Top 10 Cybersecurity Threats in 2022

TechRounder PDF Edition

Live article: https://www.techrounder.com/security/top-cybersecurity-threats-in-2023/

By Vipin PG | Published December 1, 2022 | Updated March 8, 2026 | Format: Analysis | 5 min read

In brief

Today’s level of connectivity brings us to the ultimate question: how to stay safe and avoid cyberattacks in 2022? Unfortunately, while we are used to seeing technology at home and the office, the number of cyber incidents isn’t decreasing.

Today’s level of connectivity brings us to the ultimate question: how to stay safe and avoid cyberattacks in 2022? Unfortunately, while we are used to seeing technology at home and the office, the number of cyber incidents isn’t decreasing.

More importantly, such attacks are becoming alarming since they are both hard to detect and prevent. As a result, businesses are prioritizing cybersecurity to avoid damaging consequences, such as revenue or reputational loss.

There’s no surprise here, as being proactive is the most important thing about an effective cybersecurity strategy. To achieve this goal, you need to be aware of the leading cybersecurity risks that the world faces today. So let’s not waste time and jump right into it.

1. Bad Cybersecurity Hygiene

Yes, your online habits matter. For instance, your cybersecurity hygiene isn’t top-notch if you use a public WiFI network, as it imposes a risk of getting hacked easier. You also need to forget working in public coffee shops where many people might get a good peek at your sensitive data. And let’s not forget sticky notes and writing down your passwords; that’s a big no as well.

Despite the simple fact that everyone knows the basics of cybersecurity, statistics show that many skip important measures that would keep their data secured. For example, organizations rely on their staff members to remember passwords rather than install a proper password manager.

The same goes for WiFi networks. In addition, not enough businesses and people at home are using VPNs or multi-factor authentication to prevent leaving security gaps.

2. Application Security Vulnerabilities

Program errors can occur due to bad code or a virus that accessed the device. Application security is a big deal when maintaining a good security program. Online criminals are becoming more sophisticated, launching complex attacks against businesses and individuals.

Remember to stay far away from pirated software, even if you plan to use it at home. Also, keep up with the classics and update your software regularly.

3. Ransomware Attacks

Of course, ransomware isn’t a new groundbreaking thing that we would be shocked about. Despite that, ransomware attacks remain steadily damaging. Recent research showed that 66% of companies suffered from a ransomware attack, resulting in major revenue loss.

Such consequences forced company leaders to fire employees and minimize costs. That said, any security vulnerability opens a new door for a hacker to strike. Therefore, it’s important to have proper security hygiene to minimize ransomware risks.

4. Mobile Device Risks

Even if we would like to forget the global pandemic, we can’t, as its impact is experienced daily. One of the turning points for many industries during the pandemic was the quick shift to the digital scene. That meant more remote services and more hours spent on mobile devices. Automatically, that makes a more significant number of people who use such devices and a more significant number of targets for cybercriminals.

5. Configuration Errors

Unfortunately, configuration mistakes happen, and they occur mainly because of incorrect system states, including unintended system behavior or system failures.

Despite the popular misconception, even professional security systems can have at least a single error, especially during software installation. That’s why organizing internal security tests is crucial to mimic attackers and check if the misconfiguration error chances rise.

6. Cloud Vulnerabilities

Even though cloud services are becoming more secure over time, the widespread use of this technology still raises some security questions today. Security specialists recently developed cloud technology to combat cyberattacks, creating a zero-trust policy.

Unfortunately, that means the cloud functions as if it was already breached, requiring users to constantly surpass extra security checks, such as authentication and sign-ins, during every step.

7. IoT Devices

Do you know a household that doesn’t have at least one smart device? IoT, or the Internet of Things, illustrates a network of physical devices, aka "things" that are connected. This enables the devices to exchange data in the network.

Sadly, the number of devices we use in corporate settings and personal smart devices creates an even larger sphere for cybercriminals and their attacks. Once a criminal breaches one device, they can easily access data held by another device in the IoT network.

8. Bad Data Management

Many data breaches happen due to poor data management, including stolen credentials. You’re doomed if a bad actor gains access to your passwords. That’s why data management is a skill that you might want to add to your list.

With all of the data that we have on our hands, it’s important to structurize information. In some cases, automation and AI-enabled services might help to minimize human error and avoid data breaches.

9. Poor Post-Attack Policies

If you become a cyberattack victim, that doesn’t mean you won’t fall into the attacker’s trap again. Companies that don’t have a step-by-step policy regarding what to do after a cyberattack are more likely to experience more significant damage, not to mention continuous attacks.

That’s why all security gaps need to be patched asap. Thanks to technology, we now have special patching services that automatically detect and eliminate vulnerabilities that were created due to human error.

10. Lack of Multi-Layered Security

How to mitigate and prevent cyberattacks? Well, it’s simple. If one solution doesn’t do the trick, think about multi-layered security. It’s designed to help your security team asses the main risks and create a clear cybersecurity strategy consisting of all the needed controls and protections. If your business is protected by layered security, your customers are most likely protected at every stage.

The most important part of the customer journey is the onboarding process. Usually, companies with money flow choose to add at least one security layer with an AI-powered identity verification service.

That means they check their customers’ IDs before allowing them to access their digital platforms. This prevents fraudsters and criminals who steal identities from committing financial crimes and getting their hands on sensitive information.

What’s Next for Cybersecurity?

Cybersecurity will most likely be at the top of the list regarding businesses and their priorities. As recently calculated by TechTarget, it is speculated that more than half of the companies will use cybersecurity as the primary factor to determine partnerships and new business engagements by 2025.

This leads us to the main idea that even though protecting yourself against cybersecurity threats can be exhausting at times, it’s vital to update your knowledge and step up your game in your defense strategy.

References

1. idenfy.com - https://www.idenfy.com/