

BLACKCLOAK®

A man with a beard and mustache, wearing a dark suit, white shirt, and striped tie. His face is split vertically down the middle. The left side of his face is in shadow and appears to be a different texture or color, while the right side is more defined and has a blueish tint. He is looking down with a serious expression, and his hands are clasped in front of him.

PREDICTIONS 2027

DIGITAL EXECUTIVE PROTECTION IN REVIEW



Dr. Chris Pierson,
Founder and CEO,
BlackCloak

Foreword

Security leaders need to confront 2027 knowing that attackers have learned to bypass traditional enterprise defenses by weaponizing one of our most basic human instincts—trust.

Ready or not, trust has become the new security perimeter, and failing to take a disciplined approach to authenticating it in the year ahead can come at a very hefty price.

For years, organizations have invested billions of dollars protecting corporate networks, devices, identities and data. Attackers have responded by looking beyond those defenses to the people with the greatest access, authority and influence and to the personal lives and trusted relationships that surround them.

This inner circle includes the spouses, significant others, children, assistants, colleagues and other people an executive communicates with and inherently trusts. Attackers increasingly understand that compromising or impersonating someone within that circle can be easier than attacking the executive, or the enterprise, head-on.

Artificial Intelligence makes that strategy even more dangerous. Attackers can conduct reconnaissance, map relationships, build convincing impersonations and launch highly personalized attacks in a fraction of the time it once required. At the same time, much of the personal information traditionally used to establish trust and validate identity should now be assumed compromised.

Your Social Security number is not a secret. Your date of birth is not a secret. Your address, phone number and family relationships may not be secrets either.

That means trust can no longer be assumed. It has to be validated.

This is one reason we developed Impersonation Protection at BlackCloak, giving executives an out-of-band method to authenticate communications. It represents a broader shift security leaders need to make as AI renders many of the traditional signals we have relied upon to establish trust increasingly unreliable.

And it is only one part of what needs to change.

The predictions we are making for 2027 reflect what I believe is the next stage in the evolution of Digital Executive Protection. Organizations will increasingly simulate attacks against executives before adversaries can launch them. Authentication will move toward stronger proof of identity. Insurance carriers will help turn executive security controls from recommendations into requirements. The artificial separation between physical and digital executive protection will continue to disappear. And boards will increasingly demand measurable evidence that these investments are actually reducing risk.

These aren't five isolated trends. They point to something much bigger.

Digital Executive Protection is becoming an enterprise risk discipline.

Protecting an executive and their family can no longer be treated as a perk or a concierge service bolted onto an existing security program. Personal risk becomes enterprise risk when an attacker can exploit someone's digital life or inner circle to commit financial fraud, breach the organization, damage its reputation or even cause physical harm.

Attackers already understand that reality.

In 2027, defenders will have to prove they do too.

Dr. Chris Pierson,
Founder and CEO, BlackCloak

Contents

The Year in 5 Numbers	5
Predictions 2027	6
Prediction 01 Attack timelines collapse and defense moves to simulation in the home	7
Prediction 02 Authentication moves out of band as personal data no longer proves identity	10
Prediction 03 Corporate insurance turns Digital Executive Protection into a requirement for coverage	13
Prediction 04 Digital and physical executive protection become one program, with one owner	17
Prediction 05 The category matures, and so does executive risk reporting	21
A Year in Review	24
Privacy & Identity Defense	25
AI Threat Protection	27
Executive Threat Intelligence	28
Personal Security Operations	29
Our 2026 Predictions, One Year On	31
Sources	38
About the Research	40

The Year in 5 Numbers

75%

of security teams surveyed were involved in at least one incident in the past 12 months that originated from a senior leader's or a family member's personal device, home network, or personal account, and 43% handled more than one¹.

3

most common threat vectors targeting senior leaders or their families in 2026 were: Phishing or smishing to personal accounts, AI generated impersonations, and credential harvesting/taking over personal accounts¹.

8.7

is the average number of total staff hours a security team spends investigating and remediating a single personal executive incident, including any downstream corporate impact¹. 28% of organizations took over 11hrs per incident.

54%

of organizations have no documented procedures in their incident response plan for executive breaches involving assets the organization does not own or manage¹.

85%

of security leaders surveyed believe it would be helpful to use a vendor to detect and mitigate incidents targeting executives in their personal lives. Yet only 6% do so currently, which is even more concerning when you consider half of these leaders did not discover such incidents through their own tools or scans¹.

DIGITAL EXECUTIVE
PROTECTION

**PREDICTIONS
2027**



Attack timelines collapse
and defense moves to
simulation in the home

01



The prediction

The time between detecting risk exposure in an executive's personal digital life, and an attack exploiting it will shrink significantly. "Using AI, threat actors can direct agents to undertake reconnaissance on multiple individuals, their families and contacts, build the attack, and run it in the time it used to take to plan," notes Matt Covington, SVP of Product, BlackCloak. "AI does the same thing for an attacker as it does for software engineering. It cuts the cost and time required to execute it." As such, personalization stops being the expensive option for a threat actor, and a one-size-fits-all consumer defense solution will be increasingly less effective.

