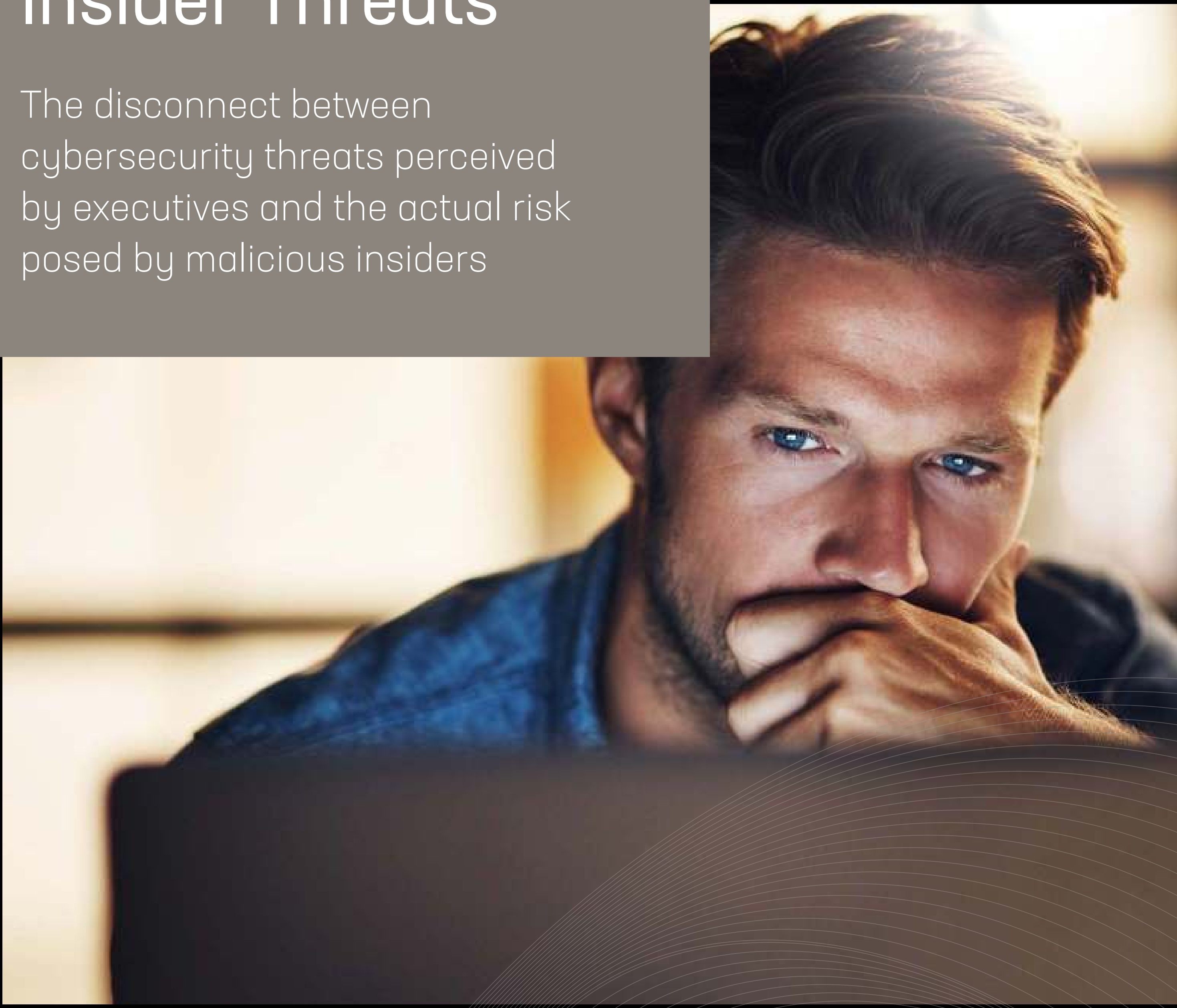
Constella

SURVEY REPORT

Insider Threats

The disconnect between cybersecurity threats perceived by executives and the actual risk posed by malicious insiders



