March 2019

TechTidbit.com

brought to you by Tech Experts

What Are The Top Cybersecurity Trends For 2019?

Thomas Fox is president of Tech Experts, southeast Michigan's leading small business computer support company.

Several events in 2018 brought cybersecurity to the forefront of public consciousness, as major sectors– from financial institutions to Facebook– were affected by cybercrime.

According to Forbes, 34 percent of US consumers had their personal information compromised in 2018. Security experts and business leaders are constantly looking for ways to keep two steps ahead of hackers.

Cybersecurity trends for 2019 are a popular topic. Here is what's anticipated this year in the cybersecurity realm.

Tougher regulations

As digital capabilities are rapidly gaining a worldwide foothold, data is becoming our most highly-valued commodity.

Many governments are already recognizing the pressing need to protect citizens' personal information, especially amid mounting pressure from constituents who seek to hold companies accountable. This year will see the rest of the world follow suit, enacting laws that punish corporations and other entities that do not take data security seriously enough.

It's anticipated that such legislation will seek to ensure greater protection for connected devices (also known as the Internet of Things or IoT). These measures are also expected to set cybersecurity standards that reflect the value of the protected data.

Stiffer penalties

Enacting legislation is a step in the right direction, but appropriate consequences are usually needed to enforce it. The EU led the way in taking a firm stand against cybercrime with the GDPR. The Golden State followed with the California Consumer Privacy Act, which takes effect in 2020.

These initiatives establish considerable punitive measures for hackers. The UK required Equifax and Facebook to pay maximum fines as mandated by its data protection law. This year, it's predicted that several companies, such as British Airways, Facebook, and Google will come under intense scrutiny, and more jurisdictions are likely to enact stiff penalties– perhaps totaling as much as a billion dollars– for compromising data security.

Consistent data breach patterns

Cybercriminals primarily use email and compromised privileges to access consumers' personal data or engage in other illegal activities, and that trend is likely to remain the status quo in 2019. Businesses and other organizations are advised to put safeguards in place to control privileges and monitor emails, hyperlinks, and attachments.

Cyber weapon capabilities revealed

During the post-World War II era, nuclear war seemed to be the most imminent threat to national security. Today, cyber weapons are believed to carry the greatest potential for harm. Many governments have been developing their cyber arsenal for years, with some using their newfound capabilities to disrupt political systems.

Most of these clandestine efforts have been carried out behind closed doors. However, as the threat increases and countries are forced to fine-tune their tactics to defend themselves, they will likely bring their endeavors to light to create a deterrent.

Showing hostile governments what might happen should they choose to attack may prevent them from completely unleashing their digital demons– at least for a while.

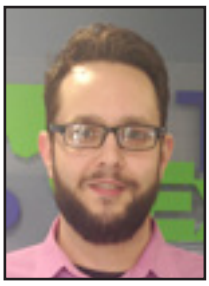
There will likely be outliers who will continue to launch cyber attacks, despite efforts to discourage them. Therefore, companies should

Continued on page 4

Many governments are already recognizing the pressing need to protect citizens' personal information, especially amid mounting pressure from constituents who seek to hold companies accountable. This year will see the rest of the world follow suit, enacting laws that punish corporations and other entities that do not take data security seriously enough.

Windows 10: New Issues Ahead Of The Spring Feature Update

"Polarizing may be the way to describe Windows 10 as people often love it or hate it, not much in between. It is my belief that this is due to the numerous issues, such as data loss via Windows update, broken software, and totally failed systems. Going forward, I don't think we'll see another OS quite like Windows 10 in the eyes of its users."



Jason Cooley is Support Services Manager at Tech Experts.

Windows 10 isn't as universally despised as Windows 8, but isn't as loved as Windows 7. Windows 7 actually had reported growth for the number of users last month, despite being released 10 years ago.

Polarizing may be the way to describe Windows 10 as people often love it or hate it, not much in between. It is my belief that this is due to the numerous issues, such as data loss via Windows update, broken software, and totally failed systems. Going forward, I don't think we'll see another OS quite like Windows 10 in the eyes of its users.

From an IT standpoint, not being able to install Microsoft Office after updating Windows is both annoying and baffling. Two products made by the same company, causing issues with each other. It seems like Windows 10 has a revolving door of problems. The latest issues are no exception. Recently, users attempted (and failed) many times to push the new Windows 10 updates to their system. This was met with a generic error that Windows can't communicate with the update server.

This seems minor in itself, but it's telling of a larger failure on Microsoft's part to do proper planning before implementing changes. While there has not been a clear report on what happened, Microsoft is ready to patch and fix its latest issue. There is, however, a work around if you can't wait for the newest update.

