TOP 08 CYBERSECURITY THREATS

$4.45 million

Average cost of a security breach [1]

Effective breach protection begins with understanding the threats. Here are the top cybersecurity threats you need to prepare for.

01 Malware and ransomware

Sophisticated malware and ransomware cyberattacks continue to escalate, with tactics like fileless malware proving particularly challenging to detect. Cybercriminals use command and control (C2) communication attacks to take over compromised computers to steal data or carry out distributed denial of services (DDoS) attacks.

72%

Organizations impacted by ransomware in 2023 [2]

90%

Phishing attacks that begin with an email [3]

02 Phishing attacks

Unsurprisingly, many malware and ransomware attacks are carried out via emails and other means that deceive users into revealing sensitive information or downloading malicious content.

03 Stolen credentials

Stolen credentials are big business on the Dark Web, where cybercriminals buy and sell credentials and personal information for illicit activities that range from malware to ransomware-as-a-service to financial fraud.

24.6 billion

Stolen credentials available on the Dark Web [4]

95%

Companies that experienced an API security incident in the past year [5]

04 API attacks

Bad actors misuse poorly coded application program interface (API) endpoints or business logic vulnerabilities to manipulate API behaviors. API attacks can be used for data breaches, fraudulent transactions, DDoS attacks, or privilege manipulation.

05 Advanced persistent threats

These covert cyberattacks often target enterprises and government networks. Using sophisticated hacking methods, intruders gain unauthorized access to a network for long periods without being detected.

84%

Companies with high-risk vulnerabilities on external networks [6]

06 Vulnerability exploits

By exploiting unaddressed security flaws, misconfigurations, and poor cyber hygiene, cybercriminals can remotely access a network and gain elevated privileges, wreaking havoc on your infrastructure through data loss, identity theft, and more.

07 Insider threats

One of your top cybersecurity threats comes from within. Authorized users with access to your data and resources can inflict substantial harm—intentionally or not.

$16.2 million

Average annual cost of insider threat security incidents [7]

83%

Organizations that have experienced at least one data breach [8]

08 Data breaches and leaks

Whether data is leaked from the inside due to human error or malicious insiders or accessed or stolen from the outside by bad actors, the repercussions can be devastating—both financially and reputationally.

Assess your security breach protection readiness

- [ ] How well does our security program address our needs?
- [ ] What is my organization's risk tolerance?
- [ ] What security incidents have occurred, and have vulnerabilities been addressed?
- [ ] What are our threat vectors?
- [ ] What sensitive data do we need to protect?
- [ ] Do we have the skills and resources to detect, respond to, and mitigate security incidents effectively?
- [ ] What security policies and best practices do we use, and how well are they working?
- [ ] What cybersecurity tools are in place, and how well are they working?
- [ ] What level of visibility and alerting do we have?
- [ ] What are our publicly facing exposures, and how well are they addressed?

Schedule your complimentary Cybersecurity Workshop

Led by GDT security experts, this half-day workshop will help you understand your cybersecurity program's strengths, limitations, gaps, and exposures. You'll walk away with actionable recommendations to help you bolster your defense and lower risk.

Claim my Cybersecurity Workshop

1. Source: IBM
2. Source: Statista
3. Source: Verizon
4. Source: Digital Shadows
5. Source: Gartner
6. Source: Positive Technologies
7. Source: Ponemon Institute
8. Source: IBM

GDT | cisco Partner