2022 | Survey Report

Executive Summary

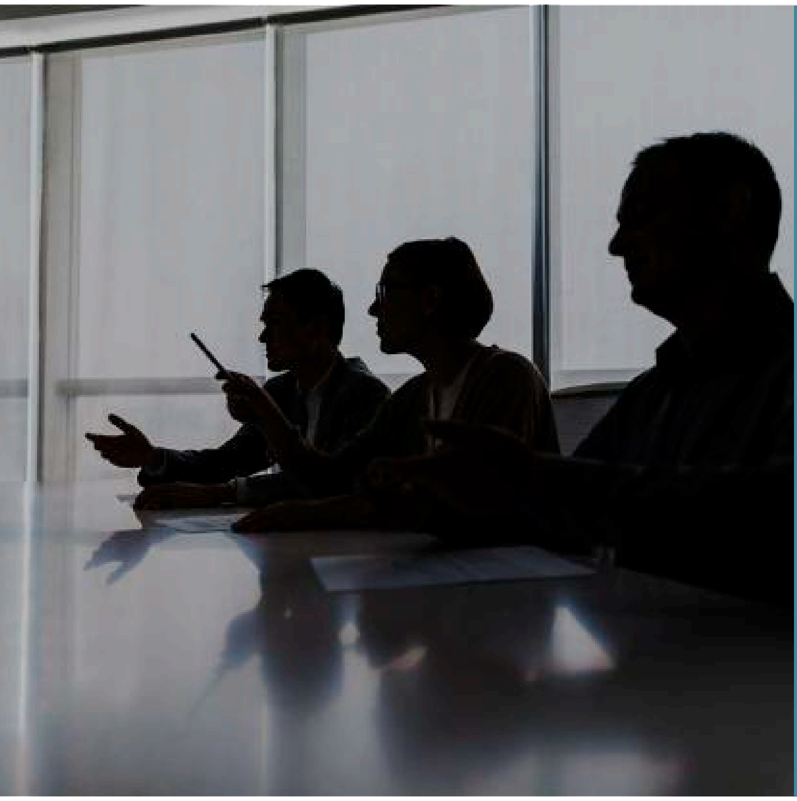
The pandemic has offered a new opportunity for bad actors to wreak havoc on corporate security protocols. Targeted cyber threats have steadily increased in the last 18 months and are expected to increase throughout the remainder of 2022. Although phishing is the number one initial attack vector for cybercriminals, executives surveyed were most concerned about the impact of insider threats on their organization.

Constella Intelligence and Pulse surveyed 100 global cybersecurity leaders within enterprise organizations to find out what types of threats their organizations have been exposed to, how they are combating them and what they intend to do to safeguard their organization from cyberthreats in the future.

The key findings and insights communicated in this survey report serve as an informative and educational overview of the behaviors and experiences of cybersecurity leaders across industries and geographies. Additionally, this report offers insight into how they are dealing with an increase in cyberattacks, partially driven by remote work as a result of the pandemic, and how leaders are responding to this challenge.

KEY TAKEAWAY

Global executives in major industries – including financial services, software, and healthcare – across North America and EMEA – ranked malicious insiders as the greatest threat vector of concern (34%), even though they are rarely the cause of the most damaging cyberattacks. According to the survey, while malicious insiders actually accounted for only 7% of the most damaging attacks in 2021, more than one in three executives ranked them as the #1 attack vector of concern, followed by phishing and software vulnerabilities.



> “The human element continues to drive breaches. This year 82% of breaches involved the human element. Whether it is the use of stolen credentials, phishing, misuse, or simply an error, people continue to play a very large role in incidents and breaches alike.”
>
> **2022 Verizon Data Breach Investigations Report**

KEY FINDINGS

1

Malicious insiders ranked as the #1 attack vector of concern for the C-suite and executives despite rarely being the initial threat vector used in the most damaging cyberattacks. Nearly one in five respondents admitted that they don't monitor their organization for insider threats.

