Top cybersecurity trends for 2023

BY ANNA HAMMOND · DECEMBER 28, 2022 · LAST UPDATED ON MARCH 6, 2025

We look ahead to some key cybersecurity trends for next year.

Importance of remote working security measures

While the pandemic may seem like a thing of the past, many of its effects are here to stay. This includes working from home and hybrid working.

The idea of people keeping their laptops and other work devices at home may sound like a safer alternative. But in reality, this new way of working presents a fresh set of security risks.

Securing one network, such as an office, is in some ways simpler than the risks attached to numerous home ones. This expanding attack surface places increased importance on training employees around key security practices.

Things like safe password handling and keeping all devices updated should be a core part of the onboarding process. Network administrators, meanwhile, will continue to utilize the 'zero-trust' approach that has seen rapid adoption in a post-covid world.

Increasing transparency around cybersecurity

With both the frequency and cost of cyber-attacks and data breaches increasing, it's no wonder that the public view on security has also changed. People are far more aware of the importance of cybersecurity and rank robust security as a mandatory requirement, rather than a bonus.

In a recent article for Spiceworks, Tony Liau, vice president of product marketing at Object First, said breach-hit organizations should not try to downplay or hid security incidents and be transparent in their messaging.

"They'll need to admit to the problem and provide details on what steps they are taking to mitigate the issue and prevent future breaches," Liau said. "Customers will appreciate this honesty and will be more likely to do business with companies that are open and transparent about their cybersecurity practices."

As part of our own effort to assist our partners with their own transparency and compliance requirements, this year we created the Intigriti Trust Center, which displays our security posture in real time.

Crowdsourced security's continued growth

In what has been a challenging year for many businesses, crowdsourced security has continued to grow from strength to strength. In a recent projection by Future Market Insights, the market is expected to reach $243 million in 2032, with a predicted growth rate of 7.8% over the next 10 years. This is no doubt the result of businesses making bug bounties and other crowdsourced security services a permanent fixture.

Ethical hackers have responded to this, with the latest cybersecurity workforce study from industry organization (ISC)² indicates that the global cybersecurity workforce is now 4.7 million people – the highest it's ever been.

Growth in AI-powered applications

The recent beta launch of ChatGPT highlighted the incredible potential that artificial intelligence (AI) holds for cybersecurity industry.

As we recently reported, ChatGPT has shown to be adept in several cybersecurity functions, many of which directly impact the bug bounty industry. This includes creating custom code for scanning and writing penetration test reports.

READ MORE How AI is changing the game for cybersecurity

But it's not quite as simple as that. AI represents a threat as much as an opportunity. Machine learning models are being used to write malicious code, and applications such as ChatGPT may allow attackers to scale up their convincing phishing campaigns.

AI is a new sandbox for developers, and adopters of this technology will need to ensure their AI systems are safe from AI-specific threats.

Ongoing game of cat and mouse

If there's one thing that's the same every year, it's that cybersecurity is continuous back and forth between the latest attack techniques and the methods used to protect against them. Looking ahead to 2023, this was summed up by John Dwyer, head of research at IBM Security X-Force:

> **"Almost as fast as the cybersecurity industry releases new security tools, adversaries evolve their techniques to circumvent them. This year will be no different. We expect to see cyber criminals set their sights more specifically on MFA and EDR technologies.**
>
> **With some attackers having succeeded at circumventing non-phishing-resistant MFA this past year — and more organizations relying on it than ever before – this technology will grow as a top target next year. Similarly, adversaries have been honing EDR evasion techniques. We expect to see a massive spike in the number of EDR evasion tools for sale on the dark web."**

It's becoming increasingly difficult to stay protected against every emerging threat, particularly as organizations' security workforces are being spread thin.

If this is true for your business, a **bug bounty** or other crowdsourced security service could help you to offload this burden by putting it in the safe hands of our ethical hacking community.

REQUEST A DEMO

intigriti.com/demo

VISIT THE WEBSITE

intigriti.com

GET IN TOUCH

hello@intigriti.com