DTS DanTech Services
Computers under control!™

Technology Times October 2022 Issue

"With over 20 years of experience providing remote support to clients that rely on technology, I know what it takes to deliver business continuity. Add to that another 20 years of support in the service industry you'll not find another company that takes customer service to heart as I do. Find out for your business what a difference it makes. "

What's Inside:

Got IT Problem? - Click Here!

Cybersecurity Trends You Should Know About in 2022

By Karim Ahmad

What are the greatest security threats you face this year? What are the cybersecurity trends helping you fight attacks? Here's what you need to know.

Cybersecurity trends have evolved considerably over the past few years. As hackers have become more adept at breaking through advanced firewalls, companies have had to update their systems. Millions around the globe are affected by data breaches, while cyber crime continues to run rampant. Cybersecurity is a major concern for businesses, individuals, and organizations alike.

Rising Ransomware Threats

One of the biggest cybersecurity trends of 2022 is the rise of ransomware attacks. **Ransomware essentially holds your files hostage** until you pay a specific amount, usually in cryptocurrency. Obviously, there's no guarantee that your files will be unlocked even after you make the payment. In most cases, it's a slippery slope, with **ransomware gangs** preying on the less tech-savvy and demanding increasing sums of money. All it takes is a single malicious file download to spread the infection throughout a hard drive.

This is a serious problem for companies, especially if an unsuspecting employee downloads ransomware on to their computer. There's a risk of the entire network being held hostage, which could effectively grind business to a halt. But obviously that's also a problem for individuals—no one is safe from ransomware. In the first half of 2021, the total ransomware payments reported by banks were **$590 million**.

- Continued on page 3

Your computer was hacked!

You may be right if your computer or phone is acting strange and you suspect you've been hacked or infected by a virus. When hackers target business organizations, they are after personal and financial data, trade secrets, and access information to extort victims or breach sensitive data. In that case, you must take quick action to protect your information and prevent the attack's spreading through your digital and professional network.

Quarantine Your PC. Isolate the infected computer as soon as possible. As long as you're connected to the internet, the hacker has access to the device and its directory. Unplug your computer from the network and avoid any wireless or physical connection. Make sure you're offline and turn all Wi-Fi connections off, both by software and hardware.

Change your passwords. First, you need to change your PC's access password. Then, change all your passwords using an unaffected computer or smartphone—email, social networks, subscriptions, etc.

.

Remove external hard drives. If you have USB flash devices and external hard disks connected to your PC, make sure you disconnect them from your device. Don't forget to "eject" them first. (Select the relevant folder and then click "eject.")

If you're positive you've been hacked, you should also delete your computer's hard disk. Back up whatever files you have (you may even save them to the cloud, such as Google Drive, or email tiny files to yourself); if you're not comfortable doing so, seek the assistance of an IT specialist.

Alert those connected to you. Hackers will try to spread by breaching an individual and targeting their network. The reason is simple. Your friends are more likely to open messages from you without thinking twice.

UNSURE?
CALL 907-885-0501

What is a Cybersecurity Mesh? What It Means for Today's Enterprises?

Fully centralized IT networks may be a thing of the past, but many enterprises are still clinging to their old ways. It's not always easy for larger companies with complex IT architectures (such as banks, heavy manufacturing companies, and government organizations) to keep pace with a more distributed model. Today's modern architectures are pushing more data processing to the edge, and many rely on multiple cloud implementations and datacenters to make their businesses run smoothly.

Zero Trust Strategy. The cybersecurity mesh is a key component of a zero-trust network philosophy, whereby any device is by default not trusted to access the broader network. Perimeter-focused security often fails because as much as 34 percent of data leaks and breaches originate on the inside of the network itself. A distributed cybersecurity mesh that utilizes zero trust adapts to emerging threats and changing access needs. Threats can be detected in real-time and assets such as data and devices can be protected better than simple VPN passwords. The mesh ensures that all data, systems, and equipment are treated equally and securely — it doesn't matter where they are located in (or out) of the network. Any connection to access data is by default considered "unreliable" until it is verified by the security protocol.

Protecting Applications and IT Services. When it comes to rolling out large-scale applications in an enterprise environment, the concept of a service mesh is also catching on. Companies are increasingly deploying microservices (an architectural style that structures apps as a collection of services that are loosely coupled and independently delivered, rather than as one monolithic service). Protecting applications like these in a cybersecurity mesh adds efficiency and transparency to the process, and it can be combined with a zero-trust strategy to harden the security posture.

