Total	100%	100%

Q37d. Our organization's executives and their families understand the threat to their personal digital assets.	FY2025	FY2023
Strongly agree	15%	12%
Agree	23%	26%
Unsure	18%	17%
Disagree	15%	20%
Strongly disagree	29%	25%
Total	100%	100%

Q37e. Our executives take some personal responsibility for the security of their digital assets and safety.	FY2025	FY2023
Strongly agree	9%	6%
Agree	23%	26%
Unsure	12%	13%
Disagree	25%	21%
Strongly disagree	31%	34%
Total	100%	100%

Part 4. Understanding the risk of cyberattacks against executives.

Q38. Who is most responsible for digital executive protection? Please select only one choice.	FY2025	FY2023
Business units	12%	16%
Executive suite	9%	8%
IT operations	20%	21%
IT security	23%	27%
Legal	7%	5%
Physical security	10%	8%
No one is most responsible	19%	15%
Total	100%	100%

Q39. Does your organization assess the physical risk to executives and their families?	FY2025	FY2023
Yes	46%	41%
No	54%	59%
Total	100%	100%

Q40. Does your organization assess the risk to executives' digital assets when working at home?	FY2025	FY2023
Yes	41%	38%
No	59%	62%
Total	100%	100%

Q41a. Does your organization train executives on how to secure personal digital assets in the workplace?	FY2025	FY2023
Yes	43%	37%
No	57%	63%
Total	100%	100%

Q41b. If yes, how often	FY2025	FY2023
Annually	23%	23%
Quarterly	9%	9%
Bi-monthly	8%	8%
Monthly	7%	7%
As needed	15%	15%
Following an attack	38%	38%
Total	100%	100%

Q42a. Does your organization train executives on how to secure personal digital assets outside the confines of the business?	FY2025	FY2023
Yes	41%	36%
No	59%	64%
Total	100%	100%

Q42b. If yes, how often	FY2025	FY2023
Annually	15%	21%
Quarterly	11%	10%
Bi-monthly	8%	9%
Monthly	9%	8%
As needed	19%	18%
Following an attack	38%	34%
Total	100%	100%

Q43. Does your organization provide self-defense training for executives? the business?	FY2025	FY2023
Yes	63%	53%
No	37%	47%
Total	100%	100%

Part 5. Your role

D1. Check the Primary Person you or your IT security leader reports to within the organization.	FY2025	FY2023
CEO/Executive Committee	10%	8%
Chief Financial Officer	9%	7%
General Counsel	5%	4%
Chief Information Officer	16%	19%
Chief Technology Officer	10%	12%
Compliance Officer	6%	8%
Human Resources VP	9%	8%
Chief Security Officer/Executive Protection	8%	7%
Chief Information Security Officer	16%	16%
Chief Risk Officer	6%	8%
Other (please specify)	5%	3%
Total	100%	100%

D2. What is the worldwide headcount of your organization?	FY2025	FY2023
1,000 to 5,000	35%	32%
5,001 to 25,000	35%	31%
25,001 to 75,000	20%	37%
75,000+	10%	
Total	100%	100%

D3. What industry best describes your organization's industry focus?	FY2025	FY2023
Agriculture & food service	7%	8%
Communications	4%	5%
Defense & aerospace	2%	3%
Energy & utilities	8%	4%
Financial services	18%	18%
Health & pharmaceutical	11%	12%
Hospitality	6%	6%
Industrial/manufacturing	11%	9%
Retailing	6%	7%
Services	6%	5%
Technology & software	10%	11%
Transportation	7%	10%
Other (please specify)	4%	2%
Total	100%	100%

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.