Technology Consulting Group

Six key cybersecurity trends you need to know about

Microsoft

As the world becomes more connected and digital, cybersecurity is becoming more complicated. As an experienced technology provider, we know how challenging it can be to prioritize where to focus security efforts. Between infrastructure, data, and apps in the cloud, there's a lot more to protect. We can help.

1hr 42min median time it takes an attacker to begin moving laterally within a corporate network once a device is compromised[1]

98% of cyberattacks can be protected against with basic security hygiene[2]

You're only as strong as your weakest link

Keeping up with today's threats means securing every area of vulnerability, including email, identity, endpoint, Internet of Things (IoT), cloud and the external attack surface. Here are six things you need to know to prevent compromise.

1 Email remains a top vector—and a focus area for defense

In 2022, 35% of ransomware involved the use of email.[3] Phishing attacks increased by 61% from 2021 to 2022.[4] Attackers are commonly using legitimate resources to carry out their campaigns. It's getting harder to tell the difference between real and malicious emails.

Using safeguards like URL checking and disabling macros will help strengthen your security posture. Tackling more advanced email threats requires that you correlate email signals into broader incidents, visualize the attack, and understand how attackers are taking advantage of other parts of the environment to leverage legitimate resources. We can help you keep your guard up as threat actors increase the quality of social engineering in their attacks, using AI and other tools to be more persuasive.

72 minutes
median time it takes an attacker to access private data if you fall victim to a phishing email[5]

2 The expanded identity landscape also expands opportunities for threat actors

Attackers are getting more creative in circumventing multi-factor authentication (MFA) and phishing kits have made it even easier to steal credentials. The fact is, managing the identity attack surface is more than just securing user accounts. You also need to cover cloud access and workload identities too. For instance, attackers frequently get access to third-party accounts and then use those credentials to infiltrate the cloud and steal data. Often, this is accomplished through workload identities, which can be overlooked in permissions auditing.

Attacks targeting identity will continue to grow in volume and variety. Let us help you ensure that you have complete visibility into your identity and access.

921
Password attacks per second in 2022, a 74% increase from 2021[6]

93%
of Microsoft investigations during ransomware recovery engagements revealed insufficient privilege access and lateral movement controls[7]

3 Hybrid environments and shadow IT have increased endpoint blind spots

The sheer number of devices in today's hybrid environments has made securing endpoints more challenging. Unmanaged servers and BYOD personal devices contribute to the shadow IT landscape—and are particularly appealing to threat actors. And it only continues to grow. We are ready to help you improve endpoint visibility and security hygiene.

3,500
Average number of connected devices in an enterprise that are not protected by an endpoint detection and response agent[8]

4 IoT devices are proliferating, and so are IoT threats

IoT devices are an often overlooked endpoint attack vector. Interestingly, as organizations harden routers and networks to make them more difficult to breach, IoT devices are becoming a threat target of choice. For instance, an IoT device can exploit vulnerabilities to turn IoT devices into proxies—using an exposed device as a foothold onto the network. Frequently, organizations often have no visibility into IoT devices, and can even contain dangerous vulnerabilities, such as outdated, unsupported software.

There are emerging regulations for IoT security in various countries, but it's vital to gain more visibility into all your attack surfaces—and that includes IoT devices.

41 billion
IoT devices expected in enterprise and consumer environments by 2025[10]

60%
of security practitioners say IoT and operational technology (OT) security is one of the least secured aspects of their infrastructure[11]

5 Protecting the cloud is critical, but complex

Organizations are increasingly moving infrastructure, application development, workloads, and data to the cloud. This radical shift has increased the number of new attack vectors for cybercriminals to exploit, with many gaining access through gaps in permissions security. Cloud app development is a top cloud attack vector. So is cloud storage. And sometimes, cloud services providers themselves can be affected.

For app development, we recommend embracing a "Shift-left" security approach—that is, thinking about security at the earliest phases of app development. We can help you integrate your cloud and multi-cloud assets with your security tooling.

895
man-in-the-middle phishing attacks detected per month by Microsoft Defender for Cloud Apps, on average[12]

84%
of organizations that suffered ransomware attacks did not integrate their multi-cloud environments into security operations tooling[13]

6 Securing the external attack surface is an internet-scale challenge

Today, an organization's external attack surface spans multiple clouds, complex digital supply chains and massive third-party ecosystems. It also extends beyond its own assets, and includes suppliers, partners, unmanaged personal employee devices, and newly acquired organizations. Fact is, the internet is now part of the network, and despite its almost unfathomable size, security teams must defend their organization's presence throughout the internet to the same degree as everything behind their firewalls.

Are you aware of your external connections and exposure? Let us help you gain more visibility into your external attack surface and identify vulnerabilities throughout the entirety of your environment and extended ecosystem.

1,613
cyberattack–related data compromises in 2021; more than all data compromises in 2020[14]

53%
of organizations experienced at least one data breach caused by a third party from 2018-2020[15]

Our services and solutions help to keep your business protected

As a Microsoft partner, we're here to help you take advantage of the Microsoft Security solutions that give your business the security strategies you need to keep up with evolving threats. We have the expertise to assess, pilot, and deploy the right Microsoft security solutions for your business, along with a variety of managed services to help streamline your security operations.

Learn more about what we can do to help secure your business.

Contact us today

https://techcgroup.com/contact

9012903591

sales@techcgroup.com

1. 2022 Microsoft Digital Defense Report, p. 21
2. 2022 Microsoft Digital Defense Report, p. 108
3. 2022 Microsoft Digital Defense Report, p. 108, t, p. 28
4. 2022 Verizon Data Breach Investigations report, p. 28, tate-of-phishing-report-reveals-more-than-255-million-attacks-in-2022-signaling-a-61-increase-in-phishing-year-over-year-301659518.html
5. 2022 Microsoft Digital Defense Report, p. 21
6. 2022 Microsoft Digital Defense Report, p. 2
7. 2022 Microsoft Digital Defense Report, p. 14
8. 2022 Microsoft Digital Defense Report, p. 14
9. 2022 Microsoft Digital Defense Report, p. 92
10. https://www.businesswire.com/news/home/20190618005012/en/The-Growth-in-Connected-IoT-Devices-is-Expected-to-Generate-79.4ZB-of-Data-in-2025-According-to-a-New-IDC-Forecast
11. "The State of IoT/OT Cybersecurity in the Enterprise" 2021 Ponemon Institute Research Report, p. 2
12. 2022 Microsoft Digital Defense Report, p. 95
13. 2022 Microsoft Digital Defense Report, p. 16
14. 2021 Identity Theft Resource Center Annual Data Breach Report, p. 5
15. https://www.comparitech.com/antivirus/malware-statistics-facts/