March 2020

TechTidbit.com

brought to you by Tech Experts

The Five Broad Categories Of The Cybersecurity Framework

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

One of the key methods that the NIST recommends businesses do on a continual basis is focus on these five categories as you assess your cybersecurity framework. These should be done regularly, and proactively, in order to be the most effective.

The categories are broad and cover a wide array of tools that businesses can use to build a cybersecurity framework that best supports their business security needs. They are: **identify, protect, detect, respond and recover.**

The first step you should take is to **identify** who should and should not have access to your business's privileged information, and then maintain strict physical access rules for those personnel who don't need that access.

NIST recommends that you do not allow cleaning and maintenance staff unsupervised access to rooms that contain computers or other technology that stores sensitive information.

Further recommendations include performing extensive background checks on all prospective employees, setting systems to lock down after several minutes of inactivity and maintaining separate accounts for each user.

The second category NIST mentions is to **protect**, which focuses on the ability to limit or contain the effects of a cybersecurity event.

Key recommendations include: limiting access to every part of the business information and systems, utilizing surge protector and uninterruptible power supplies, assigning a specific day of the month to perform patches for all software and regularly updating the firmware and operating systems for every system in your group.

Firewalls, securing your wifi, and training your employees on security best practices round up the extensive list in this category.

A key requirement to any cybersecurity framework is the proactive detection of a cyber event. Anti-virus, spyware or other malware programs can and should be installed on each of your systems.

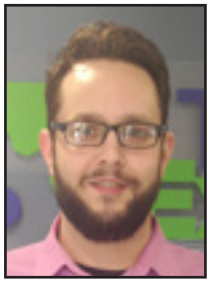
NIST recommends that you install two different programs from two different vendors for maximum security. You can even take it a step further and include Remote Monitoring and Management (RMM) Services as a part of your security protocol. RMM is an even bigger added layer of security in your ability to detect threats before they cause damage to your systems.

NIST recommends business develop a plan for the immediate **response** needed in the event of a natural disaster, fire or other event - the same applies to cyber

Continued on Page 4

A key requirement to any cybersecurity framework is the proactive detection of a cyber event. Anti-virus, spyware or other malware programs can and should be installed on each of your systems.

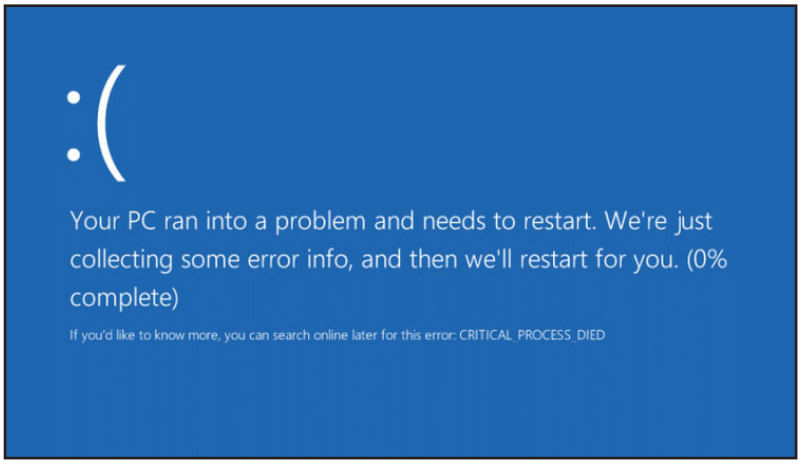
Windows 10 Issues Persist After Windows 7 Retires



Jason Cooley is Support Services Manager at Tech Experts.

January marked the end for Windows 7. After ten years and more than a few extensions, Microsoft finally made the cut-off and will no longer be updating what many would call its most reliable operating system ever.

Many businesses held out as long as possible, and some have even paid for privatized extended support.



Microsoft certainly had to split its focus while having more than one operating system in production, but with the end of Windows 7, one would assume that Windows 10 would have more developers working on the issues and updates as they arise.

It hasn't been long, but so far, we have not seen anything to indicate a brighter future for Windows 10.

Now, Microsoft is no stranger to a failed OS. Who can forget Windows ME (Millennium Edition), Windows Vista, and even Windows 8? These were deemed failures and had a much shorter life span than favorites like Windows XP and Windows 7.

That said, Windows 10 won't fall into the same category as ME, Vista, or Windows 8. Windows 10, when correctly functional, really is one of the better user experiences there has been. It has already proven commercially to be more successful with a larger market share than any of the failed systems.

Of course, that could also be attributed to the fact that there was another OS available at the times of ME, Vista, and Windows 8. Windows ME couldn't break the grasp that Windows XP had. Vista was a victim of Windows XP and Windows 7. Windows 8 was decimated by Windows 7 and Windows 10.

Windows 10 from a user standpoint is not a failure, but there are a few ways that it exceeds the issues that some of these failed operating systems had.

Windows 10 has had some fairly widespread issues. The most recent problem? A majority of Windows 10 users found themselves unable to use the search feature in Windows. The start menu would allow you to open it, but the search never returned results.

Microsoft was able to fix the issue within a day or so, but what caused the issue?

The broken search was related to a broken link to Bing search. The search function is integrated with Bing, and the functionality of the feature was completely broken because of it.

There have been other issues as well. One of my favorite and most unique problems with Windows 10 was a few month span during an entire feature update where Microsoft had broken the ability to install Microsoft Office.

There was no fix. If the problem occurred, you had to either roll back to install Office or wait until the next feature update.