The defensive answer to the problem is one enterprises already know but have never needed to apply to a household. Red and purple teaming are routine inside the corporate perimeter so they can expose vulnerabilities before an adversary does. "Executives will need attack simulation plans tailor made to the unique risks they face. Running simulated attacks exposes the specific vulnerabilities behind those risks," Covington says.

Signals behind the prediction

We have already seen the effect of AI on enterprise cyberattacks and the market has moved quickly to change defense tactics. As the softest entry point to the corporation, it is no surprise that this trend will extend to executives too. "You can personalize the entire attack pipeline now," says Chris Carter, OSINT and Threat Intelligence Manager, BlackCloak. "Threat actors could be on a walk while their agents are crafting an attack plan. Any defender that is not reciprocating attackers at the same level of technology is placing their executives at risk."

External signals that influenced this prediction

- Google Threat Intelligence Group reported in September 2026 that adversaries are moving from prompting to agentic workflows, including an operation that planned, built, scanned, and ran mass credential harvesting in under six hours².
- Writing on critical infrastructure in July 2026, Madison Horn warned about the speed of modern cyber risk, the impact on national security, and that defenders need to use AI to keep pace, rather than only defend against it³.
- The FBI's 2025 Internet Crime Report, published in April 2026, carried a dedicated section on artificial intelligence for the first time⁴, demonstrating growth in the scale and severity of this threat.



Why it is key for 2027

For organizations, the practical application to reduce executive risk will require taking what is genuinely known about a person: their exposed data, their properties, their family and staff, their public profile, and the devices on their network, before running simulated attacks against that profile and fixing what succeeds. Without the infrastructure in place to support this additional work, security teams will struggle to keep up with, let alone stay ahead of a motivated threat actor.



Authentication moves out
of band as personal data
no longer proves identity



The prediction

By 2027, an executive's Social Security number, date of birth, addresses, relatives, and phone numbers will have to be treated as information an adversary already holds. Organizations will need to move away from authentication that relies on personal knowledge because stolen data can no longer serve as meaningful proof of identity.

AI expands that problem beyond what a person knows. Authentication based on what someone knows or possesses—or whether they sound or look like the expected person—will all become less reliable.

Agents can research an executive, reconstruct their relationships, reproduce their voice and appearance, create convincing pretexts, and repeat the attack across multiple channels until something works. Defenders, however, must avoid both approving an attack and disrupting the legitimate executive. Manually reviewing every interaction will not scale against automated impersonation.

Deepfake detection will remain useful as a signal, but it cannot become the trust boundary. "A generator needs to evade a classifier only once; a classifier must continue working across every new model, modality, and transformation," says Swai Dhanoa, Head of AI, BlackCloak. "Watermarking faces a similar limitation because there is no universal standard and no way to require malicious or open-source models to participate."

The result will be a move toward human-factor authentication: independently confirming that a trusted person intended a specific action. Out-of-band authentication will be one mechanism, but the larger shift will be from recognizing an identity to verifying intent. "Threat actors are going to use AI and deepfakes more at the help desk support level. We started to see that this year, pretending to be an executive or an assistant to get access to an account," notes Dhanoa.

Signals behind the prediction

We regularly see attackers taking an executive's identity and impersonating them, using SIM swapping to intercept the code that authorizes a password reset, and telephone number spoofing. "Once a threat actor has taken the persona of an executive and reset their passwords they can then go after people within their inner circle and beyond," says Dhanoa.

In our 2025 research, 59% of security professionals rated deepfake detection as difficult or highly difficult, and 53% said technology that lets executives confirm the identity behind a message is highly important^{5,6}, which is why we launched Impersonation Protection, an out-of-band method for executives to authenticate communications from their contacts, earlier this year.

External signals that influenced this prediction

- NIST's Digital Identity Guidelines state that knowledge-based authentication is not an acceptable authentication secret, and that knowing a Social Security number is not sufficient evidence of identity⁷.
- Research on the Phantom Deal campaign describes attackers using real executive identities, corporate history, forged documents, WhatsApp, and personal email to manufacture a believable transaction, with no malware and no compromised corporate mailbox⁸.
- CISA, the FBI, and international partners describe attackers impersonating employees and IT help desk staff to obtain credentials and defeat multifactor authentication⁹.



Why it is key for 2027

Removal of and monitoring personal data reduces exposure, but it cannot hide exposed information once it is in the hands of a threat actor. The objective therefore becomes twofold: to continually reduce data exposure, but also to limit what an attacker can still accomplish with it once they have it.

The new trust boundary will not be, "Does this person know the right information, possess the right device, or look and sound like the executive?" It will be, "Did the executive intend for this specific action to happen?"



Corporate insurance
turns Digital Executive
Protection into a
requirement for coverage



The prediction

With the increased number and type of executive attacks, we predict that corporate insurance will become a leading force that moves Digital Executive Protection from recommendation to requirement. Policies are already shifting and some carriers have written AI-generated impersonation attacks into their social engineering coverage, while others have excluded it from coverage completely.

We expect two security controls to lead this trend. The first is home network assessment, because executives often use personal devices and home networks for work purposes, and it is an environment very few security teams test. "Home network security is becoming a named line item in cyber insurance underwriting," says Brian Hill, Field CISO, Client Advisory, BlackCloak. "Threat actors get into an executive's personal computer which becomes the bridge into a work computer. It's a huge gap."

