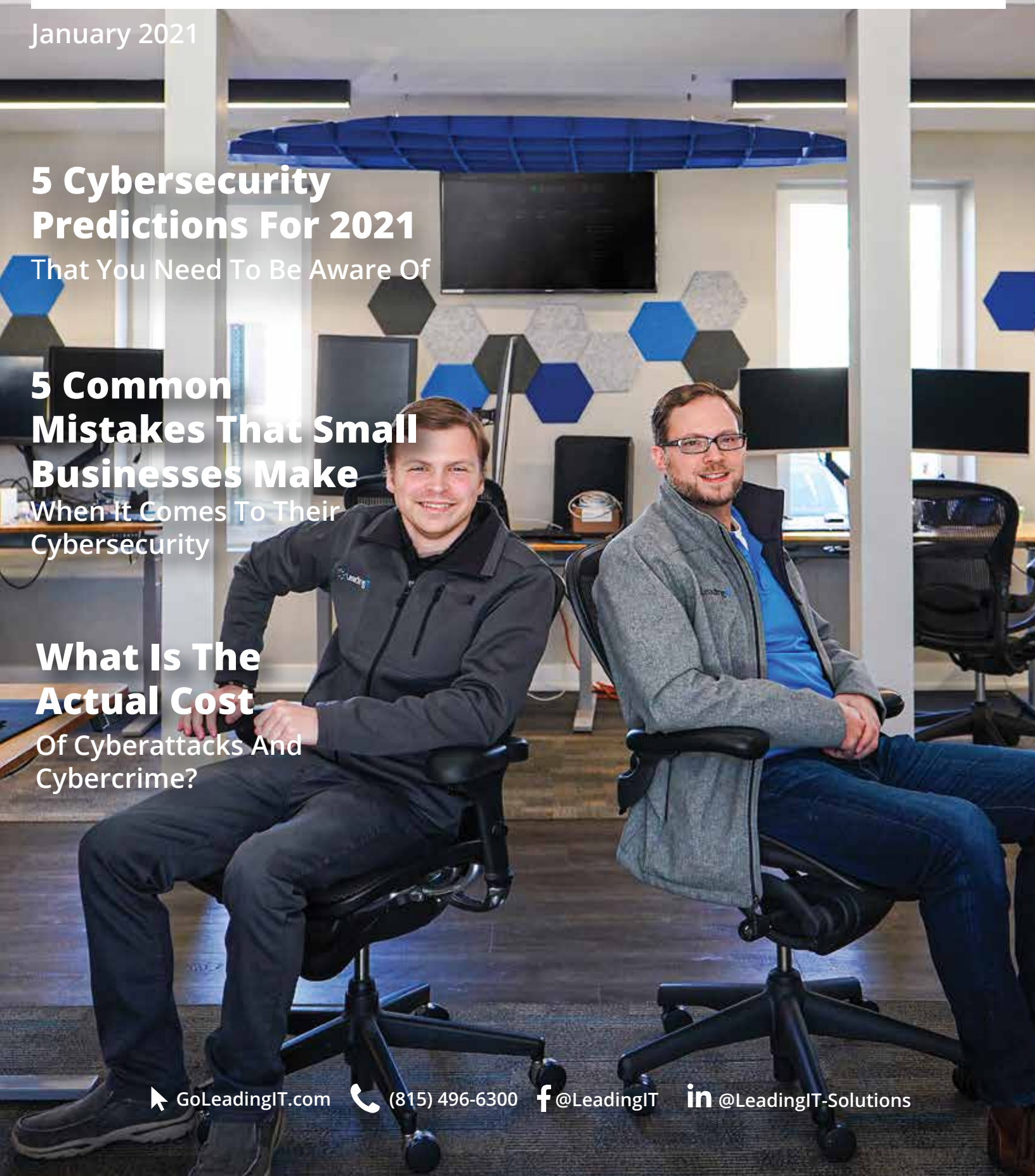
The NetWork

LeadingIT

Chicagoland CybersecurITy Support

January 2021



5 Cybersecurity Predictions For 2021

That You Need To Be Aware Of

5 Common Mistakes That Small Businesses Make

When It Comes To Their Cybersecurity

What Is The Actual Cost

Of Cyberattacks And Cybercrime?