2

Phishing is the #1 attack vector, accounting for 32% of all breaches used in the most damaging cyberattacks. Malicious Insider ranked lowest (7%) even though it's the #1 concern amongst the C-Suite.

3

35% of executives surveyed say their organization does not monitor social media for threats against their brand reputation. A brand's most vital resource is its reputation, and monitoring social media and open-sources for continuous intelligence helps you protect it. Media monitoring enables you to stay on top of threats to your brand's reputation. Keeping track of brand mentions—what is said and by whom—enables your organization to proactively fend off emerging threats as they develop.

4

More than 33% of cybersecurity leaders surveyed say their organization does not monitor their employees or executives for breached credentials. Notably, compromised or stolen credentials is the most common initial attack vector used by threat actors to penetrate an organization's network in 2022, as reported by IBM Security. Continuous monitoring of employees' corporate credentials with real-time alerts when a breach occurs gives organizations a critical window to initiate takedown before it evolves into an active cyberattack.

5

80% of executives surveyed have noted an increase in corporate governance and/or regulatory requirements to implement more rigorous cybersecurity practices in light of recent newsworthy ransomware attacks.

WHY IT MATTERS

Prioritizing technical and financial resources to address perceived concerns over more likely cyberthreats may leave organizations vulnerable to damaging attacks.

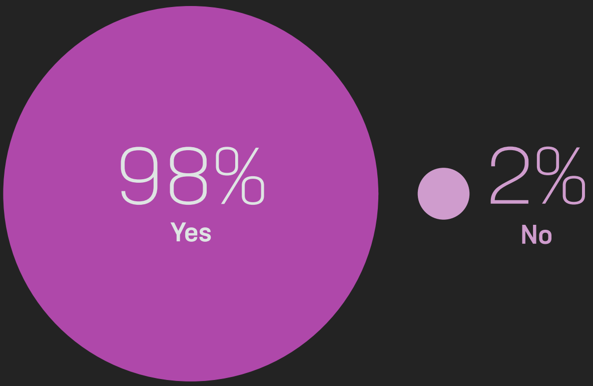
Insider threats, either unwitting or malicious actor is an area of growing concern and one of the most challenging to resolve in any cyber defense strategy.

Phishing attacks and stolen or compromised credentials cause the most damage to organizations, even among those who are prepared.

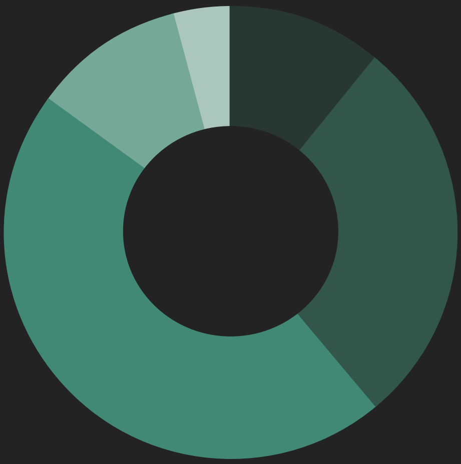
Many companies lack the teams and tools to monitor for stolen or breached credentials, insider threats, or threats to brand reputation on social media. These organizations will need to expand internal resources or retain outside support.

SURVEY RESULTS

Did your organization transition to remote work in the past 18 months?



Has your organization experienced increased targeted cyber threats (e.g. phishing, ransomware) in last 18 months, likely due to remote work?