Some examples of attacks that can be mitigated include:

- Service Impersonation: Where a hacker accesses a private application network, acts as an authorized service, and makes requests for confidential data.
- Unauthorized Access: Where a service request (even a legitimate one) tries to access sensitive data that it is not authorized for.
- Packet Sniffing: The process of intercepting legitimate requests and using them to gain access to data.

Mesh Training Can Make a Difference. Security frameworks are only as good as the IT people who implement them. That's why it's important that your cybersecurity experts are well-versed in mesh and other security options, and that a culture of continuous improvement is built into your strategy.

Mesh-focus training concepts include:

- Building data security that is based on downstream utility so that data can be accessed without exposing it unnecessarily.
- Creating a cybersecurity mesh that scales as volume of applications and data grow.
- Educating IT workers on the importance of continually monitoring and measuring application performance.

Shiny New Gadget Of The Month:

LogiTech Ergo K860 ergonomic keyboard

A FEEL-BETTER TYPING EXPERIENCE

Introducing ERGO K860, a split ergonomic keyboard designed for better posture, less strain, and more support.

You'll type more naturally with a curved, split keyframe that improves typing posture. The sloping form reduces muscle strain on your wrists and forearms – keeping your hands and shoulders relaxed.

BETTER POSTURE, BETTER RESULTS

ERGO K860's curved keyframe places your hands, wrists, fingers and forearms in a more natural posture – you'll notice the lack of strain the moment your hands land on the keyboard.

ERGO K860 has even been proven to reduce muscle activity by 21% in the upper trapezius muscle (Compared to a traditional Logitech keyboard without palm rest) — key muscle in the center of the back that stabilizes and facilitates shoulder and neck movement.

EFFORTLESS PRECISION WITH PERFECT STROKE KEYS

A fluid and ultra-precise typing experience with no compromise in speed and accuracy. Your fingers glide effortlessly across the matte surface of the keys, and tactile details make it easy to orient your fingers and stay focused. The split layout and convex curve promote a more natural hand and finger placement.

"Cybersecurity Trends in 2022" - continued from page 1

This figure is only expected to increase by the end of 2022.

The Meteoric Growth of Security-as-a-Service.

Many Security-as-a-Service businesses have gained traction as companies look into advanced, modular technologies that allow them to reduce malware or ransomware threats. Instead of building ground-up firewall solutions, an increasing number of companies are now opting for Security-as-a-Service options. These are security solutions offered by a managed security service provider, and are generally tailored according to the needs of the organization. This also ensures that the company is able to benefit by working with a team of technological experts with a better understanding of cybersecurity, as compared to hiring an in-house IT professional to focus on reactive troubleshooting and ad hoc fixes.

Geo-Targeted Phishing Attacks.

Phishing attacks continue to rise in frequency and severity. In fact, **Phishing as a Service** exists too, so it's all the more important for people to protect themselves online. Currently, phishing scams are the biggest threat that the IT industry faces. Millions fall for these elaborate scams, where cybercriminals use different methods to execute all kinds of scams, from elaborate **business email compromise schemes** to injecting malicious URLs in emails. In the past, cybercriminals would often cast a broader net and wait for people to fall prey to their scams. Now, phishing can be more personalized and geo-targeted. Scammers now use your geolocation to create custom phishing websites or email chains to target victims. This makes it difficult for individuals to distinguish between phishing scams and the real deal, which is one of the reasons why they end up falling prey to these scams.

Multi-Factor Authentication Becomes a Standard.

For too long, the global IT sector has dithered on adopting **Multi-Factor Authentication (MFA)** as a standard. That, thankfully, is now changing. Many organizations, especially in the financial technology sector, have introduced MFA and made it mandatory for all users. Multi-factor authentication essentially adds another layer of security, preventing unauthorized access to online accounts. Almost every major company now requires individuals to use multi-factor authentication, ranging from social media platforms to email services. MFA ensures that organizations can better protect their employees' data and control access. Whenever a person signs in, they must also enter a verification code, which is sent through an authenticator app, or to their registered phone number.

IoT Vulnerabilities.

The Internet of Things (IoT) has completely changed the way we interact with devices. IoT devices are dominating the consumer markets, and despite some **common security issues with IoT devices**, most people generally have high confidence in them. However, while they offer greater convenience, IoT also poses increased risks to a user's data. In case a device is hacked or hijacked, it could essentially listen in and steal information from the network. Hackers have found a new gateway to access information, and are utilizing it to the fullest. For instance, hackers often try to hack into connected camera networks or devices in order to access security systems. However, confidence is still high, with **global IoT spending growing 24 percent in 2021**. Most of the investments are by businesses in the IoT software and security space. IoT vulnerabilities pose a unique challenge, since they're used for specific purposes. The communication protocols used to connect with different devices also expose the network to software bugs or vulnerabilities, increasing the potential for harmful attacks if proper security steps aren't taken.