If you change your DNS to Google DNS or another third party DNS provider, you will be able to update Windows. While it is not confirmed, the common belief is that Microsoft sent out a bad DNS record to ISP's that caused this to occur. You can resolve it yourself, but Microsoft will be taking care of this broken update this week.

The other big news is the Spring update that is being prepared for deployment. Due to the previous feature updates causing many issues, you should delay your update as long as possible, if possible. If you don't know how to do this on your own, reaching out to an IT professional like Tech Experts could be the way to go.

The new update will feature many changes, most of which are cosmetic. This does not curb my fears for issues relating to the update. Although these types of changes normally only affect what you see on the screen, being extra cautious is probably the way to go.

Cortana and the search feature will now be completely separate, allowing you to use the standard start menu or Cortana individually. There will also be the option to uninstall many applications that you could not previously.

These include Mail, Calendar, Groove Music, Sticky Notes, and more. There will be many new themes and a few quality of life adjustments. While there will surely be more news on the horizon for the new update, do what you can to let them work out all of the issues before they become your issues as well.

Why You Should Consider VoIP For Your Business

A growing number of small businesses are switching from traditional landlines to VoIP (Voice over Internet Protocol) systems. While it can be an uphill task to overhaul the entire telecommunications system of any small business, it is definitely worth considering in light of the ever-increasing costs of traditional services. In fact, according to In-Stat, almost 79 percent of American businesses use VoIP phones, a 37 percent increase since 2009.

VoIP is a method of making phone calls using the internet as opposed to using typical landlines. VoIP services integrate IP phones, which look pretty much like traditional office phones, except they plug into an internet connection with an Ethernet cable.

Cost effectiveness
The biggest VoIP attraction is low cost. Since it is internet-based, hosted systems usually require little to no hardware investment apart from routers, Ethernet cables and the phones themselves, which are offered at reduced prices. According to estimates, the monthly service fees can run up to 40 percent less than traditional phone lines, and many providers offer monthly services with no long-term contracts.

VoIP is particularly cost-effective, if you have employees working from satellite offices or telecommuters. A telecommuter can take a VoIP phone home and make calls by plugging it into his home internet connection to make and receive calls on the company lines at no additional cost.

Other benefits
Certain VoIP service providers have introduced mobile apps that allow workers to make and receive phone calls on their mobile devices using the company phone numbers. Their privacy is therefore protected since they do not give their personal phone number. In addition, the company owns the line so if an employee leaves, calls are routed to the company rather than the employee's cell phone.

Drawbacks
While the mobility and scalability of VoIP systems are attractive features, there are some drawbacks to consider. For instance, since phones depend on an internet connection, if the connection fails, the phones would be dysfunctional. You can still as a precaution measure automatically drive incoming calls to voicemail or redirect them to the user's cell phone.

In addition, bandwidth problems could affect the quality of the calls made. If other office activities are consuming the greatest portion of bandwidth, calls will be filled with pauses and clicks, and dropped calls may also occur. There might also be extra charges for connecting to mobile phones or conference calling, and many VoIP providers don't offer 911 services or charge extra for it.

The future
The increase in VoIP adoption is undeniable, and analysts predict that it will become the predominant business phone service over the next decade.

Can Anyone Really Track Your Phone's Precise Location?

It's 2019 and everyone willingly carries a tracking device in their pockets. People can have their precise locations tracked in real time by law enforcement, the government, and advertising companies. It may sound like dystopian fiction, but it's a reality.

How law enforcement can track your location

AT&T, Sprint, and T-Mobile all sell data — including geographic locations associated with customer phone numbers — to a variety of sketchy third-party companies. This data, for instance, can be used by the bail bond industry to track people down, sometimes as accurate as a few hundred feet of their location. There's not much oversight and rogue bounty hunters have access to the data. And this isn't even a new problem.

Back in May 2018, The New York Times reported that this could happen. After the story broke, cellular carriers promised to do better. AT&T, Sprint, and T-Mobile have all promised to stop selling this data to aggregators. And it appears that Verizon already stopped before the New York Times story.

How the government can track your location

It's worth emphasizing that the government itself can still get access to your location data from your cellular company. They just need to get a warrant, then serve that to your cellular service provider.

If the technology exists, the government can get access to it with a warrant. It is quite a change from decades ago when the government had no way to track people's real-time locations with a device that's nearly always on their person.

The government doesn't even need to get your cellular company involved. There are other tricks they can use to pinpoint your location with even better accuracy, such as by deploying "stingray devices" near you. These devices impersonate nearby cellular towers, forcing your phone to connect to them.

How advertisers can track your location

It's not just your cellular carrier. Even if your cellular carrier perfectly safeguarded your data, it'd probably be very easy to track you thanks to the location access you've given to apps installed on your smartphone.