GoLeadingIT.com (815) 496-6300 @LeadingIT @LeadingIT-Solutions

5 Cybersecurity Predictions For 2021 That You Need To Be Aware Of

How different will the cybersecurity landscape be for your Chicagoland organization in 2021? Here are our top five predictions to help you prepare for the future:

1. Ransomware Will Increase In Both Scope And Severity

Ransomware has rapidly grown to be one of the most prevalent cyber-attack vectors in the last few years. This trend will continue in 2021 and beyond.

According to Cybercrime Magazine, ransomware attacks will occur every 11 seconds in 2021, an increment from every 14 seconds recorded in 2019.[1] Even if businesses invest more in protecting their computers from ransomware, there's no guarantee that bad cyber actors will move to other vectors. That's mainly because ransomware has proved to be quite an effective form of attack.

To be on the safe side, you must implement more cybersecurity protocols around spam filtering and web filtering.

2. Cybercriminals Will Focus More On Remote Workers Throughout 2021

COVID-19 forced many businesses to allow their employees to operate remotely. The result is more workers using several gadgets across many less-protected home-office environments. For cybercriminals, this is a "hacker's paradise."

Statistics from Malwarebytes show that up to 25% of organizations have grappled with malware attacks and other data breaches due to the mobile workforce's vulnerabilities.2 If businesses do not reimagine their cybersecurity approaches, we can only expect a surge in incidences where cyber attackers exploit mobile workers as entry points to corporate networks.

4. Accelerated Digital Transformation And Increased Internet Access Will Spur More Data Breaches

It's almost impossible to look back into 2021 and identify any positive highlights. Well, unless we look at it from an information technology perspective. The stay-at-home orders inspired many businesses to increase their digital transformation efforts. With several people staying indoors, the number of active internet users has risen to almost 4.6 billion (Statista).[4]

5. Consumption Of IoT Managed Security Services Will Increase Fivefold

Demand for managed security services has been on the rise for several reasons. First, the cyber threat landscape has increasingly evolved in complexity. Besides, most in-house IT experts were accustomed to offering on-premise support, which is not viable under the current circumstances.

It's not any different in the IoT security space; there's an influx in BYOD and company devices being used away from the safe in-office environments. And the truth is, most internal IT teams are ill-equipped to offer remote support. That's why, according to Gartner, the demand for IoT managed security services will increase by 500% in 2021.[7]

Let Experts Handle Cybersecurity For Your Chicagoland Business

2020 was not one of the best years in cybersecurity, and 2021 may be worse. But it doesn't have to be – the trick is to work with a seasoned IT company with a deep bench of professionals.

Sources:

[1]https://cybersecurityventures.com/top-5-cybersecurity-facts-figures-predictions-and-statistics-for-2019-to-2021/

[2]https://resources.malwarebytes.com/files/2020/08/Malwarebytes_EnduringFromHome_Report_FINAL.pdf

[3]https://phoenixnap.com/blog/what-is-data-breach-how-to-prevent

[4]https://www.statista.com/statistics/617136/digital-population-worldwide/

[5]https://pages.bitglass.com/CD-FY20Q2-RemoteWorkforceReport_LP.html?&utm_source=pr

[6]https://www.ic3.gov/Media/Y2020/PSA200401

[7]https://www.i-scoop.eu/internet-of-things-guide/growth-iot-managed-security-services-market/

5 Common Mistakes That Small Businesses Make When It Come To Their Cybersecurity

Your small business relies on your networks and computers for its day to day operations. You use them to communicate with clients and vendors, store sensitive client data, and make vital business decisions. For this reason, you need to employ the highest standard of cybersecurity to protect your system. Unfortunately for small businesses, cybersecurity is not a matter that is given priority.