The second control is anticipated to be defense against AI impersonations, because insurers are now pricing losses that originate from deepfake attacks rather than compromised systems. We believe this will turn an out-of-band control, such as Impersonation Protection, into a condition of the policy rather than a nice-to-have.



Signals behind the prediction

Corporate insurance requirements weigh heavily on organizations. When underwriters began asking for evidence of multi-factor authentication, there was a rapid response to change staff behavior. We expect impersonation controls to follow the same path.

In addition, home network scanning for executives has risen faster than any other service in buyer interest this year. This is unsurprising given that lack of visibility into personal devices, accounts, and home networks is the challenge security teams report most often¹, and the added pressure from underwriters is expected to fuel ongoing demand.

External signals that influenced this prediction

- Coalition introduced a Deepfake Response Endorsement across its policies globally, covering forensics, content removal, and crisis communications¹⁰.
- BOXX Insurance added affirmative AI and deepfake cover to its business policy in July 2026, explicitly including voice cloning and video deepfakes. The same reporting notes that other carriers moved the opposite way, excluding AI-generated deepfake fraud from standard social engineering cover for policies renewed from 1 January 2026¹¹.
- U.S. agencies issued repeated warnings during 2026 about the compromise of home and small office routers, including an FBI alert on exploitation by Russia's GRU and router hygiene guidance from the NSA and international partners^{12, 13} highlighting a previously underestimated attack vector.



Why it is key for 2027

Insurance is often what turns a recommendation into a requirement. When a carrier asks whether an executive's home network has been assessed, or what procedure confirmed a payment request before it was authorized, the answer determines whether a claim is paid. That moves the conversation from security preference to contractual obligation, and it puts a security leader in the position of having to evidence controls over an environment they do not own. No team wants to discover that gap during a large claim.





Digital and physical
executive protection
become one program,
with one owner



The prediction

Ownership of Digital Executive Protection will increasingly move to chief security officers and executive protection teams. Organizations will stop treating the executive's personal digital life as an orphan risk, and assign it a named owner, a written scope, and a budget line.

