The CISOs Report

Sponsor Brief

GOLD SPONSOR

BEYOND IDENTITY

Stolen or otherwise compromised passwords have been the most common vector for ransomware attacks and other types of data breaches, for years now. Beyond Identity removes passwords and other phishable authentication methods from the security equation, while also ensuring user devices meet applicable security policies before gaining access.

"The access control that is fundamental to Zero Trust extends to a new reality – that identity is, in effect, becoming the new perimeter."

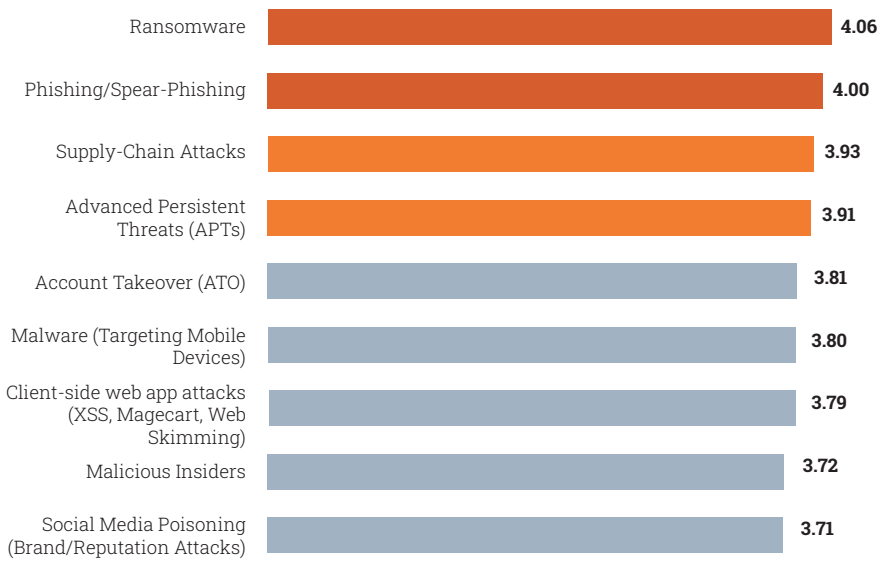
—The CISOs Report

The CISOs Report provides invaluable insights for the heads of modern cybersecurity teams – to benchmark their posture, experiences, and concerns against others; to learn from what their peers are doing and planning to do; and to validate their own plans and investments for moving forward. Selected by Beyond Identity, a Gold-level sponsor, the following critical issues highlight only a few of the key findings from this highly informative, CISO-centric research study.

WHAT LIES BENEATH

For anyone expecting that 2022 might provide a respite from ransomware, think again. The frequency of related attacks remains high, as does the level of concern for ransomware among CISOs. What do these and many other of the "most concerning" threats have in common? Passwords! Too often, weak or compromised credentials are a key enabler (e.g., with ransomware, supply chain and account takeover attacks, and advanced persistent threats), or the object of the attack in the first place (e.g., with phishing).

On a scale of 1 (lowest) to 5 (highest), please rate your concern for the following types of threats.



ZERO TRUST OR BUST

With the network perimeter no longer capable of serving as a well-defined trust boundary, many organizations are now pursuing a Zero Trust security model (see accompanying chart). This strategy – almost by definition – elevates the importance of identity, effectively making it the new perimeter. As a result, effective strong authentication (i.e., non-phishable MFA) is rapidly becoming a must-have capability for today's enterprises.

THE NEW STANDARD FOR MFA

Passwords are clearly one of the weakest links in today's security chains. Not much better, however, are MFA solutions that rely on passwords, phishable elements, or weak techniques for one of their factors. What's needed instead are MFA solutions that are truly "passwordless" – and, while we're at it, easy to deploy and frictionless to use. Hopefully the 23% of respondents indicating they have no plans to implement such a solution within the next 12 months catch on to this new standard for MFA, sooner rather than later.

ADDITIONAL FINDINGS

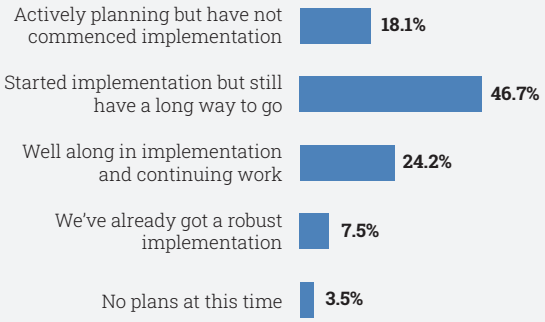
- 75% confirm their organizations were hit within the past 12 months by a cyber attack that caused material damage.
- APIs, cloud services, and data infrastructure top the list of IT components most in need of further security improvements and investment.
- The capabilities and characteristics most sought after when selecting a new cybersecurity solution are ease of deployment and ease of use, followed by high fidelity alerts and analysis.

To download a full copy of The CISOs Report, connect to: **www.beyondidentity.com/resources/cisos-report**

ABOUT BEYOND IDENTITY

Beyond Identity is fundamentally changing how the world logs in with a groundbreaking invisible, un-phishable MFA platform that provides the most secure and frictionless authentication on the planet. We stop ransomware and account takeover attacks in their tracks while dramatically improving the user experience.

Which best describes your organization's status with regard to implementing a Zero Trust security model.



Which technologies and solutions are currently in use or planned for upgrade/addition within the next 12 months?

	Already in good shape	Plan to upgrade	Plan to add	No plans
Network detection and response (NDR)	46.6%	28.4%	15.9%	9.1%
Third-party security and/or risk management (TPSRM, TPRM)	45.5%	28.4%	12.5%	13.6%
Extended detection and response (XDR)	38.6%	29.5%	20.5%	11.4%
Client-side web application protection	31.8%	18.2%	22.7%	26.1%
Passwordless multi-factor authentication (MFA)	30.7%	19.3%	27.3%	22.7%
Security orchestration, automation and response (SOAR)	27.3%	26.1%	28.4%	18.2%
Network/micro-segmentation	23.9%	37.5%	27.3%	11.4%
Container security	22.7%	30.7%	26.1%	20.5%

CISOs CONNECT

CISOs Connect is an invitation-only interactive community of trusted cyber peers, with more than 500 Chief Information Security Officers (CISOs) and subject matter experts. Connected by common interests, this membership-community allows cyber experts to share knowledge and expertise through proprietary content, original research, and analysis while exchanging information, ideas and collaborating with trusted colleagues to make informed professional, business and technology decisions. CISOs Connect is known for its succession training and mentorship.