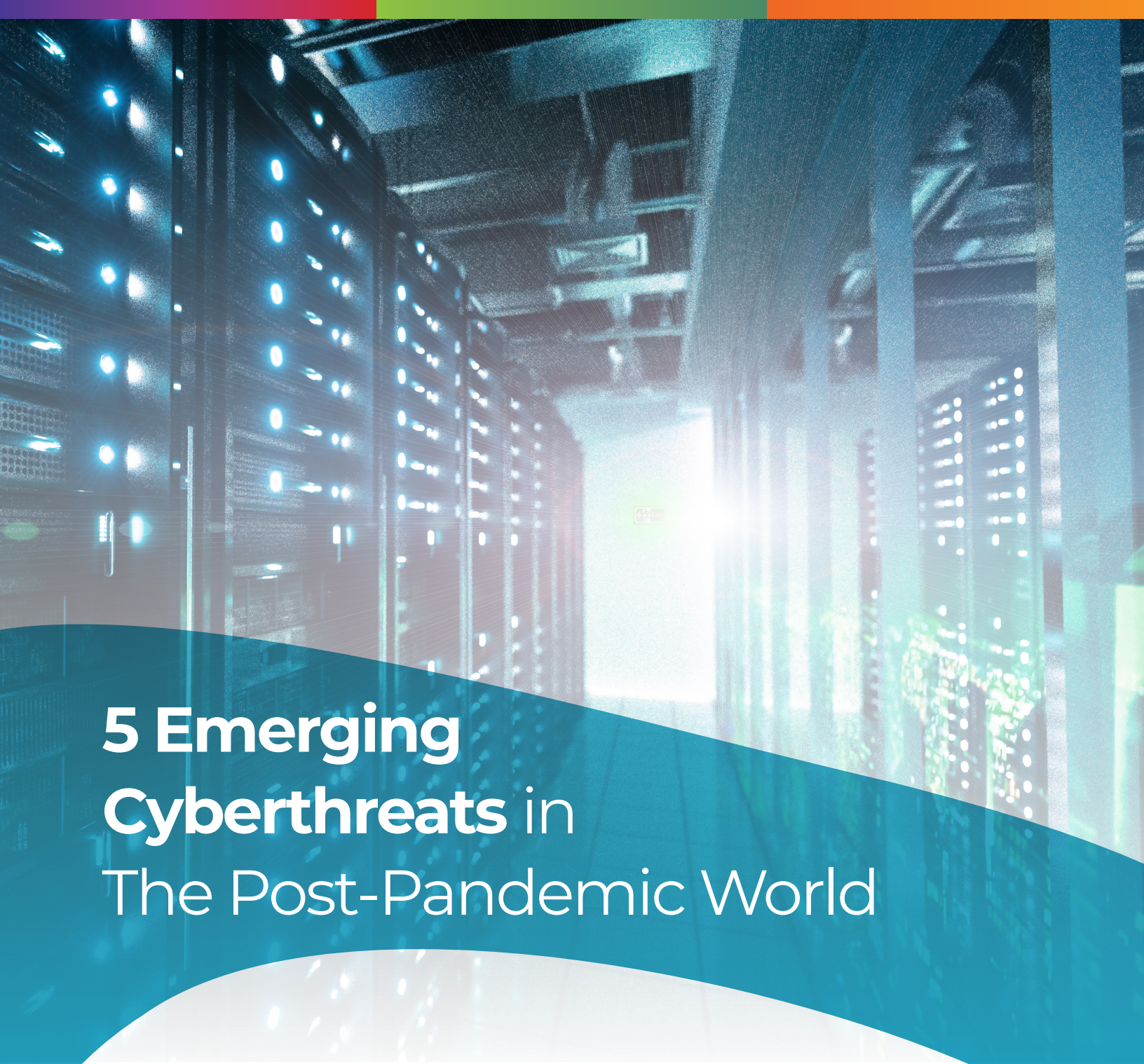

5 Emerging **Cyberthreats** in The Post-Pandemic World

kinetic business by windstream

With so many businesses moving services and applications to the cloud and remote employees leaning on these systems, many organizations are struggling to fast-track their network capabilities, especially cybersecurity. Unfortunately, remote systems were not as shielded as on-premises IT infrastructures, and the rush of remote workers has left a myriad of unsecured gaps that malicious actors have been quick to exploit.