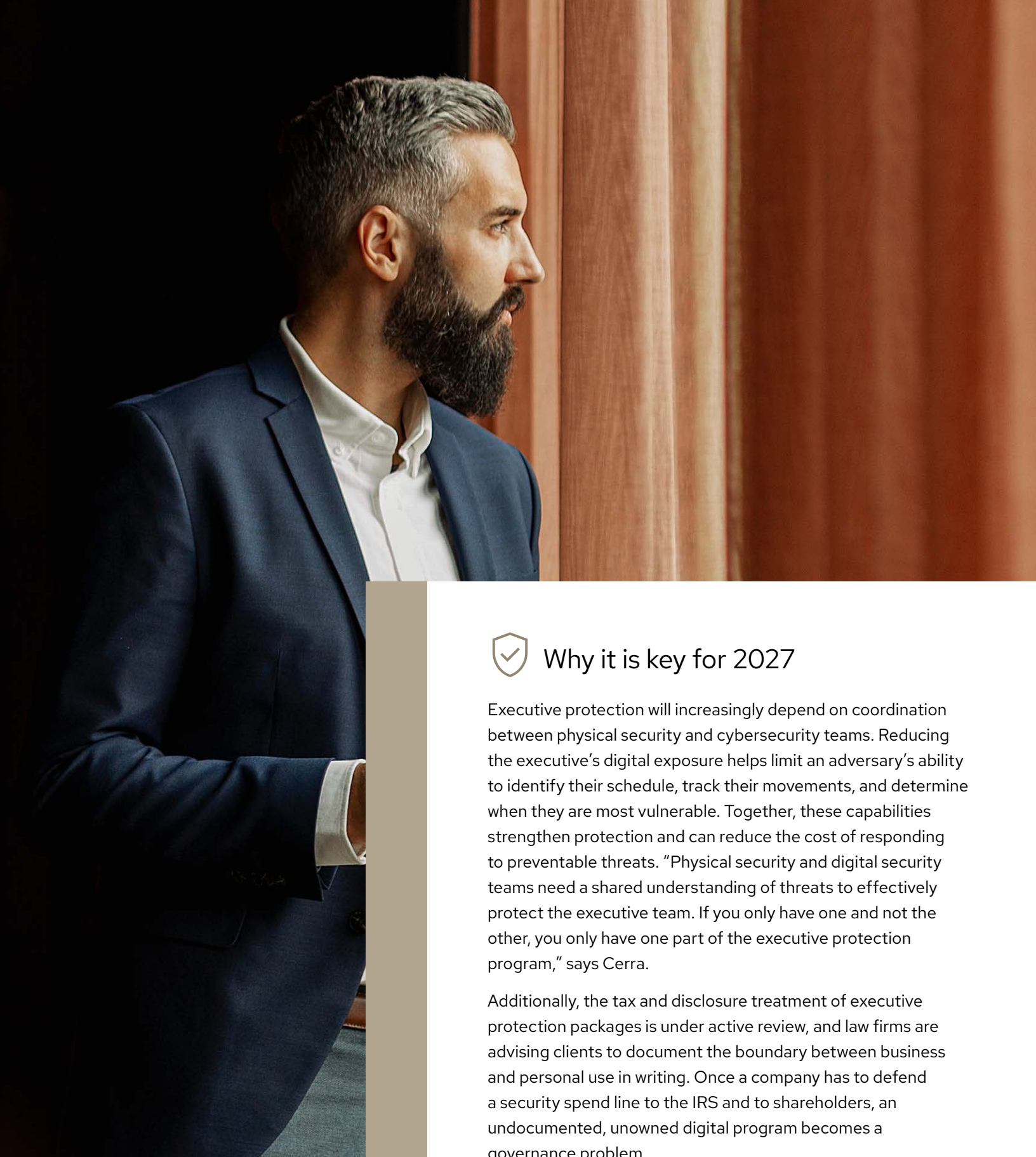


Signals behind the prediction

Throughout the last 12 months we have witnessed a steady uptick in the number of executive protection teams taking ownership of the digital side of their work. “Physical attacks often start with the digital footprint. That online reconnaissance is the first thing a bad guy is going to do anywhere in the world, and it starts with a Google search,” notes Hazel Cerra, Director of Digital Security Convergence, BlackCloak. “For Executive Protection teams, arrival and departures demand heightened attention. Any digital information that reveals an executive’s location or timing can turn those moments into opportunities for an attacker.”

External signals that influenced this prediction

- More than 1/3 of S&P 500 companies provided executive security prerequisites in 2025¹⁴.
- Reported incidents targeting corporate executives doubled year over year 2024-25, many of which were physical¹⁵.
- Supreme Court Justices Elena Kagan and Amy Coney Barrett testified to Congress in July 2026 in support of a budget request covering both physical security and cybersecurity. Barrett described a swatting incident at her home, which requires an attacker to know a home address¹⁶.
- Google Cloud has described attackers collecting executives’ routines, movements, family relationships, and travel schedules, and recommends integrating digital intelligence into physical security strategy¹⁷.



Why it is key for 2027

Executive protection will increasingly depend on coordination between physical security and cybersecurity teams. Reducing the executive's digital exposure helps limit an adversary's ability to identify their schedule, track their movements, and determine when they are most vulnerable. Together, these capabilities strengthen protection and can reduce the cost of responding to preventable threats. "Physical security and digital security teams need a shared understanding of threats to effectively protect the executive team. If you only have one and not the other, you only have one part of the executive protection program," says Cerra.

Additionally, the tax and disclosure treatment of executive protection packages is under active review, and law firms are advising clients to document the boundary between business and personal use in writing. Once a company has to defend a security spend line to the IRS and to shareholders, an undocumented, unowned digital program becomes a governance problem.

05

The category matures,
and so does executive
risk reporting



The prediction

As Digital Executive Protection becomes a line in the security budget, organizations will expect it to be reported like any other security investment. The measure that is emerging is a risk score for each executive, tracked over time and reported to the board. "We're seeing a lot of clients ask for the KPIs and metrics around their personal risk measurements," says Ingrid Gliottone, Chief Experience Officer, BlackCloak. "Success will no longer be measured just on how many sites you removed details from. The measure of risk needs to broaden and take into account how well that information is kept off those sites over time, an executive's device and home network posture, credential exposure, and impersonation risk."

Signals behind the prediction

Data broker removal is where most organizations enter this category and many mistakenly feel DBR activity is sufficient. The number of sites an executive has been removed from is a poor proxy for risk because information reappears as new records are purchased and new breaches occur. It also doesn't take into account any other risk vector, delivering a false sense of security.

As a vendor, our obligation is not only to reduce our Clients' digital exposure, but to prove its value. We have seen the category mature over the years and work with security teams to provide the key indicators they need to monitor and report on success. Increasingly, the request is to present executive risk in a similar way to corporate risk, via a single score.

External signals that influenced this prediction

- Gartner frames the response to executive targeting as an organizational security strategy rather than an executive perk, which is the framing that invites reporting in parity to corporate risk¹⁸.
- Executive security spending is now disclosed in proxy filings and rising year over year¹⁴. Once a cost is visible to the board in that way, we expect it to be held to the same standard of justification as any other line, which is where a per-executive risk score becomes an expectation.



Why it is key for 2027

A budget line that cannot be adequately reported on is a problem for any security leader. Giving a defensible number, tracked per executive and over time, is what moves DEP from a service the company buys to support their executives, to a program the company runs as part of an overall risk mitigation strategy.

Digital Executive Protection: A Year In Review

Our 2027 Digital Executive Protection predictions are based on observation and industry research. This section discusses the key market movements in full. Broken down into the four core areas of Digital Executive Protection, we cover what our own research found, what governments, regulators, and independent researchers reported during the year, and what it means for your organization.