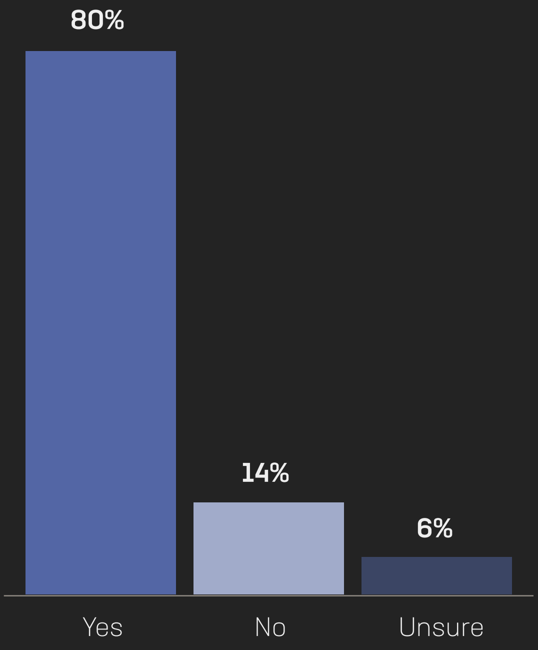


- ● 11% Significantly
- ● 28% Moderately
- ● 46% Slightly
- ● 11% Not at All
- ● 4% Unsure

85%

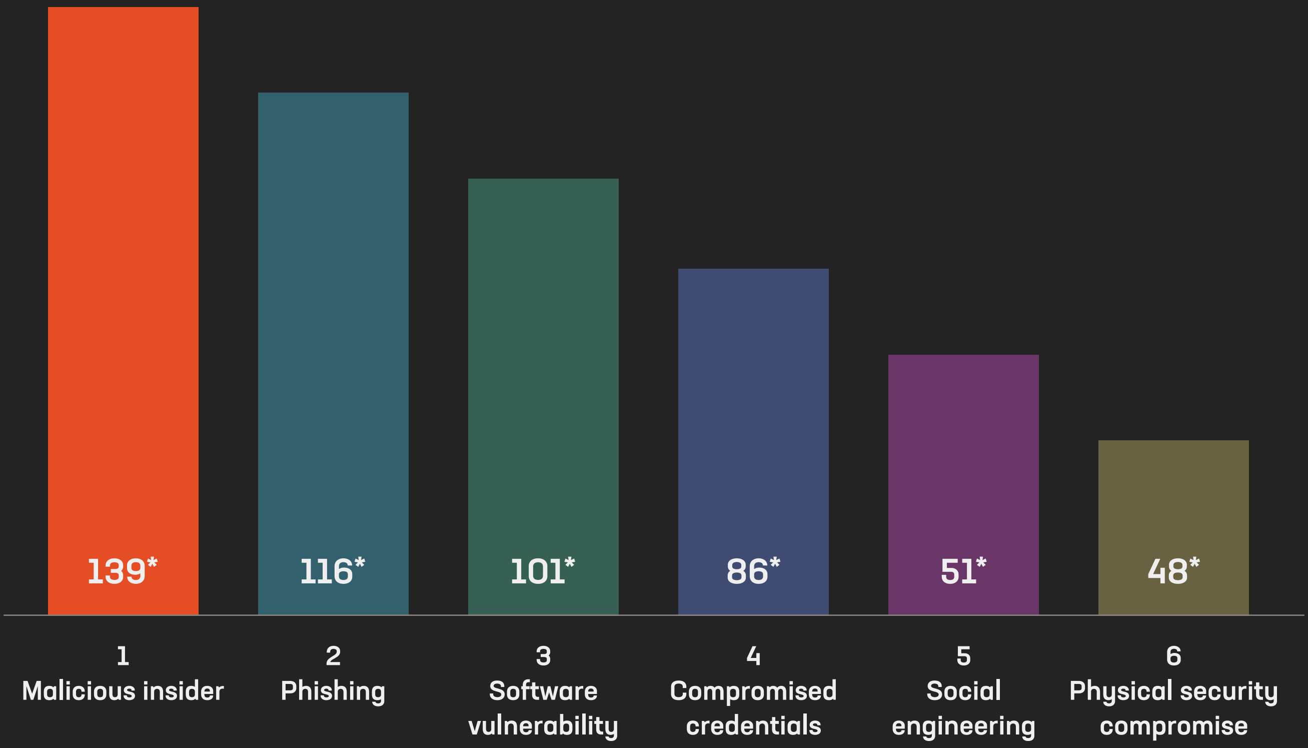
of respondents' organizations have experienced some increase in targeted threats corresponding with increased remote work.

