the NetWork LeadingIT
Chicagoland CybersecurITy Support
October 2021

# Cybersecurity Awareness Month

## White House Memo Urges Business Leaders To Increase Cybersecurity

## Invest In Cybersecurity Or Risk Closing Down

## How Multi-Factor Authentication Increases Your Defense Against Cyber Crime

## Do You Know Your "Cyber Credit Score"?

GoLeadingIT.com (815) 496-6300 @leadingit @leadingit-solutions

# White House Memo Urges Business Leaders To Increase Cybersecurity

As cybersecurity experts are still trying to unravel the recent Colonial Pipeline and JBS meatpacking company hacks, the White House urges all U.S. organizations to beef up their ransomware prevention measures. These warnings come in the wake of the Department of Homeland Security announcing revised cybersecurity requirements for pipeline companies.

### Ransomware Attacks Are on the Rise

According to Reuters, ransomware attacks have significantly increased in frequency and impact over the last few months. While confirming this, Anne Neuberger, the cybersecurity advisor at the National Security Council, released a public memo advising businesses to take ransomware hacks more seriously. The notice partly read, "The threats are serious, and they are increasing." However, the increment in the frequency of ransomware attacks did not come as a surprise. This is because the COVID-19 pandemic provided some sort of hacker's paradise. Most organizations hurriedly implemented half-baked work-from-home models without critically evaluating their long-term cybersecurity impacts. As a result, we've seen employees carry more corporate gadgets to less-secure home-office environments where they're more exposed to compromise. Even worse, some organizations allowed staff to connect their personal gadgets to corporate networks to facilitate remote working. These devices do not have the same level of protection as company-given gadgets, hence provide an easy backdoor to your systems.

### Ransomware Attacks Are Becoming More Complex

Initially, ransomware attacks were simple breaches where hackers encrypted personal devices and demanded a few bucks as ransom. Over the years, cyber actors have continually advanced their trade by targeting businesses using more complex tactics and demanding bigger ransoms. Last year saw a tremendous increase in supply chain attacks where hackers targeted several organizations simultaneously.

### Ransomware Attacks Threaten Core Business Functions

A typical ransomware breach involves hackers compromising your network, accessing and encrypting your files and data, and then demanding a ransom to restore access. Even with the evolution of cyberattacks, this technique hasn't changed that much. Ransomware attackers still primarily focus on unauthorized access and stealing of corporate data. However, going by the recent Colonial Pipeline and JBS meatpacking company breaches, the nature of ransomware attacks might change soon. Hackers no longer only focus on data theft. They also seek to deliberately disrupt normal operations by denying businesses access to critical files, slowing down networks, or shutting them altogether. Such interruptions are usually very costly, and any company would stop at nothing to avert or thwart them—including paying hefty ransoms. Bad cyber actors are aware of this and are using it to coerce companies into hastily paying ransoms. As it seems, this tactic works pretty well for them—JBS paid a ransom of over $11 million and the Colonial Pipeline over $5 million to Russian-based hackers in attacks just one month apart.

Continue reading: goleadingit.com/blog.

# Invest In Cybersecurity Or Risk Closing Down

The internet has enabled businesses to reach broader markets and enhance efficiency through computer-assisted automation. Initially, most businesses only invested in cybersecurity to enhance consumer confidence or abide by data privacy standards. Cybersecurity is no longer an auxiliary add-on; it is a necessity. Here's why:

"60% of Small Businesses Die Within Months of a Cyberattacks"

Most cyberattacks happen to small and medium-sized companies, and 60% of them close within six months of a hack or breach. In the U.S, 43% of organizations that suffer catastrophic data losses do not reopen, and 51% run out of business within two years. So, why are cyberattacks so severe?

**1. Cyberattacks Are Expensive**

Data theft is a bigger concern for modern-day organizations than physical thefts. Typically, cyber attackers gain unauthorized access to your systems and steal or encrypt your data. They will then demand ransom in exchange for not publishing the information or for restoring your access. The average ransom fee is about $200,000, and the total cost of recovering from a cyberattack is approximately $3.86 million. Unless you're operating a multinational company that posts millions in returns per day, a single cyberattack is enough to bring your business to its knees.