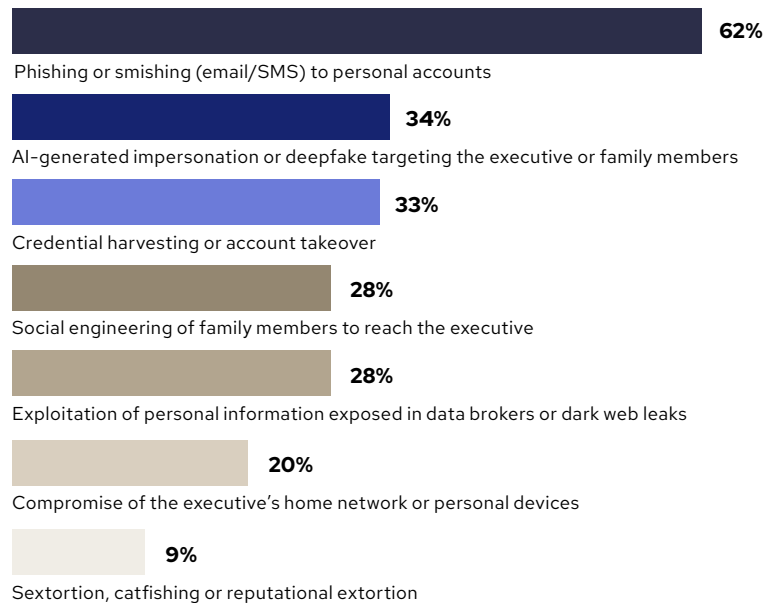


Privacy & Identity Defense

Exposed personal information continues to enable targeting

In 2026, a third of security teams (33%) named credential harvesting or takeover of personal accounts among their three most common threat vectors, and just over a quarter (28%) named the exploitation of personal information exposed through data brokers or dark web leaks¹.

What are the most common threat vectors your team has encountered in incidents targeting senior leaders or their families outside the corporate environment? (Select up to 3)



Source: Techstrong PulseMeter, Personal Exposure, Enterprise Risk: Formalizing Response for Executive Soft Targets





This sentiment is not without a solid foundation. The Identity Theft Resource Center recorded 3,322 publicly reported U.S. data compromises in 2025, 5% more than in 2024. This is the highest annual total it has tracked and we anticipate a continuing trend when the 2026 report is released. Although the number of victim notices fell in 2025 to around 279 million, which the ITRC attributes to fewer very large breaches¹⁹, it rose again in the first half of 2026 to more than 471 million, already exceeding the 2025 total²⁰.

Regulators were active this year too. California's deletion platform went live in January, and by August more than 500,000 residents had registered and brokers had reported deleting tens of millions of records²¹. California's regulator fined data brokers that failed to register²², and in September it warned that incorrect information in the state's data broker registry would also attract daily fines²³. Elsewhere, Connecticut enacted a data broker registry and a future centralized deletion mechanism in May²⁴, Vermont strengthened its existing data broker law, and New Jersey new legislation²⁵.

For security teams, the practical point is that constant removal and monitoring of personal exposed data is needed. Standard data detection and removal reduces what can be found through people-search sites at any point in time, while continual monitoring and removal is needed for personally identifiable information (PII) that is exposed through new breaches and PII that resurfaces on data broker sites after the initial take-down. It is also important to note that not all data can be removed from data broker sites. In such instances, suppression techniques are required to hide it from online search results.



AI Threat Protection

AI-enabled impersonation is increasing and remains difficult to detect

Public data released this year shows impersonation-based fraud growing more broadly. The FBI received 1,008,597 complaints in 2025, up from 859,532 in 2024, with reported losses rising 26% to \$20.9 billion. For the first time it reported AI-related complaints as a separate category⁴, highlighting the growing severity and scale of the threat.

The Federal Trade Commission reported that losses to impostor scams rose from \$2.95 billion in 2024 to \$3.5 billion in 2025²⁶, and we expect this to rise. Although these figures do not isolate the role of AI in the attack, they do show impersonation continuing to grow each year.

Looking ahead, Deloitte's Center for Financial Services projects that generative AI could enable U.S. fraud losses of up to \$40 billion by 2027²⁷.

When we asked security professionals what would help, 53% said technology that enables executives to confirm the authenticity of the messages they receive is highly important⁶.



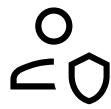
Executive Threat Intelligence

Targeting of executives and their families is increasing

Public data released in 2026 shows targeting of senior figures rising year over year. The Security Executive Council, working with Mercyhurst University, found that open-source reported incidents targeting corporate executives in 2025 had doubled the 2024 total by the end of October, the highest level it has recorded. Physical incidents made up 85% of the total reported, and cyber incidents 14%¹⁵. The U.S. Capitol Police investigated 14,938 threat assessment cases involving Members of Congress, their families, and staff in 2025, a 58% increase on the 9,474 cases it investigated in 2024²⁸.

Although these statistics depict a trend prior to 2026, it is anticipated we will see the number of cases growing. France provided one of the clearest year-over-year comparisons that influences this opinion. In June 2026, the French Interior Minister reported 77 cases of unlawful detention, extortion, kidnapping, or attempted crimes linked to the cryptocurrency sector in the first half of the year, compared with 45 in the whole of 2025. Around 200 people had been arrested, and the ministry announced a new plan built around intelligence sharing, closer cooperation with the industry, and operational coordination with other countries²⁹.



