Huntress Cybercrime Trends Report

Additional Findings

Cybercrime attack types, motivations, and impact

1. Most common type of cybercrime experienced by organizations this year:

Malware infections	**53.4%**
Phishing attacks	**44.3%**
Business email compromise (BEC) attacks	**36.0%**
Website defacement or denial-of-service attacks	**35.4%**
Insider threats leading to data theft or sabotage	**32.3%**
Credential stuffing or account takeover attacks	**28.0%**
Supply chain compromise leading to cyber incidents	**24.4%**
Cryptojacking incidents	**21.0%**
Intellectual property theft	**19.4%**

2. Main motivation behind cyber attacks:

Financial gain	**26.9%**
Data theft	**23.3%**
Reputational damage	**14.9%**
Disruption of operations	**10.9%**
Ideological reasons, such as “hacktivism”	**8.7%**
Unknown causes	**8.7%**
Not applicable, no incidents	**6.6%**

3. Estimated yearly financial loss from cybercrimes:

Less than $1,000	**2.6%**
$1,000–$10,000	**3.3%**
$10,001–$50,000	**10.9%**
$50,001–$100,000	**14.9%**
$100,001–$500,000	**26.6%**
$500,001–$1,000,000	**17.3%**
More than $1,000,000	**14.4%**
No significant financial impact	**6.8%**
Do not track this metric	**3.1%**

Perceived preparedness for cybercrimes

1. Cyber incident preparedness for non-IT leadership:

Very prepared	**63.8%**
Somewhat prepared	**32.3%**
Not very prepared	**3.1%**
Not prepared at all	**0.7%**

2. Security measures to detect and mitigate a multi-stage attack that doesn't rely on traditional malware signatures:

Very confident	**57.9%**
Somewhat confident	**36.5%**
Not very confident	**5.4%**
Not confident at all	**0.2%**

3. Most underfunded or under-resourced training:

Security awareness training	**16.1%**
Network security	**14.2%**
Cloud security	**13.3%**
Supply chain/third-party risk management	**12.9%**
Threat intelligence	**10.2%**
Data loss prevention	**8.9%**
Identity and access management	**7.4%**
Application security	**6.6%**
Vulnerability management	**6.5%**
Endpoint security	**3.9%**
Other	**0.2%**

Anticipated and unanticipated threats

1. Greatest unanticipated risk to your organization in the next 12–18 months:

AI-powered social engineering	**37.8%**
Hybrid attacks, combining social engineering with technical exploit	**21.2%**
Insider threats, malicious or negligent	**7.2%**
Business email compromise	**6.3%**
Deepfakes	**6.1%**
Manipulation of remote work environments	**6.1%**
Supply chain social engineering	**5%**

SMS/smishing and voice/vishing attacks	**4.6%**
Other	**0.2%**
None of the above pose an unanticipated risk	**5.5%**

2. Biggest risk to organizations:

Organized criminal groups	**25.7%**
Competitors	**19.2%**
Malicious insiders	**18.1%**
Hacktivists	**15.7%**
Negligent insiders	**12%**
Nation-state actors	**8.9%**
Other	**0.5%**

3. Most significant shift in cybercrime attacks:

Proliferation of AI-powered attacks	**41.7%**
Increased regulation and compliance requirements	**17%**
Greater targeting of specific industries or critical infrastructure	**15.9%**
Increased sophistication of attacks	**14.9%**
Growing impact of state-sponsored attacks	**10.5%**