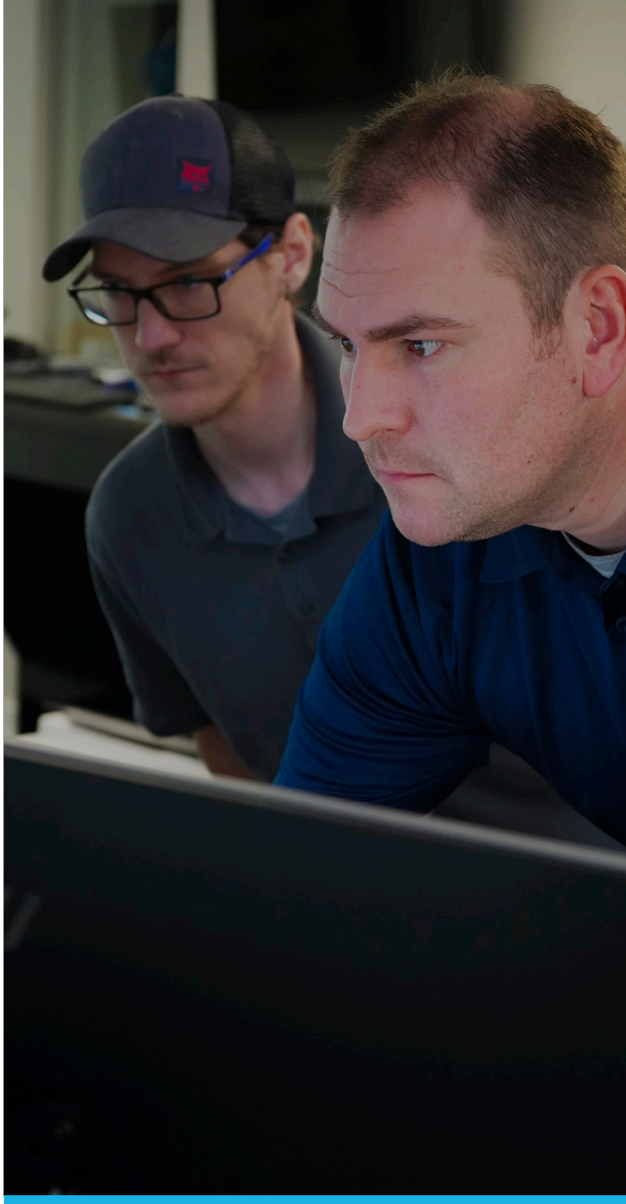
**2. They Stall Operations**

Based on the recent hacks, cyber attackers seem to focus more on disrupting operations than on stealing data. Let's take the recent Colonial Pipeline hack, for example. The ransomware attack forced the company to shut down its entire gasoline pipeline system for almost a week after hackers gained access to their networks. According to Colonial's Chief Executive Officer, Joseph Blount, that was "absolutely the right thing to do" because they didn't know the attackers or their motives. Over 90% of businesses that lose their data centers for ten days or more go bankrupt in less than one year. Bad cyber actors are using this to scare organizations into paying the ransom.

**3. Cyberattacks Are Bad for Your Reputation**

The modern consumer is very cautious about how you obtain, store, and use their data. They expect you to safeguard whatever information they trust you with, whether it's their credit card credentials, purchase histories, logins, name it. If you cannot meet this expectation by falling prey to hackers, you lose their trust. This can result in loss of customers, both present and prospects. For instance, Facebook lost a significant chunk of its active users after the 2019 Cambridge Analytica Scandal. According to Mixpanel, the tech giant's posts, likes, and shares dropped by approximately 20%. While Facebook survived the reputational damage, that's not always the case, especially for SMBs that don't have the same financial muscles to bounce back.

Continue reading: goleadingit.com/blog.



Throughout this Cybersecurity Awareness Month, we want to make one thing clear:

Cybersecurity begins with the basics. As you plan to roll out the latest intrusion detection and prevention technologies, do not overlook the simple data security best practices.

# How Multi -Factor Authentication Increases Your Defense Against Cyber Crime

If you've found yourself prompted for a second form of authentication when you log into a website or an app, you've experienced the wonders of multi-factor authentication (MFA).

### What is Multi-Factor Authentication?

Multi-factor security requires more than one form of identity verification from users. According to SearchSecurity, multi-factor authentication typically combines two or more of the following independent authentication factors, per Search Security and Security Boulevard:

- Something the user knows, like a password
- Something the user controls, like a security token
- Something that is part of the user, like fingerprint verification
- Where the user is (location)
- A specified window of time assigned to the user for authentication

Many implementations of multi-factor authentication are limited to two from the above list, which is why you may also see MFA referred to as two-factor authentication (2FA). Using more than one kind of credential to verify identity ensures the authentication process's security even if one of the factors ends up compromised.

Continue reading: goleadingit.com/blog.

# Do You Know Your "Cyber Credit Score"?

With cyber attacks on the rise, insurance companies are starting to audit and review customers with a cybersecurity credit score to better assess your risks to them. Using an outside-in approach, organizations are being rated for their cyber standards.

Insurance companies may raise your rates, or in some cases cancel your policies based on these new ratings. LeadingIT's all-inclusive service gives clients the peace-of-mind that their systems are secure, backed-up, tested regularly and thereby insurable.

Please contact us today if you have any questions regarding your cybersecurity credit score.


## WE ARE CELEBRATING!

### Anniversaries

Devin Lindelof - October 5, 2020

### Birthdays

Garrett McCleary - October 5th

Martin Blair - October 16th

Read Our Blog For More: https://www.goleadingit.com/blog

LeadingIT