2023 Cyberthreat Defense Report

Executive Brief

Platinum Sponsor

HUMAN

Survey Demographics

- Responses from 1,200 qualified IT security decision makers and practitioners
- All from organizations with more than 500 employees
- Representing 17 countries across North America, Europe, Asia Pacific, the Middle East, Latin America, and Africa
- Representing 19 industries

> *"Web and mobile attacks are a significant threat to ecommerce companies, financial institutions, and basically any organization that advertises or sells products on the web or through mobile apps… Some of these attacks can also be used to acquire credentials from just about any commercial or government organization."*
>
> *– 2023 CDR*

CyberEdge Group's tenth annual Cyberthreat Defense Report provides a penetrating look at how IT security professionals perceive cyberthreats and plan to defend against them. Based on a survey of 1,200 IT security decision makers and practitioners conducted in November 2022, the report delivers countless insights IT security teams can use to better understand how their perceptions, priorities, and security postures stack up against those of their peers.

Notable Findings

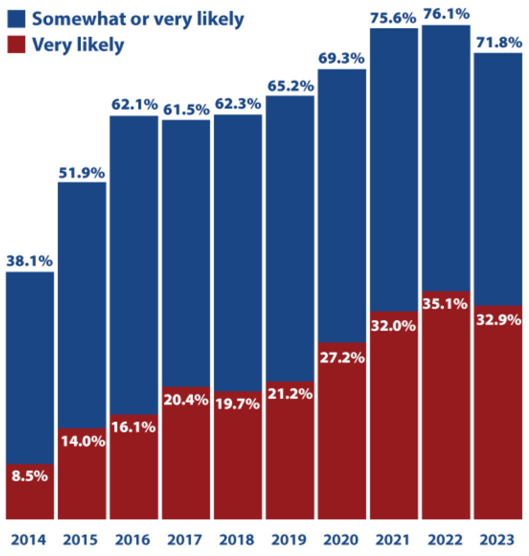
- **Pressure on security teams may be easing.** IT security professionals are showing a bit of optimism. Compared with last year's survey, the percentage of organizations expecting a successful cyberattack in the coming 12 months fell from 76.1% to 71.8%.
- **But attack surfaces are growing.** Organizations are concerned about their capabilities in areas like attack surface reduction, third-party risk management, and brand protection.
- **Web and mobile attacks are top of mind.** Security teams are particularly sensitive about attacks that can result in account takeovers and various types of online fraud.
- **Bot management and API protection are popular.** Among application and data security technologies, they lead in "planned for acquisition" and "currently in use," respectively.

Glimmers of Hope Among Islands of Concern

After years of losing ground, data in this year's CDR provides evidence that IT security teams are becoming slightly optimistic. The percentage of organizations that experienced a successful cyberattack in the previous 12 months peaked two years ago. The number saying that a compromise in the coming year is likely or very likely fell 4.3% from last year, from 76.1% to 71.8%.

However, IT security professionals are concerned about their organizations' capabilities in many areas. They are least confident about attack surface reduction (through practices such as patch management and pen testing), third-party risk management, user security education, brand protection, and cyber risk quantification.

Percentage of organizations indicating compromise is "more likely than not" in the next 12 months

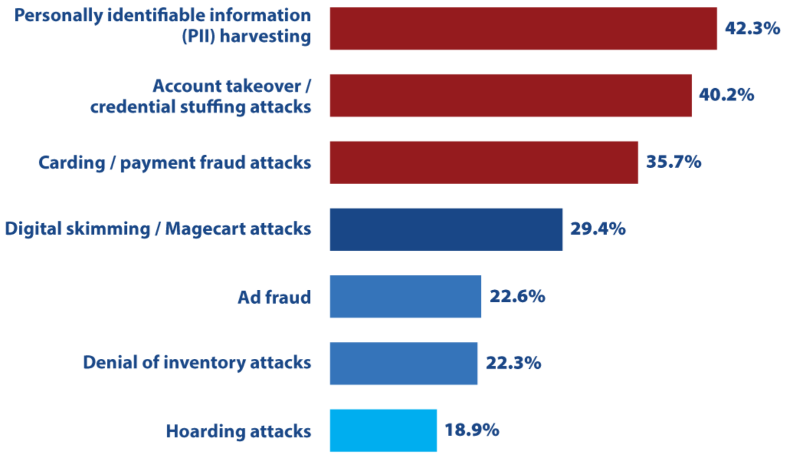


Digital Attacks Keep Security Teams Up at Night

When asked to pick three types of web and mobile application attacks that most concerned them, IT security professionals most often name PII harvesting, account takeover (ATO) and credential stuffing attacks, and carding and payment fraud attacks. These are followed by digital skimming and Magecart attacks, ad fraud, and denial of inventory attacks.

There is no doubt about the pervasiveness of web and mobile attacks. Nine out of ten organizations (91.5%, to be precise) say they were affected by at least one of them in the past year. Among major industries, finance, retail, and telecom and technology organizations were affected most often, with healthcare and education not far behind.

Most-concerning web and mobile application attacks



Bots and APIs Draw Attention

When it comes to application and data security technologies, this year's rising stars (solutions most often planned for acquisition in the next 12 months) are bot management , application security testing, and application container security tools. This is the third year straight that bot management has led the list, reflecting the major role bots play in ransomware, spam, DDoS, and other top-of-mind attacks.

The "must-haves" (solutions currently in use at the most organizations) are API protection products, database firewalls, and web application firewalls (WAFs).

Application and data security technologies in use and planned for acquisition

	Currently in use	Planned for acquisition	No plans
API gateway / protection	60.6%	30.9%	8.5%
Database firewall	60.1%	29.0%	10.9%
Web application firewall (WAF)	55.4%	35.8%	8.8%
Database activity monitoring (DAM)	51.7%	36.1%	12.2%
Application container security tools/platform	50.8%	40.1%	9.1%
Cloud access security broker (CASB)	50.2%	35.4%	14.4%
Application delivery controller (ADC)	50.2%	33.7%	16.1%
Runtime application self-protection (RASP)	49.3%	35.8%	14.9%
File integrity / activity monitoring (FIM/FAM)	46.4%	39.9%	13.7%
Third party code analysis	45.1%	35.3%	19.6%
Static/dynamic/interactive application security testing (SAST/DAST/IAST)	44.6%	41.2%	14.2%
Bot management	35.9%	43.6%	20.5%

About Human Security

HUMAN is a cybersecurity company that protects organizations by disrupting digital fraud and abuse. We leverage modern defense to disrupt the economics of cybercrime by increasing the cost to cybercriminals while simultaneously reducing the cost of collective defense. Today we verify the humanity of more than 20 trillion digital interactions per week across advertising, marketing, e-commerce, government, education and enterprise security, putting us in a position to win against cybercriminals. Protect your digital business with HUMAN.

CYBEREDGE

About CyberEdge Group

CyberEdge Group is an award-winning research, marketing, and publishing firm serving the needs of information security vendors and service providers. Our expert consultants give our clients the edge they need to increase revenue, defeat the competition, and shorten sales cycles. For information, connect to our website at www.cyber-edge.com.