In light of recent newsworthy ransomware attacks, has there been an increase in corporate governance and/or regulatory requirements to implement more rigorous cybersecurity practices?



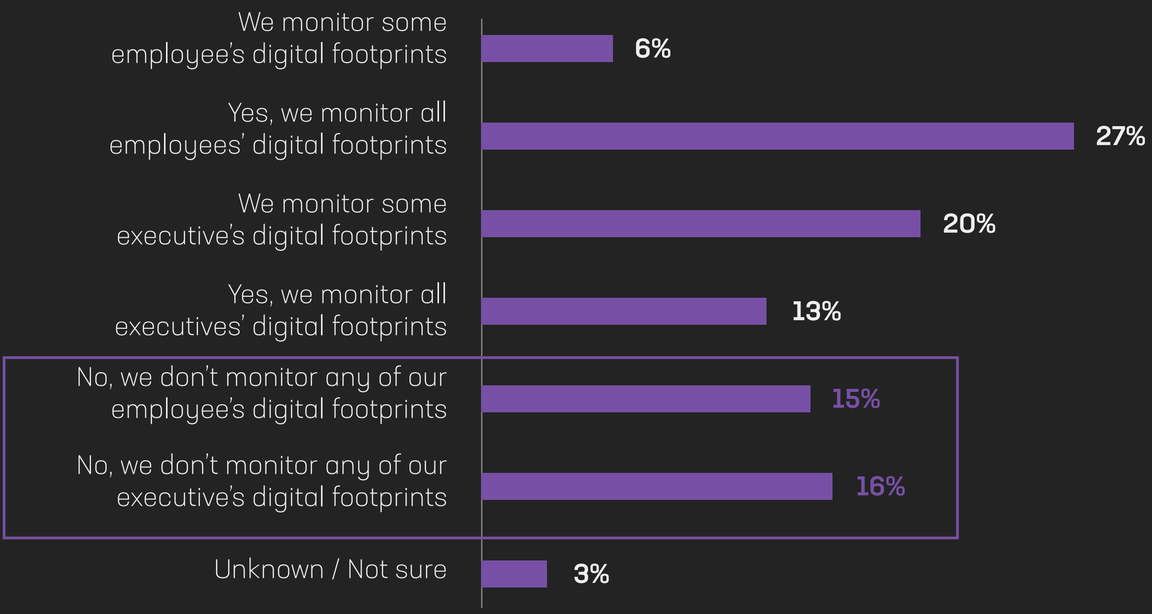
Constella

What 3 initial attack vectors are you most concerned about? (Choose 3 in rank order, with highest concern first).