1. Underestimating Your Vulnerability To Cyber Attacks

Most small businesses assume that only large corporations are susceptible to cyber threats. Well, this is not the case. The reality is that both small and large companies in virtually every industry are susceptible to cyberattacks. According to a report by The Manifest, 15% of small businesses were victims of cyberattacks.[1] 5% of small businesses were victims of virus attacks, 7% were victims of hacks, and 3% were victims of data breaches in 2019.[2] Cybersecurity Ventures predicts that by the year 2021, businesses will fall victim to ransomware every 11 seconds, and cyberattacks will cost them more than 6 trillion US dollars annually.[3]

While this is proof that small businesses are also vulnerable to cyberattacks, it also serves as a caution to other small businesses to take appropriate cybersecurity precautions.

2. Relying Solely On Your Default Security System

Whether you are using Macs or PCs, your default security system isn't robust enough to protect your business. For example, Windows Security is known to have weaker malware detection rates compared to other leading antivirus programs and has proven poor performance in hands-on phishing protection tests. The dissatisfactory performance of Windows Security is alarming for many business executives because of the frequent discovery of cybersecurity vulnerabilities in the operating system.

While Macs were thought to be traditionally more secure than PCs due to the limited malware developed for the operating system, cyber threats against Macs are growing by the day.
With all this in mind, your best defense is installing an antivirus program or software that offers real-time protection and safeguards your sensitive data from cyber threats.

3. Depending On Free Antivirus Software

You wouldn't lock your house with a low-cost padlock, so why would you secure your sensitive data using free antivirus software? Why shouldn't you use free antivirus software?

• Free antivirus programs provide low detection rates.
• Leading free antivirus software violates your privacy by harvesting data about your usage.
• The most downloaded free antivirus software issue false positives to appear efficient.
• Several free antivirus software carries intrusive ads and malware.
• The most popular free antivirus programs suffer from cyber threats making them counterproductive to use.

In today's changing cyber threat landscape, using free antivirus software is not sufficient to prevent advanced and persistent attacks. Actually, using free antivirus software will cost your organization in the long run. You'll ultimately find yourself experiencing downtime or scrambling to find solutions once your system is already compromised.
Maintaining an extensive security system that prevents malware and malicious downloads and offers quick malware detection requires resources.

4. Relying On Outdated Software

Your organization should use full proof and high-end programs to protect its servers and networks. Most small businesses overlook the importance of updated software, thus exposing themselves to cyberattacks. Updating software is one of the most efficient ways to keep cybercriminals at bay. As technology keeps on advancing, so do cyber threats, and in most cases, these threats evolve faster than companies can update their cybersecurity controls.

The best way to protect your system from hackers is to update your cybersecurity software regularly. You should implement policies to ensure that all your software is timely updated.

5. Not Being Proactive

It is far less expensive to prevent a cyber-attack than it is to recover from one. It's crucial to think of proactive approaches rather than reactive approaches when managing your organization's cybersecurity. Proactive cybersecurity refers to methods used to prevent cyberattacks. These methods include:

• Endpoint and network monitoring
• Cybersecurity training
• Cyber threat hunting

Developing a comprehensive cybersecurity policy is your best chance of ensuring your cybersecurity controls are standard, keeping malicious actors on at bay, and preventing your business from making these common mistakes.

Sources:
[1]https://themanifest.com/mobile-apps/data-safety-small-businesses-2020-cybersecurity-statistics
[2]https://www.prnewswire.com/news-releases/15-of-small-businesses-experienced-a-cybersecurity-threat-last-year-but-majority-show-desire-to-increase-cybersecurity-resources-301046022.html
[3]https://cybersecurityventures.com/cybersecurity-almanac-2019/
https://theiabm.org/top-5-cybersecurity-mistakes-companies-make-avoid/
https://businesstown.com/common-cybersecurity-mistakes-small-businesses-make/
https://smallbiztrends.com/2020/11/cybersecurity-mistakes.html
https://business.infostot.com/2020/11/the-5-major-cybersecurity-mistakes-to.html
https://consoltech.com/blog/5-common-mistakes-cyber-security/
https://analyticsindiamag.com/windows-vs-macos-vs-linux-for-cybersecurity/

What Is The Actual Cost Of Cyberattacks And Cybercrime?

