the NetWork

LeadingIT

Chicagoland CybersecurITy Support

March 2022

Invest in Cybersecurity or Pay More for Insurance Premiums

Is Your Organization Making These Three Critical Mistakes?

Get the Most Out of Your 2022 Cybersecurity Budget

LeadingIT Acquires Dura-Tech Enterprises Further Expanding Chicagoland Presence

Welcome to the Team!

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

Invest in Cybersecurity or Pay More for Insurance Premiums

As cyberattacks continue increasing in volume and severity, cyber liability insurance providers are getting keener on organizations' security postures. The stronger your intrusion detection and prevention systems are, the cheaper your policy is likely to cost. Some insurance carriers may even cancel your policy if they think you don't have sufficient cybersecurity measures.

You must have heard of the school district that published an over 334% increase in its cyber liability insurance costs. It was the forefront topic in almost every cybersecurity news site late last month. This dramatic rise in premiums from $6,661 in 2021 to $22,229 this year didn't come as a surprise to some people. There has been a continuous spike in costly breaches that have disrupted business operations across the country. Naturally, carriers must increase their coverage costs and enforce more stringent qualifications or risk running at a loss. We all know that the latter is not an option.

How Does Cyber Insurance Work?

To help you understand why the lack of elaborate cybersecurity systems and protocols can increase your cyber policy costs, let's first look at how cyber insurance works. Cyber liability insurance coverage, popularly known as cyber insurance, is a policy that shields you from the costs of cyber incidents. Most carriers offer them as supplements to standard property policies, but you can also acquire them separately.

Depending on the carrier, a policy may cover anything from loss of company data to ransomware payments, downtime costs, arising legal expenses, and any other breach-related losses. They operate like standard insurance covers—if the bad guys infiltrate your systems and compromise your files or operations; you claim compensation for the arising losses.

Why Is Your Cybersecurity Posture Crucial to Insurers?

As you must have realized, policy providers bear all the financial losses from cyberattacks. So, the more vulnerable your systems are to breaches, the more the payouts from the insurer.

According to The Ponemon Institute, the average cost of a data breach in 2013 was about $136.00. Today,

Left to right: Steven, Dale, Nathan, Peter, Eric

IBM estimates that breach incidents cost organizations about $3.86 million, meaning that insurance carriers now pay out nearly thirty thousand times what they'd paid less than a decade ago. No wonder the cyber liability insurance market recorded an average loss ratio of 103% last year.

To survive, the cyber insurance industry has to do one thing: Tighten qualification requirements and become more stringent on organizations' implementation of proper cybersecurity layers. That explains why MFA is now mandatory.

MFA is a requirement in order to qualify for cyber insurance coverage

Given that ransomware accounts for almost half of all insurance claims, ransomware prevention can help carriers reduce their exposure.

Continue reading: goleadingit.com/blog

Pictured on the cover, left to right: Jeremiah, Steven, Peter, Eric, Nathan & Dale

Is Your Organization Making These Three Critical Mistakes?

Recent research by Verizon shows that over 86% of data breaches are financially motivated. A similar study by CSO Online estimates the average cost of each cyberattack to be about $3.9 million. According to IBM, this figure could be as high as 8.64 million in the U.S. The bad news is that almost 70% of business executives feel that their cybersecurity risks are increasing by the day. What do these figures mean for your Chicagoland organization?

All evidence points to one thing—cyberattacks are expensive, and they're getting costlier and more severe. You've probably heard this a million times. Right? The irony, however, is that even though everyone knows that the global cybersecurity situation is continually worsening, Varonis approximates that only 5% of company folders have proper protection. Most people still overlook standard data security practices like password expiration and complexity protocols, MFA, regular network assessment, and employee cyber awareness training.

> "**Human error accounts for 95% of all data breaches.**"

We cannot overstate the risks you're exposing your organization to by not taking cybersecurity seriously. Here are a few common mistakes, their risks, and tips to avoid them:

1. Failure to Train Employees on Cybersecurity Awareness

Most organizations focus on shielding their systems from external interference and disregard internal threats. Your staff is the most crucial defense line in the war against cybercrime and your weakest link. Even with the most advanced ransomware prevention technologies, your network isn't safe if your employees lack proper cybersecurity training.

2. Not Deploying Multi-Factor Authentication

Multifactor Authentication adds an extra cybersecurity layer beyond your passwords. MFA is no longer a luxury; it's one of the essential cybersecurity solutions every business should have.

Continue reading: goleadingit.com/blog

Get the Most Out of Your 2022 Cybersecurity Budget

It's almost impossible to scan through any news website today without finding an article on a recent data breach. And in each publication, you'll read about how the breaches inconvenienced and devastated the affected businesses.

Cyberattacks are inarguably every modern-day business leader or owner's most significant concern. The constant barrage of breaches makes cybersecurity integral to the survival of any organization. Budgeting to keep your files and IT infrastructure safe does not differ from setting funds aside for regular utilities like electricity—it's something you cannot simply avoid.