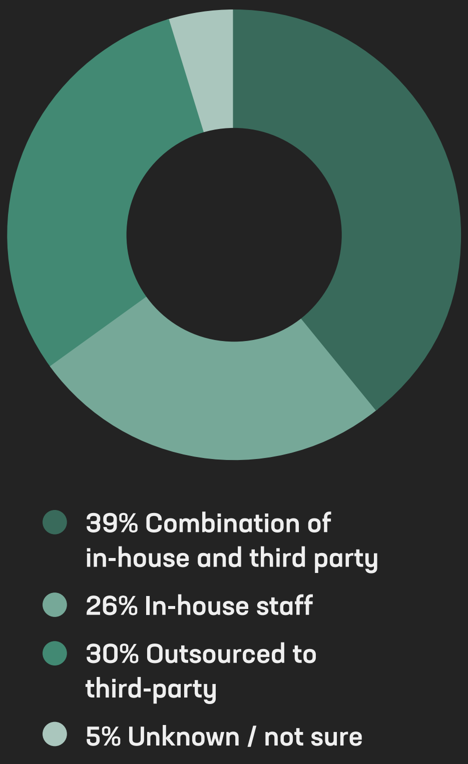


*Respondent Ranking Score

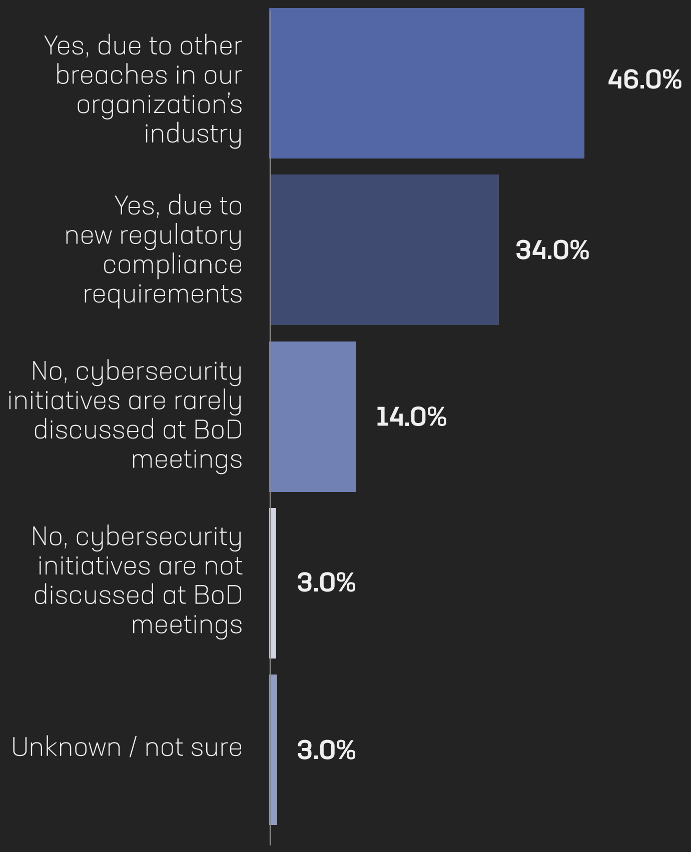
Do you currently monitor your employees' and/or executives' external digital footprints for digital threats (such as compromised credentials, personal information in the deep or dark web, or social media) that could be weaponized in a cyberattack?



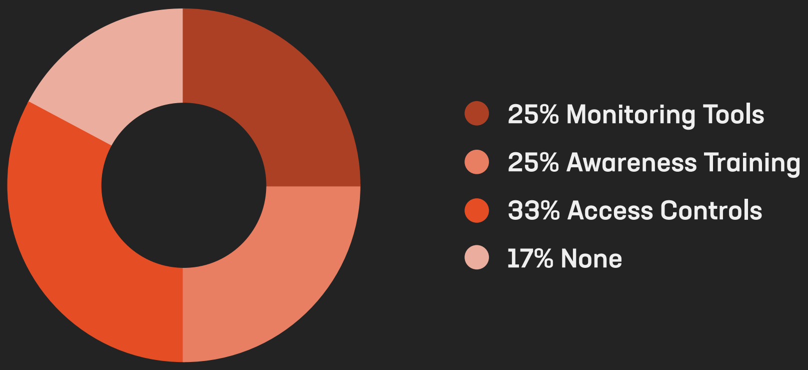
How do you monitor your executives' and/or employees' external digital footprints?