How vulnerable is your company to a cyberattack? A cyberattack can cost your business millions in downtime and lost productivity. According to the 'Evil Internet Minute' report released by RiskIQ, by 2021, cybercrime will cost the globe an average of 11.4 million U.S. dollars per minute.[1]

What Is The Impact Of The Pandemic On Cybercrime?

VMware conducted a survey to find out what impact COVID-19 had on the cyber-attack landscape.[2] The survey involved more than 1000 respondents from Singapore, the United Kingdom, the United States, and Italy. The survey reported that 88% of U.S. cybersecurity professionals said attack volumes have increased as more employees work remotely. 89% said their organizations had experienced cyberattacks linked to COVID-19 malware.

Researchers from NormShield looked for websites using the names of the ten commonly used drugs over the last several months.[3] They found a dramatic spike in the number of websites generated to get the attention of anxious shoppers looking for a coronavirus vaccine. According to research by McAfee, the United States ranks first among countries with malicious detections.[4]

The First Quarter Of 2020 Saw An Increase Of 25% In Ransomware Attacks

Specialist insurer Beazley reported an increase of 25% in ransomware attacks in the United States during the first quarter of 2020 compared to the last quarter of 2019.[5] Industries mainly affected by the cyberattacks were the healthcare sector, the manufacturing sector, and financial institutions.[6]

Examples of these cyberattacks include:

1. Phishing emails announcing a COVD-19 vaccine.

2. Reference links to websites that are infected with malware.

3. Fake landing pages allegedly showing the latest Coronavirus infection rates.

Cyberattacks have had devastating effects on businesses such as:

• Disruption and seizing of business.

• A damaged business reputation leading to loss of clients and decreased sales and profits.

• Lawsuits from affected clients.

How Can You Enhance Your Organization's Cybersecurity?

It is far less expensive to prevent a cyber-attack than it is to recover from one. It may take you months or even years to fully recover from cyberattacks. Your Information Technology infrastructure is very vital to your day to day business operations.

The following are cybersecurity controls that you should implement to enhance your cybersecurity:

1. Installation of security software such as antivirus programs on your computers and systems to detect and remove malicious programs.

2. Implement robust user authentication processes such as complex passwords, two factor and multi-factor authentication methods, and biometric authentication.

3. Enable email spam filtering to filter out incoming emails for phishing content and automatically move them to a separate folder.

4. Secure mobile devices used by employees through encryption, password protection, and enabling the 'remote wiping' option:

5. Implement firewalls to establish a barrier between your internal network and incoming traffic from external sources to block malicious traffic.

6. Implement cybersecurity awareness training programs to train your employees on what to look out for to distinguish phishing emails.

Sources:

[1]https://www.riskiq.com/resources/infographic/evil-internet-minute-2020/

[2]https://ir.vmware.com/websites/vmware/English/2120/us-press-release.html?airportNewsID=85da6289-ab5e-40e²-86f7-d2b731b0dc93

[3]https://www.helpnetsecurity.com/2020/04/10/covid-19-fears/

[4]https://www.mcafee.com/enterprise/en-us/lp/covid-19-dashboard.html

[5]https://www.globenewswire.com/news-release/2020/06/09/2045639/0/en/Beazley-Breach-Insight-Ransomware-rises-25-in-Q1-2020.html

[6]https://www.theguardian.com/society/2020/oct/28/us-healthcare-system-cyber-attacks-fbi

https://www.securitymagazine.com/articles/93195-report-shows-114m-lost-globally-every-minute-to-cybercrime

https://www2.deloitte.com/content/dam/Deloitte/ng/Documents/risk/ng-COVID-19-Impact-on-Cybersecurity-24032020.pdf

https://think.taylorandfrancis.com/special_issues/covid-19-cybersecurity/

https://www.brosix.com/blog/challenges-of-telecommuting/

https://www.ey.com/en_be/covid-19/why-remote-working-will-be-the-new-normal-even-after-covid-19

WE ARE CELEBRATING!

Anniversaries
Stephen Taylor
January 1, 2010

Birthdays
Dave Gregory
January 7

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