You almost expect there to be issues with third party software during a new update, but when it's the company's own product? It is definitely a headscratcher. Relatedly, there were frequent problems with Office activation and the Microsoft store being completely missing or broken.

While Windows 7 didn't have all of the features that Windows 10 did, it seemed to be much more reliable.

We can only hope that Microsoft gets those extra developers working so Windows 10 can be as reliable as its predecessor. Despite these issues, the potential is there.

Ransomware Attacks On Healthcare Providers Rose 350% In Q4 2019

Ransomware assaults against healthcare providers expanded an astounding 350 percent during the last quarter of 2019 with the quick pace of assaults previously proceeding all through 2020.

Ransomware attacks dominated healthcare headlines during the later part of 2019 with attacks on IT vendors disrupting services on hundreds of dental and nursing facilities, while a number of hospitals, health systems, and other covered entities reported business disruptions from these targeted attacks.

Also, in December, Blackberry Cylance specialists revealed that another ransomware variation known as Zeppelin was spotted focusing on the human services division and tech associations through the supply chain.

IT research group Corvus broke down the ransomware attacks of the last few years to get a feeling of malware's effect on the part and its assault surface and discovered there were in excess of 24 announced ransomware occurrences a year ago.

These findings mirror similar reports, which also noted that these numbers are likely lower than the actual number of attacks – as some ransomware victims do not report the incidents to the public.

In fact, Emsisoft research shows that more than 759 healthcare providers were hit with ransomware last year, reaching crisis levels.

Further, the trend has continued in 2020 with at least four healthcare covered entities reporting attacks in January alone. According to Corvus, the number is more than any other quarter in healthcare since Q3 2017. And if the rate continues, there will be at least 12 reported during Q1 2020.

The researchers also found that healthcare actually has a smaller attack surface, on average, than the web average. Those that have reduced their overall exposure, especially hospitals, have limited the risk of exposure.

But health services and medical groups are the most at risk in the sector, according to the data.

That's not to say that healthcare is successfully securing its attack surface. For example, one of the most common exposure types is through the remote desktop protocol, which is associated with a 37 percent greater likelihood of a successful ransomware attack.

Healthcare is also struggling to secure its email security, overall. Eighty-six percent of healthcare covered entities don't use scanning and filtering tools on their email platforms. Even hospitals, which typically leverage these services at a higher rate, are failing to deploy this tool at a successful rate (just 25 percent use the tech).

What's more, health practitioners, such as dentists and physicians are 14 percent less likely on average to use the most basic form of email authentication, which are known to prevent suspicious emails from making it to the inbox.

It's concerning, as Corvus showed that more than 91 percent of ransomware attacks are the result of phishing exploits.

"Hospitals use email scanning and filtering tools more than average, but the average is low," researchers wrote. "These services are associated with a 33 percent reduction in the likelihood of a ransomware attack. All healthcare entities should strongly consider

Continued on page 4

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

Ransomware Attacks On Healthcare Providers Rose 350% In Q4 2019, continued

such services to help prevent phishing."

Corvus also found that hospitals are six times more likely to internally host their own servers, instead of leaning on a third-party vendor. As a result, those entities have "the responsibility for maintaining some aspects of security in their court: keeping up with the everchanging threats rather than handing it off."

"As commodity ransomware has become more readily available and examples of successful attacks on smaller organizations, like local governments, gain attention, attackers may well turn their attention to organizations like individual health practitioners or nursing/long-term care facilities," researchers wrote.

"We can see that the security measures at these kinds of organizations are average at best, and in some areas worse," they continued. "Healthcare organizations of all sizes are at risk… They should be taking advantage of opportunities to improve email security."

As the number of successful ransomware attacks increased, several industry stakeholders released guidelines to help organizations shore up their defenses, including the Department of Homeland Security, Microsoft, NIST, and the Office for Civil Rights. Healthcare organizations, especially those with limited resources, should turned to these insights to bolster their defenses.

Lastly, the FBI has continually reminded organizations that they should not pay the ransom for a host reasons, including that there is no guarantee the hackers will unlock the data and the threat actor may launch a subsequent attack.

Ransomware attacks have cost the healthcare sector at least $160 million since 2016, according to Comparitech.

This article was adapted from research published by Health IT Security.

The 5 Broad Categories Of The Cybersecurity Framework, continued

attacks. Businesses should develop a cyber attack response plan that includes details on the roles and responsibilities of certain employees, what to do with information systems in the event of an incident, who to call, and what constitutes a cyber event.

Furthermore, NIST recommends you do this at an employee level, letting each employee know what his or her role will be in the event of a disaster.

The last category NIST defines is **recover.** NIST has 4 recommendations as to a process to use to help your business recover with minimal damage should an attack occur. They are:

- Make full backups of all business data monthly either on an external hard drive (stored in a different location), or online cloud storage
- Make automatic incremental backups of important data, and store them in three different ways: removable media such as an external hard drive, a separate isolated server, and cloud backup and online storage from a cloud provider.
- Utilize Cyber Insurance - cyber, like health, auto, or business insurance, can help your business recover both physically and financially if a cyber event were to occur.

  Some cyber insurance providers even offer cybersecurity experts who can further help you identify where, what and how you are vulnerable and give suggestions on how to fix those insecurities.
- Conduct regular assessments of processes, procedures and technologies and make corrections or improvements as necessary.

Cyber attacks are a real and present danger to your business, but you can mitigate the risks by following the above suggestions.