As innocuous as they may seem, Weather apps are particularly bad. You install a weather app and give it access to your location to show you the local weather. But that weather app may also be selling your data to the highest bidder. You likely didn't pay money for your weather app, so the developers will need to make money somehow to keep the lights and servers on.

The city of Los Angeles is currently suing the Weather Channel, saying that its app intrusively mines and sells its users' location data. Back in 2017, AccuWeather was caught sending its users' location data to third-party advertisers — even after updating the app to remove that feature.

It's best to avoid giving third-party apps access to your location. Stop using third-party weather apps and use your phone's built-in weather app instead.

How your family can track your location

Your phone is capable of determining its location and sharing it in the background, even if the screen is off.

You don't need to have an app open. You can see this for yourself if you use a service like Apple's "Find My Friends," which is included on iPhones. Find My Friends can be used to share your precise real-time locations with family and friends. After you give someone access, they can open the app, and Apple's servers will ping your phone, get your location, and show it to them. Of course, this is only with your permission, but it just shows how pervasive this technology is.

"It's 2019 and everyone willingly carries a tracking device in their pockets. People can have their precise locations tracked in real time by law enforcement, the government, and advertising companies. It may sound like dystopian fiction, but it's a reality."

Contact Information

24 Hour Computer Emergency Hotline
(734) 240-0200

General Support
(734) 457-5000
(888) 457-5001
support@MyTechExperts.com

Sales Inquiries
(734) 457-5000
(888) 457-5001
sales@MyTechExperts.com

Take advantage of our client portal!
Log on at:
www.TechSupportRequest.com

TECH EXPERTS

15347 South Dixie Highway
Monroe, MI 48161
Tel (734) 457-5000
Fax (734) 457-4332
info@MyTechExperts.com

Top Cybersecurity Trends For 2019? continued from page 1

do their best to be prepared– developing a proactive, rather than a reactive, strategy.

IoT working against us

Adding to our ever-increasing network of connected devices could have disastrous consequences. It's expected that cybercriminals will be able to program these devices to attack humans.

It may sound like the stuff of a dystopian sci-fi novel, but industry leaders predict that 2019 could well be the year that we see people using machines to target other humans to the point of causing great harm or even death.

Hackers, for instance, may set programmable thermostats to keep homes unbearably warm or cold, or intentionally cause navigation systems in self-driving cars to suddenly go awry, colliding with other vehicles or striking pedestrians.

These incidents could become so widespread that they span entire countries or transcend continents. For now, people still have some control over their devices. Unfortunately, however, more dire predictions are forecast when the day dawns that we surrender such control completely to artificial intelligence (AI).

Multiple layers of authentication

In the near future, you may need more than a password to log into your email, social media, and other Web-based accounts. Windows expert Susan Bradley reported to CSO that, "Only using a password to authenticate is increasingly leaving us open to phishing and other attacks."

As hackers become more adept at accessing your information, you may be asked to answer additional questions after supplying your password to verify that it's really you. As this will likely prove frustrating for most users, IT providers are seeking a simpler, more sustainable solution.

Of course, with the advancement of technology comes more sophisticated security measures too, so hopefully, these predictions will not be fully realized.

It makes sense though, to do everything possible to protect the integrity of your data and ensure that your team is on the same page about the security precautions you plan to take. It's also important to stay current on the latest legislation, standards, and technology to ensure that you're in compliance with applicable regulations and that you have the tools to provide continuous data protection.

Utilizing the right strategy will also help you adapt to new developments in data security without disrupting operations or leaving sensitive information vulnerable while you search for appropriate solutions.

What's The Difference Between Internet, Intranet, & Extranet?

The terms intranet, Internet, and extranet are often used interchangeably; however, there are some important differences between them. To better understand these differences, it is useful to look at the prefixes.

The prefix intra means within, inter means between, and extra means beyond. So how does this translate to online-based networks?

Basically, the Internet is an open entity that anyone in the world can access. It is open to everyone who has a working computer or device and appropriate Internet access.
An intranet is a private network that is typically limited to authorized users.

For example, most major organizations operate some form of intranet that only employees of the business can access and use. Intranets are usually employed to support a corporate culture and objectives and provide a platform on which employees can share information, communicate, collaborate, and network.

They are generally faster than the Internet because the information is stored on local network servers as opposed to being accessed from data centers throughout the world.

An extranet combines some elements of both the Internet and intranet. It is open to people both within and outside an organization; however, only people who have pre-arranged authorization can access it. An extranet is a restricted network that some, but not all, members of the public can access. A company may develop an extranet to create a mechanism by which it can connect with suppliers, customers, and other external agencies without making the content visible to the general public.