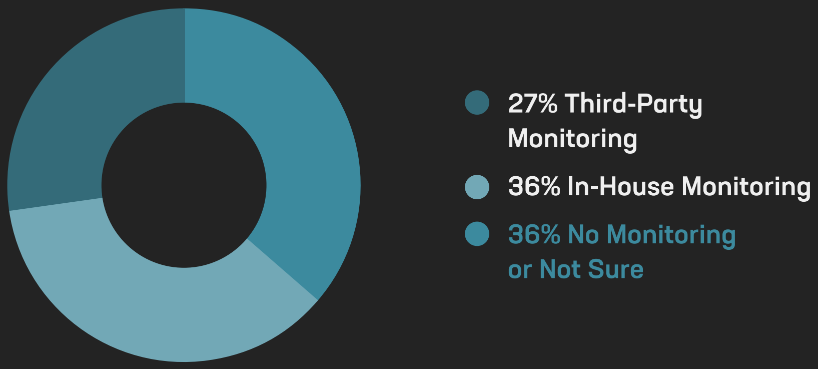
Has your board of directors gotten more engaged with cybersecurity in the last 12 months?



What measures has your organization implemented to monitor and protect your company from "insider threats" due to either employee errors or intent to do harm?



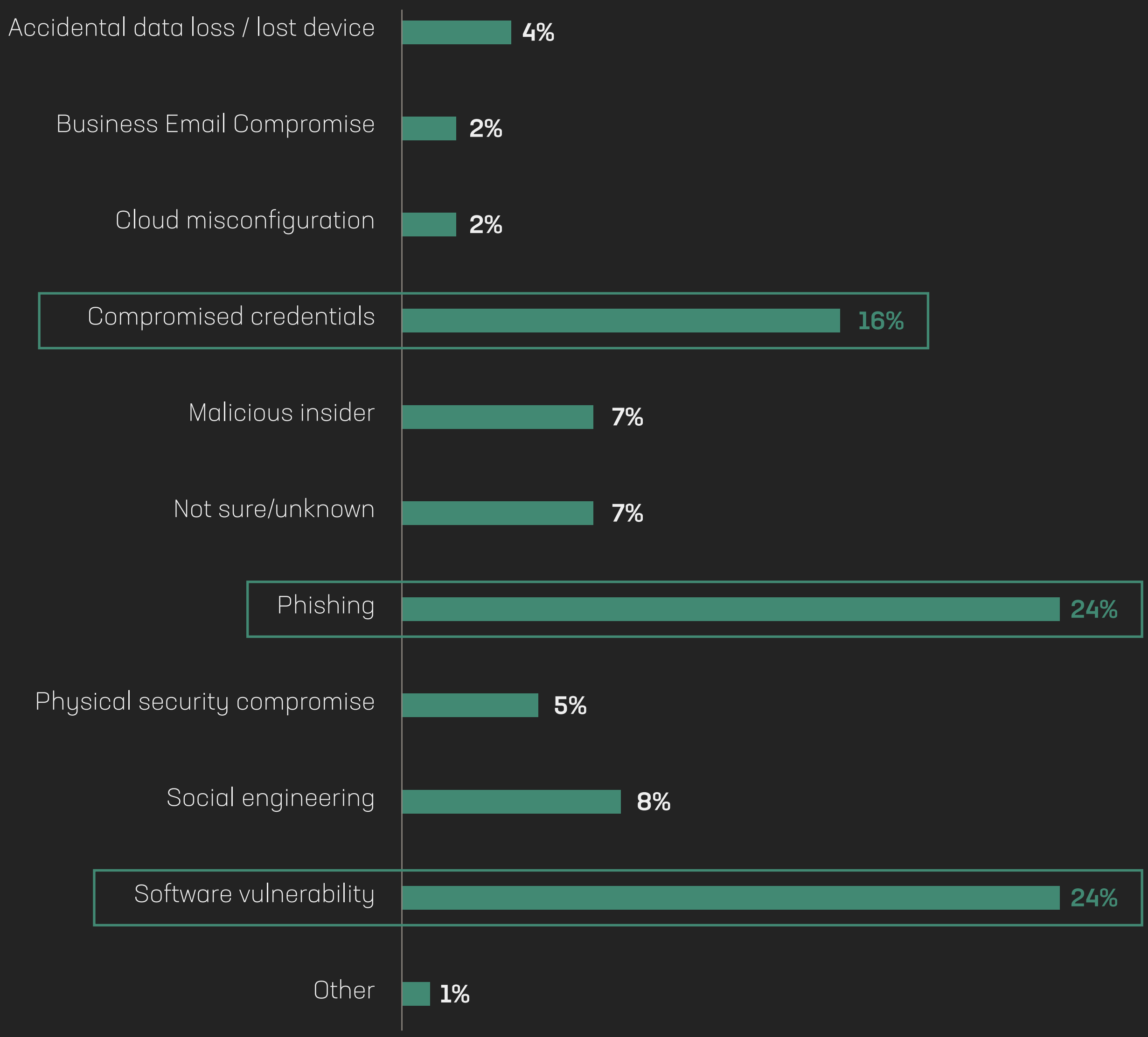
How does your organization monitor social media for threats against your brand or brand reputation?