While the pandemic may have been the catalyst for change, the technological shift that shaped the workplace in 2020 appears to be here to stay. And as the story develops, so are the increasing cyberthreats that businesses are facing.

As businesses contemplate the security challenges facing their organizations in the coming months and years, it seems helpful to identify some of the growing threats in North America and highlight some basic strategies that can help to shore up networks in the post-pandemic world. After a cursory review of the reports for 2020, these were the predominant threats identified by SMEs for 2021 and beyond.

1. Malware/Ransomware
2. DDoS
3. Social Engineering
4. IoT
5. Cloud Applications

kinetic business by windstream.

Malware/Ransomware

Numbers

According to RiskIQ, $2.9 million is lost to cybercrime every minute, with top companies paying around $25 per minute as a result of data breaches. As cybercrime reports indicate, malware, more specifically ransomware, represents a big chunk of this cost. A recent study by Deep Instinct revealed that malware attacks have grown by a whopping 358% overall and ransomware is up by 435% compared to 2019.

Threats

While malware, in general, continues to wreak havoc on businesses around the globe, Cyber Experts reported a variety of malware attacks that impacted U.S. business networks in 2021. The following are worth noting, as these malware threats appear to be picking up steam.

- **Clop Ransomware -** Works by encrypting your files and asks you to pay a certain ransom amount to have them decrypted.
- **Fake Updates -** Tricks users into hacking themselves by sending fake emails and asking them to install an OS update
- **Zeus Gameover -** Mainly targets finances and can easily access your bank account details and get away with all the available funds.
- **News Malware Attacks -** A common trick where hackers use trending news to target unsuspecting people.
- **Social Engineering -** Shifting from computers to humans, hackers use deception to lure employees into giving out personal details.
- **AI Attacks -** Taking advantage of gaps in artificial intelligence (AI) technology, hackers create links to help them get into your system.
- **Cryptojacking -** Cybercriminals are taking advantage of cryptocurrencies, mining the digital currencies effortlessly by installing cryptojacking malware entities on phones and computers.
- **Freeware -** More than 600 million mobile users have already downloaded this malware without realizing it, the virus charges the users large amounts of money even after uninstalling the app.
- **Ransomware as a Service (RaaS) -** One of the most popular security threats of the year where people pay expert hackers to carry out the cybercrimes on their behalf.
- **IoT Device Attacks -** Hackers target IoT devices, which don't contain hefty security measures, making them easy to manipulate and utilize to access data.

Protection

It's unrealistic to think you can stave off all malware attacks. Still, there are some tried and true methods to minimize your vulnerability, including software and firewalls. While some of these solutions are obvious, they are the most common and effective tools identified by Cyber Experts to address the constantly changing tactics of the dark digital world.

kinetic business by windstream.

DDoS Threats

Numbers

According to the FBI's IC3 report, an estimated 4.83 million Distributed Denial-of-Service (DDoS) attacks have been attempted since the first half of 2020. More than 929,000 DDoS attacks occurred in May of 2020 alone, which represents the single largest number of attacks ever seen in a single month. It has been reported by Helpnet Security that each hour of service disruption costs businesses an average of $100k.

Threats

With the demands of the pandemic, these past few years have seen organizations embrace remote work at unprecedented rates. According to Helpnet Security, this increased online traffic and dependence on digital services has made systems extremely vulnerable to cybercriminals.

One of the emerging methods of attack for bad actors are DDoS attacks, which are becoming increasingly pervasive, malicious, complex and costly to address. They come in the form of cyberattacks that take down an online service, like a website or application, to prevent users and customers from accessing critical resources. The attackers will then typically generate large volumes of packets or requests to ultimately overwhelm the target system, using multiple compromised or controlled sources to generate the attack.

However, cybersecurity experts say that bad actors are now more focused on shorter, more complex attacks. By their estimates, super-sized 15-plus vector attacks have increased 2,851% since 2017, while the average attack duration dropped 51% from the same period last year. Moreover, single-vector attacks fell 43% while attack throughput increased 31%, topping out at 407 Mpps.