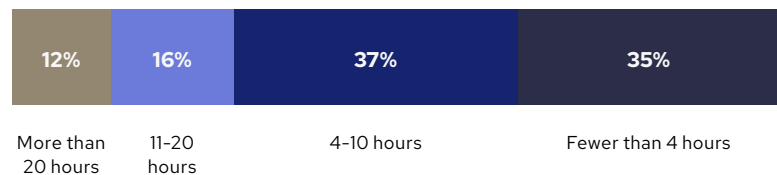


Personal Security Operations

Home networks drew attention from U.S. authorities during 2026. In March, the FBI issued an alert on AVrecon malware, found on routers and other connected devices in around 163 countries, which criminals used to sell access to compromised devices as residential proxies³⁰. In April, the Department of Justice and the FBI announced a court-authorized operation to neutralize the U.S. portion of a network of home and small-office routers compromised by a unit of Russia's military intelligence directorate, known as APT28, and used for DNS hijacking³¹.

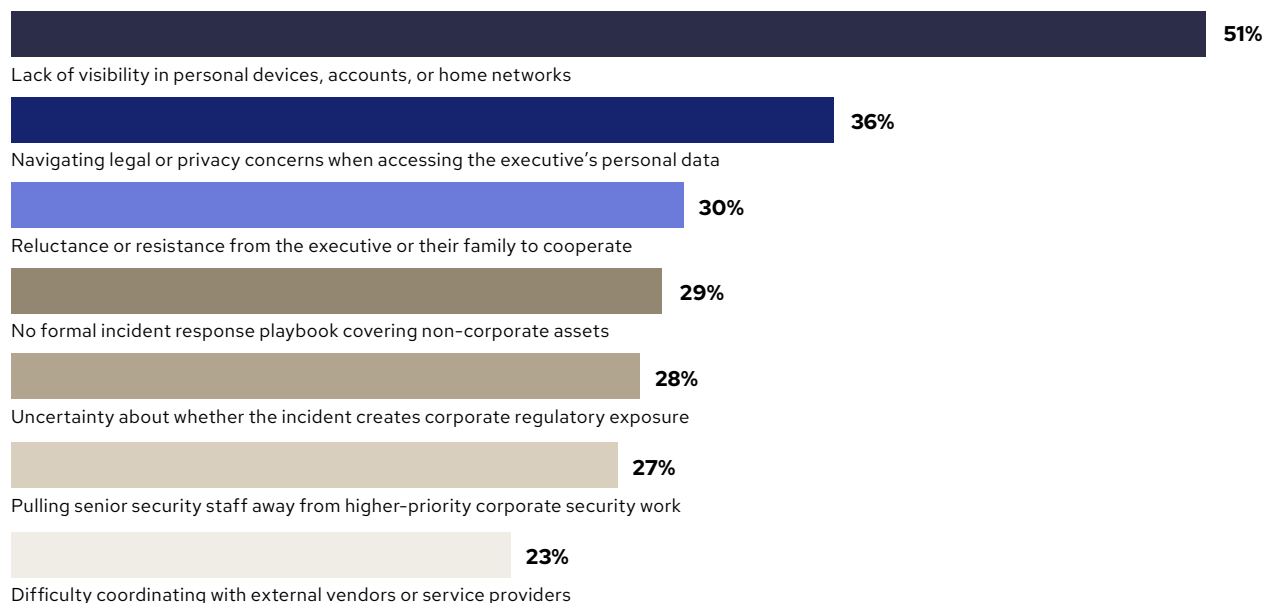
Our June 2026 survey shows the amount of personal incident response work security teams are now having to undertake. Three in four security teams (75%) were involved in at least one incident in the past 12 months that originated from a senior leader's or family member's personal device, home network, or personal account, and 43% experienced more than one¹. Each incident took an average of 8.7 total staff hours to remediate, and 12% of respondents reported more than 20 hours¹.

On average, how many total staff hours does your team spend investigating and remediating any one incident that originates from a senior leader's personal digital life? Including any downstream corporate impact in your estimate. (Select one)



Source: Techstrong PulseMeter, Personal Exposure, Enterprise Risk: Formalizing Response for Executive Soft Targets

Which of the following challenges has your team experienced when responding to a security incident involving a senior leader's personal digital life? (Select all that apply)



Source: Techstrong PulseMeter, Personal Exposure, Enterprise Risk: Formalizing Response for Executive Soft Targets



Teams also described the difficulties of protecting executives in their personal lives. The most commonly cited challenges were a lack of visibility into personal devices, accounts, or home networks (51%), legal or privacy concerns (36%), and reluctance or resistance from the executive or their family (30%). Just under half (46%) have documented procedures for incidents involving non-corporate assets, while 36% rely on informal processes and 18% have none¹.

There continues to be clear interest in vendor support to protect executives' personal devices, home networks, and provide incident response. 85% of respondents in our survey reported an external service handling these incidents would be helpful and 61% expected it to reduce their operational burden moderately or significantly.

Our 2026 Predictions, One Year On

With so many market influences shaping Digital Executive Protection over the year, and the unpredictable hand of threat actors adding to the mix, we wanted to review our 2026 predictions to see how they fared.

Each prediction has been reviewed for accuracy and rated as follows:

SUPPORTED

The available evidence is consistent with the forecasted prediction.

LARGELY SUPPORTED

The prediction is supported, but one or more elements are not yet evidenced.

PARTLY SUPPORTED

Some elements of the prediction are evidenced and others are not.

NOT YET EVIDENCED

We have not found sufficient evidence either way to prove the prediction.