Cybersecurity Regulations Likely to Get Stricter.

As the world moves to remote models of work, companies and governments alike are doubling down on cybersecurity. We can expect cybersecurity regulations to get stricter with time, especially as decentralization of access becomes the norm. However, protecting a company's network is important, and in order to do this, many regulatory bodies have made it mandatory for organizations to offer user awareness and cybersecurity training to their professionals.

Datafication

Datafication is simply transforming everything in our life into devices or software powered by data. So, in short, Datafication is the modification of human chores and tasks into data-driven technology.

From our smartphones, industrial machines, and office applications to AI-powered appliances and everything else, data is here to stay for longer than we can ever remember! So, to keep our data stored the right way and secure and safe, it has become an in-demand specialization in our economy.

Datafication leads to a higher need for IT professionals, data scientists, engineers, technicians, managers, and so much more. Even more useful is that anyone with a sound knowledge of technology can do a certification in data-related specializations to find a job in this space.

Data jobs are more about skills than big-level qualifications, and we have so many successful leaders emerging from smaller cities and developing countries like India. You can also equip yourself with this useful trending skill by doing a course like RPA to help you understand how automation works in the world of data. Let's look at some popular data careers:

- Big Data Engineers
- Robotics Engineers
- IT Architect
- Business Intelligence Analyst

Artificial Intelligence Is Not a Strategy. It Is a Customer Experience Accelerator

If you read the news covering artificial intelligence (AI) developments on any given day, you may feel pangs of fear and dread. From the recent UN report on AI's potential to harm human rights to the use of AI in spyware to hack into journalists' phones, it can seem as though the developers and creators of AI applications have lost control of its powerful potential. But these reports lose sight of the more effective and well-governed developments that are supporting and optimizing real work and the interchanges happening every day between humans and AI. When AI is approached comprehensively for how it can optimize an entire system-- including the humans within that system-- it has a higher chance of delivering meaningful impact.

The Global AI Agenda, an MIT report from March 2020, found that customer care was one of the top use cases for AI. 60 percent of executive respondents believe AI will play a role in 11 percent to 30 percent of their processes-- a considerable but not necessarily dominant influence on how most businesses operate.

Bots are a good place to start.

One of the fastest areas of adoption for AI in the enterprise is chatbot applications. It's often a good place for companies to get started with AI and see quick results. By 2024, Insider Intelligence predicts that consumer retail spend via chatbots worldwide will reach $142 billion-- up from just $2.8 billion in 2019. Back in 2018, pundits were heralding the death of chatbots because as text-based phone trees, they hardly provided a personalized or knowledgeable experience, and their impact was more frustration than a path to cost-savings -- and certainly not a mechanism for building brand loyalty. Today's bots use natural language understanding to translate requests to intent and AI-enabled knowledge to converse more naturally. Beyond enabling better conversations, chatbots are the key to richer conversational intelligence. Sometimes the interactions are very simple at face value but have a cascade effect that profoundly changes a series of customer experiences.

What customers really want is instant access to someone (or something) that understands what they need. Good bots are personalized, they know who you are and understand how to respond accordingly such as leveraging a customer's profile or transferring to the appropriate agent when needed. Self-service customer engagement is trending towards delivering that-- but companies need to work with a partner that can deliver at scale.

Supporting a growing AI-Native Workforce

These successes are the tip of the iceberg in an accelerating market for AI. Companies also need to expand the aperture in how success is measured against the human-side of the AI equation. Contact center employees are often a customer's primary point of interaction with a business. The volume of customer interactions agents handle has increased by nearly 20 percent on average and spiked 35-40 percent in some cases during the pandemic, according to a poll among Genesys Customer Advisory Board members. This puts tremendous pressure on agents and technology on the front lines of these interactions. In a recent Genesys study, agents identified their strengths. Over half of respondents classified thoroughness and completeness as their top abilities, while less than 10 percent thought empathy and listening were their greatest strengths. When looking at this through the lens of AI implementation there are two critical takeaways.

First, employees need systems that support a balance between complex tasks and easy to execute deliverables that satisfy a sense of accomplishment and completion of work at the end of a workday. AI that truly augments and considers human abilities needs to support users holistically and this means balancing high touch, high-level tasks with work that satisfies the need to mark off our list of to-dos at the end of the day.

Ultimately the goal is to make the work more rewarding for employees. Having the important infrastructure and insights needed to deliver better customer experiences can achieve this. Developers of AI applications must consider how it impacts not only the end-user speaking to an AI chatbot, but the employee partnering with AI to create a great brand experience and a great work experience.