This translates into greater challenges, as the increase in attack complexity and speed, coupled with the decrease in duration, gives security teams less time to defend their organizations from increasingly sophisticated attacks. However, increasing traffic over shorter durations doesn't seem to be the only thing worrying cybersecurity experts. It appears that criminals are now employing artificial intelligence (AI) to perform DDoS attacks. According to an article in the Boston Business Journal, hackers managed to steal the data of 3.75 million TaskRabbit app users and 141 million users were affected by the app's downtime. But the poison can also be the cure, as AI can also look for the weak spots, especially if there is a massive amount of data involved.

Protection

When it comes to solutions, building defenses against DDoS attacks is more than just using a great threat mitigation solution. In the past 18 months or so, especially with the COVID-19 based social limitations, security experts are seeing a rise of ransomware-driven attacks and other Advanced Persistent Threats (APT) related to DDoS. The following are some DDoS protection techniques used to help mitigate the risk of DDoS threats.

- **Reduce Attack Surface Area -** One of the first techniques to mitigate DDoS attacks is to minimize the surface area that can be attacked thereby limiting the options for attackers and allowing you to build protections in a single place.
- **Plan for Scale -** Two key considerations for mitigating large scale volumetric DDoS attacks are bandwidth (or transit) capacity and server capacity to absorb and mitigate attacks.
- **Transit Capacity -** When architecting your applications, make sure your hosting provider provides ample redundant internet connectivity that allows you to handle large volumes of traffic.
- **Know What is Normal and Abnormal Traffic -** More than just rate limiting, advanced protection techniques go a step further and intelligently only accept traffic that is legitimate by analyzing the individual packets themselves.

kinetic business by windstream.

Social Engineering

Numbers

Cisco reported that successful spear phishing attacks accounted for 95% of breaches in business networks in 2020, with phishing attempts soaring by 667%. In the report, 43% of workers admitted to making mistakes that compromised cybersecurity. Last July, Twitter fell victim to a successful phishing attack, which netted scammers more than $100k.

Threats

Social engineering attacks are not only becoming more common against enterprises and SMBs, but they're also increasingly sophisticated, according to Digital Guardian. With hackers devising more clever methods for fooling employees into handing over valuable company data, enterprises must use due diligence in an effort to stay two steps ahead of cybercriminals.

According to a SME with Digital Guardian, the most common social engineering attacks by far come in the form of "I just need." Basically, someone calls the company claiming to represent the phone company, internet provider, etc., and starts asking questions. They claim to have a simple problem or know about a problem that can be fixed quickly but they just need one little thing. It could be as innocuous as asking for a username or someone's schedule or as blatant as asking for a password. Once the attacker has this information, they call someone else in the company and use the new information to refine their attack. Lather, rinse, repeat.

Protection

So, what does a company do to prevent being victimized by such trickery? For starters, humans need to be trained, as they are the weakest link. Companies should consider employing, at the very least, a bi-annual training for each user group (end users, IT staff, managers, etc.) so that everyone is aware of the latest attacks. Digital Guardian suggests that companies should:

- **Take a baseline assessment** of employee understanding.
- **Help employees understand** why their security discretion is vital to corporate health.
- **Create a targeted training program** that addresses the riskiest employees and/or prevalent behaviors first.
- **Empower employees** to recognize potential threats and independently make correct security decisions.
- **Improve knowledge retention** with short interactive training sessions that work easily into employees' busy schedules and feature proven effective learning science principles.
- **Monitor employee completion of assignments** and deliver automatic reminders about training deadlines.
- **Show measurable knowledge improvement** over time with easy-to-read reports for executive management.

kinetic business by windstream.

Internet of Things (IoT)

Numbers:

IoT malware has shown continued growth since 2018, according to Business Insider. But, according to reports, these attacks increased even faster in 2021. IoT attack volume in the first six months of 2021 rose 59% from the first six months of 2020 — a period which itself showed a 50% jump over the same time in 2019. Threat Post reported that the half of 2021 saw 1.5 billion attacks, up from 639 million during the previous half year, which is more than twice the volume.