C-suite executives reported that the 3 initial attack vectors of most concern were:

1. Malicious Insider
2. Phishing
3. Software Vulnerability

In looking back at the most damaging cyberattack your organization has experienced, what was the initial attack vector?



Constella

Conclusion

In today's threat landscape, monitoring social media and the deep and dark web for threats to your brand, executives, and employees is critical. Across all major sectors, accelerating digital transformation combined with remote workforces and increasingly distributed supply chains and operations means that attack surfaces are continuously expanding. Now more than ever, organizations need the tools to anticipate and mitigate risk through proactive real-time employee, brand, and reputational intelligence by continuous monitoring of social media, and the deep and dark web.

Insider threats (either unwitting or malicious actors) remain one of the most challenging vulnerabilities to resolve in any cybersecurity strategy. How else can organizations and leaders limit the risk associated with increased use of various devices, communications channels, collaboration platforms, user accounts, and networks? Stricter password protocol and VPN usage restrictions are of paramount importance to reducing this risk at the corporate level. However, individual awareness and best practices must be strengthened along with greater corporate governance to identify and act on potential insider threats before a breach occurs.

About Constella Intelligence

Constella Intelligence is a global leader in digital risk protection that works in partnership with some of the world's largest organizations to defeat digital risk by continuously monitoring social media and the surface, deep and dark web for exposed corporate credentials and hostile conversations to identify emerging threats and unmask malicious insiders. Our solutions are a unique combination of proprietary data, technology, and human expertise to anticipate, identify, and remediate targeted threats to your people, your brand, and your assets at scale—powered by the most extensive breach and social data collection from the surface, deep and dark web on the planet, with over 100B attributes and 45B curated identity records spanning 125 countries and 53 languages.

Our recent work has been featured in major mainstream media like the Wall Street Journal, World Economic Forum, Forbes and Krebsonsecurity.com in addition to other notable media.

To learn more about how you can proactively anticipate, identify, and remediate targeted threats to your people, your assets, and your brand try our Exposure Risk Tool to see if you or your company has been exposed - FREE.

Why Constella

OUR TEAM

We're a diverse multinational team committed to becoming the most trusted global partner for defeating digital risk. Constella integrates interdisciplinary intelligence community analysts, infosec pioneers, military veterans, and tech entrepreneurs with advanced analysis of surface, deep, and dark web to protect what matters most.

OUR INSIGHTS

Our diverse team of expert multidisciplinary cyber intelligence analysts delivers real-time, actionable insights to identify emerging threats to your organization, including insider threats and reduce risks emerging from social media, surface, deep and dark web.

OUR DIFFERENCE

Our unique technology, coupled with our world class analysts empowers advanced analysis across the entire risk surface protecting organizations, its executives and employees and their critical assets. Because, the best way to overcome future threats is by facing them today.