2026 Prediction 1

"In 2026 and beyond, we'll see an accelerated rise in organizations implementing Digital Executive Protection within their corporate cybersecurity initiatives, driven by the need to bridge the gaps between cyber and physical security and personal and professional protection, and to integrate executive risk into enterprise-wide risk management strategies."

LARGELY SUPPORTED

An Equilar report released in 2026 found that more than a third of S&P 500 companies provided security perquisites to at least some executives in 2025, 12.8% more than in 2024, and that the median value among those companies rose 20% to \$130,468. Equilar also observed that boards and management teams have taken a closer look at the personal security risks facing senior leaders¹⁴. Its definition of security perquisites includes cybersecurity protections alongside residential security and personal security staff, but the disclosures do not separate the two, so they cannot tell us how much of this growth relates to Digital Executive Protection specifically. What we can disclose is that BlackCloak has not only witnessed new highs with regards to client onboarding numbers, but also a sharp increase in awareness and interest in the category, from security leaders, industry analysts, and vendors alike.

The Security Executive Council reports growing convergence between digital threats and physical approaches to executives¹⁵. The extent to which an executive's personal life is exposed online has a direct bearing on how easy a physical attack can be planned and executed. Reducing personal online exposure addresses physical risk at an earlier stage than on-site protection can, but increasingly digital and physical executive protection are forming part of the same strategy.



2026 Prediction 2

"The relationship between privacy and security will move from passive corporate compliance to mandated personal defense. Executives will increasingly be required to take ownership of their personal security, including aggressively minimizing their digital footprints, recognizing that individual self-protection is now the essential baseline and prerequisite for secure corporate access."

PARTLY SUPPORTED

The shift toward individuals managing their own privacy is visible. California's Delete Request and Opt-out Platform opened on January 1, 2026 and lets residents send a single deletion request to more than 500 registered data brokers. By August, more than 500,000 Californians had registered, and brokers had reported deleting tens of millions of records²¹.

We found no evidence of organizations making personal digital hygiene a condition of corporate access or treating it as a fiduciary matter. Our 2026 survey does show that cooperation to improve personal cybersecurity practices between executives and security leaders is improving, with only 30% citing reluctance or resistance from an executive or family member. While this number is higher than any security professional would like, it's clear attitudes are changing as it relates to personal cyber hygiene¹.



2026 Prediction 3

"The continued advancement and democratization of AI is fueling a hyper-personalized threat landscape, with bad actors leveraging generative AI to create realistic phishing campaigns, social engineering attacks, and deepfake impersonations that are increasingly difficult to detect. This arms race is forcing cybersecurity into an AI vs. AI battlefield, driving the scale-up of specialized defensive systems with self-healing capabilities that can predict risk, seal vulnerabilities, and speed up detection."

"Consequently, global legislative frameworks like the EU AI Act will compel organizations to treat AI security and governance as a core legal imperative, embedding compliance monitoring and liability tracking into their risk strategies, while simultaneously increasing demand for vendors committed to responsible, trustworthy AI use."

LARGELY SUPPORTED

The threat side of this prediction is well evidenced. In our 2026 survey, 34% of security teams named AI-generated impersonation or deepfakes among the three most common threat vectors targeting senior leaders and their families, second only to phishing and smishing¹. In addition, the FBI's report on 2025, published in April 2026, recorded 22,364 AI-related complaints and nearly \$893 million in reported losses in its first dedicated section on artificial intelligence⁴.

The regulatory element is also in place, as most provisions of the EU AI Act, including the Article 50 transparency obligations that cover deepfakes, apply from August 2, 2026, with fines of up to €15 million or 3% of worldwide annual turnover³².



2026 Prediction 4

"The data privacy landscape is undergoing a significant legal transformation as Data Broker Removal (DBR) becomes mandated law on a state-by-state basis across the U.S."

"Therefore, while compliance with DBR laws is essential, it only addresses future data collection. As a result, in the coming year, individuals will embrace a multi-layered, continuous defense strategy that goes beyond basic removal."

LARGELY SUPPORTED

The legal shift described in this prediction took place during 2026. As previously mentioned, new state laws introduced throughout the year and California's free, state-run program may be an early sign of DBR commoditization, but their combined effect on the commercial market has not yet been measured.

The prediction was also correct in that removal alone is not enough. Removal laws apply to registered data brokers and do not reach data already exposed in breaches, and that pool continues to grow. The Identity Theft Resource Center counted more than 471 million breach victim notices in the first half of 2026, already more than in the whole of 2025²⁰, and just over a quarter of security teams (28%) named the exploitation of personal information exposed through data brokers or dark web leaks among their three most common threat vectors¹.



2026 Prediction 5

“As ultra/high-net-worth individuals implement stronger personal defenses, targeted attacks will shift from the principal to the family ecosystem, with children, spouses, assistants, and even contractors as new vectors for breaches.”

SUPPORTED

Our research supports the central risk in this prediction. In 2026, 28% of security teams named social engineering of family members, as a route to the executive, among the most common threat vectors¹, and in 2025, over half of organizations surveyed believed it highly likely that an executive’s partner or child would click on a link in a targeted phishing email⁵. The Security Executive Council now includes family members and staff targeted as an extension of the executive within its executive targeting data¹⁵.

About the research,
about BlackCloak
& Sources

Sources

Studies commissioned by BlackCloak are marked as sponsored.