Threats

With millions still working from home, Threat Post reports that cybercriminals are targeting corporate resources via home networks and in-home smart devices. They know organizations haven't quite gotten used to the new perimeter — or don't have one established.

Over the past 18 months, the lack of incident preparedness has become increasingly evident according to Threat Post. The report makes particular note of the influx of personal devices logging onto corporate networks, resulting in reduced endpoint visibility, expanded attack surface and surge in attack vectors.

Experts also find the end result of attacks on IoT gear is evolving. Infected devices are not just being used to steal personal or corporate data as mentioned, but are mining cryptocurrencies, on top of traditional DDoS attacks in which the devices are added to a botnet.

Protection

To keep IoT devices and ecosystems safe, cybersecurity experts recommended that users implement the following best practices:

- **Install updates for firmware** as soon as possible. Once a vulnerability is found, it can be fixed through patches within updates.
- **Always change preinstalled passwords**. Use complicated passwords that include both capital and lower-case letters, numbers and symbols, if possible.
- **Reboot a device** as soon as it begins acting strangely. Note: This might help eliminate existing malware, but this doesn't reduce the risk of getting another infection.
- **Review and choose security solutions** that help to protect IoT ecosystems.

kinetic business by windstream

Cloud-based Applications

Numbers

According to McAfee, cloud-based user accounts were hit by almost 3.1 million external cyberattacks throughout the past year. The shift to remote work in 2020 forced organizations and employees to become even more dependent on the cloud. For the second quarter of 2020, McAfee found a 605% increase in cloud-based threats, followed by a gain of 240% in the third quarter and 114% in the fourth quarter.

Threats

With more data and applications moving to the cloud, businesses are facing unique infosecurity challenges, and opening the door further for hackers. This trend is a perfect lure for hackers. Since the beginning of 2021, the number of attempted breaches grew by 250% compared to 2019. The criminals scan for cloud servers with no password, exploit unpatched systems and perform brute-force attacks to access the user accounts. Some try to plant ransomware or steal sensitive data, while others use cloud systems for cryptojacking or coordinated DDoS attacks.

CSO identified the top security threats organizations face when using cloud services:

- Data breaches
- Misconfiguration and inadequate change control
- Lack of cloud security architecture and strategy
- Insufficient identity, credential, access and key management
- Account hijacking
- Insider threats
- Insecure interfaces and APIs
- Weak control plane
- Metastructure and applistructure failures
- Limited cloud usage visibility
- Abuse and nefarious use of cloud services

Protection

To strengthen cloud computing defenses, businesses should pay close attention to proper cloud storage configuration, security of application user interfaces (APIs) and the end-user actions on cloud devices. While there are a myriad of solutions for protecting data and information in the cloud, these are a few that experts recommend for continued consideration:

- **Deploy MFA (multi-factor authentication)** to reduce the risk of unauthorized access due to credential compromise. When you haven't enabled MFA or you've applied a bypass setting, you've significantly increased your organization's risk, making it susceptible to threats like phishing, brute-force attempts and stolen passwords.
- **Practice Remote Desktop Protocol (RDP)** security best practices. If you absolutely have to use RDP, always make sure to abide by security best practices by implementing least-privilege principles, enabling network-level authentication, and always putting RDP-enabled services behind a VPN.
- **Deploy a cloud-based Security Event and Incident Management (SIEM)** tool. SIEM can detect risky connections from the internet, like RDP and FTP.

kinetic business by windstream.

Final Thoughts

The predominant trend for defending against cyberattacks appears to be the use of artificial intelligence to turn technology against itself. Cybersecurity is benefitting from the use of AI, and its subsets, ML, and DL, to stem the flow of cyberattacks. But as we have seen, time and again, cybercriminals are extremely versatile and innovative. AI not only enables swift and accurate analysis of data for good purposes, but it also allows data to be used for malicious reasons. The arms race between the enterprise and cybercriminals looks set to continue; however, companies now have cybersecurity strategies and services they can utilize to fend off even the most critical cyberthreats.

kinetic business by windstream

If you would like to receive additional information about cybersecurity, or are interested in learning more about any of our other business connectivity, collaboration or continuity solutions, **please click here** to select the solutions you are interested in.