All other sources are independent.

1. Techstrong PulseMeter, Personal Exposure, Enterprise Risk: Formalizing Response for Executive Soft Targets, Futurum Group, June 2026. Sponsored by BlackCloak.
2. Google Threat Intelligence Group, From Prompting to Autonomy: The Evolution of Adversarial AI, September 2026.
3. Madison Horn, "Rethinking critical infrastructure security for the age of AI," Federal News Network, July 2026.
4. FBI, "Cryptocurrency and AI Scams Bilk Americans of Billions," 9 April 2026.
5. Ponemon Institute, Digital Executive Protection Research Report 2025, including comparisons with the 2023 study. Sponsored by BlackCloak.
6. Ponemon Institute, Faked to Perfection: The rise of deepfake threats against corporate executives, April 2025. Sponsored by BlackCloak.
7. NIST, Digital Identity Guidelines, SP 800-63-4.
8. Gen Digital, Phantom Deal campaign research.
9. CISA, FBI, and international partners, joint advisory AA23-320A, updated 29 July 2025.
10. Coalition, "Coalition Adds Deepfake Response Endorsement to its Cyber Insurance Policies Globally."
11. Insurance Business, "BOXX Insurance adds affirmative AI and deepfake coverage to Cyberboxx Business policy," July 2026.
12. FBI Internet Crime Complaint Center, public service announcement on GRU exploitation of routers, April 2026.
13. NSA and partners, guidance on router hygiene against Russian cyber threats, July 2026.
14. Equilar, "Early Look: Executive Security Perks on the Rise," April 2026, covering S&P 500 proxy filings through 7 April 2026.
15. Security Executive Council, Executive Targeting Report: Analysis of Attacks on Corporate Executives from 2003-2025, February 2026.
16. CNBC and NBC News on the testimony of Justices Kagan and Barrett, 14 July 2026.
17. Google Cloud, "Personal cyberattacks against executives are rising. Here's how to stop them."
18. Gartner, Navigate Executive Protection Solutions for Digital Threat Defense, Elizabeth Kim and Mitchell Schneider, 3 November 2025.
19. Identity Theft Resource Center, 2025 Annual Data Breach Report, 29 January 2026.

20. Identity Theft Resource Center, first-half 2026 data compromise release, 22 July 2026.
21. California Privacy Protection Agency, "Half a Million Californians Have Signed up for DROP to Delete their Personal Information from Data Brokers," August 2026.
22. California Privacy Protection Agency, "CalPrivacy Brings New Round of Enforcement Actions Against Data Brokers," 8 January 2026.
23. California Privacy Protection Agency, "Enforcement Advisory Targets Incorrect Information in Data Broker Registration," Enforcement Advisory 2026-01, September 2026.
24. Davis+Gilbert LLP, "Connecticut's Newly Enacted Data Broker Law: How It Stacks Up Against California's Delete Act," June 2026.
25. Davis+Gilbert LLP, "Vermont and New Jersey Data Broker Laws Add to Expanding State Privacy Patchwork," July 2026.
26. Federal Trade Commission, "FTC Data Show People Reported Losing \$3.5 Billion to Imposter Scams in 2025," June 2026.
27. Deloitte Center for Financial Services, "Generative AI is expected to magnify the risk of deepfakes and other fraud in banking."
28. U.S. Capitol Police, threat assessment case releases for 2025, 2024, and 2023.
29. Laurent Nuñez, French Interior Minister, remarks to the Association pour le développement des actifs numériques, 30 June 2026, as reported by Le Parisien and BFM Business. Figures are the Interior Ministry's own count and cover unlawful detention, kidnapping, extortion, and attempted offenses.
30. FBI FLASH 20260312-001, "AVrecon Malware-Infected Routers Exploited as Residential Proxies by SocksEscort," 12 March 2026.
31. U.S. Department of Justice, "Justice Department Conducts Court-Authorized Disruption of DNS Hijacking Network Controlled by a Russian Military Intelligence Unit," 7 April 2026.
32. Regulation (EU) 2024/1689 (Artificial Intelligence Act), Articles 50, 99, and 113.



About the research

This report draws on four studies commissioned by BlackCloak. The Ponemon Institute's Digital Executive Protection Research Report, a survey of 586 U.S. security professionals, and its Faked to Perfection study which surveyed U.S. IT and security practitioners on deepfake risk. Techstrong Group's PulseMeter studies, Prioritizing Executive Security to Manage Risk and Personal Exposure, Enterprise Risk from June 2026, surveyed security and risk professionals. All other sources are independent and are listed above.

About BlackCloak

BlackCloak secures the personal digital lives of corporate executives, board members, high-net-worth individuals, and their families from cybersecurity, privacy, financial, and other reputational risks. Used by Fortune 500 companies across all industries, the BlackCloak Digital Executive Protection Platform is a full-category solution that delivers four pillars of protection: Privacy & Identity Defense, AI Threat Protection, Executive Threat Intelligence, and Personal Security Operations, supported by a US-based SOC that includes expert-led incident response.

Get in touch for more information

info@blackcloak.io | www.blackcloak.io

BLACKCLOAK®

© 2026. BlackCloak, Inc. All Rights Reserved.