3 Reasons Your Organization Needs a Cybersecurity Budget

You must have heard of the famous Charles Duncan McIver's quote—If you think education is expensive, try ignorance. The same applies to cybersecurity; you only realize how inexpensive data security is once you understand the potential losses from not taking it seriously. Here are some reasons you need a cybersecurity budget:

1. 60% Of Businesses Go Out of Business After a Cyberattack
2. Cybersecurity Protects Your Brand Image
3. Small Businesses Are a Top Target for Criminals and Represent 43% Of All Breaches

Plan Your Organization's 2022 Cybersecurity Budget

Don't let the cost factor prevent you from budgeting for IT. You don't have to handle all cybersecurity solutions in-house. The less inexpensive option is outsourcing managed IT services. An IT support services provider can deliver all the IT solutions your business requires at a fraction of what you'd need to handle it internally. Outsourcing not only helps you budget less but also frees you to concentrate on other business-centric tasks.

Welcome to the Team!

We are excited to introduce the newest edition to the LeadingIT staff. Nathan joins us as a level 1 technician.

Nathan

WE ARE CELEBRATING

Birthdays

Anthony Gallardo - March 4th
Steven Brimeyer - March 12th

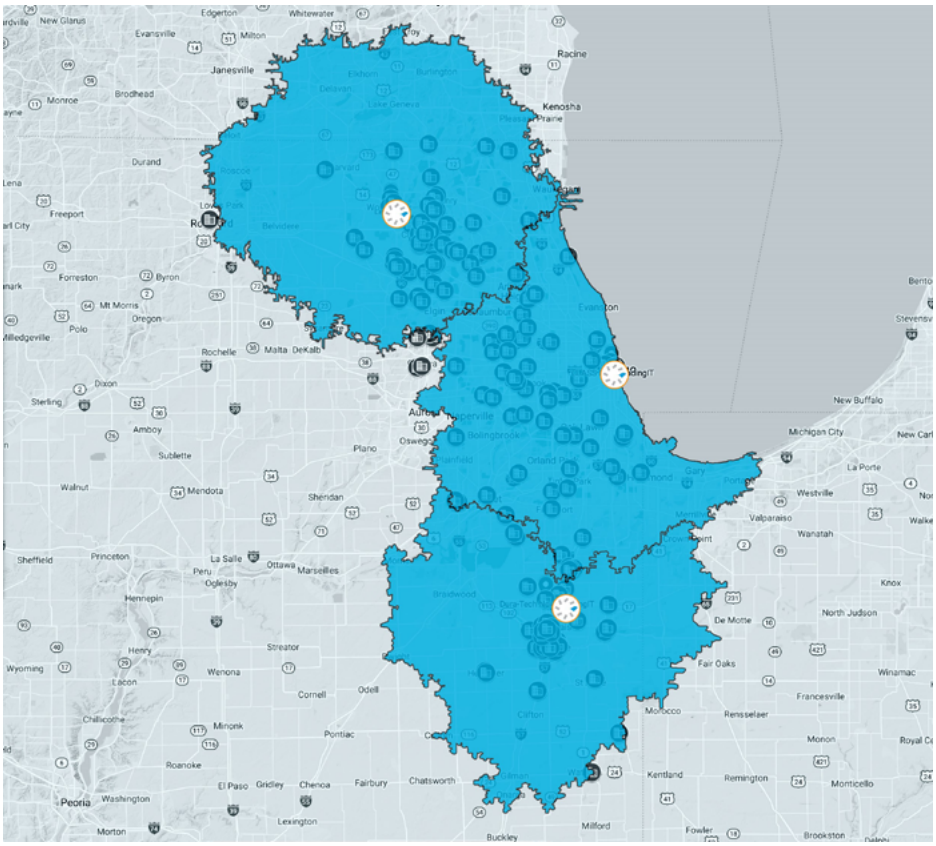
Anniversaries

Jason Frederick Jimenez- 3/4/2013
Steven Brimeyer - 3/23/2020
Christa Gibbons - 3/11/2020
Anthony Gallardo - 3/1/2021
Mark Seplowin - 3/1/2021
Dale Schwer - 3/1/2021
Jose Ledesma - 3/1/2021
Michael Seplowin - 3/1/2021

LeadingIT Acquires Dura-Tech Enterprises Further Expanding Chicagoland Presence

LeadingIT would like to announce the acquisition of Dura-Tech Enterprises, a cyber focused technology solutions provider based in Manteno, IL, working with businesses to protect their organization and improve their technology in the South Chicagoland area.

"We made the decision to invest in Dura-Tech because of its solid reputation and long-term relationships with fire districts, municipalities, banks, and school districts. Our partnership reflects the shared values of each of our companies, including fast + friendly support, with a focus on cybersecurity, so that organizations are protected from cybercrime." said Stephen Taylor, CEO of LeadingIT. LeadingIT now has almost 200 clients across Chicagoland in all different industries and a team of 25+ help desk and network engineers.



LeadingIT

Serving the Chicagoland area with offices in Woodstock, Downtown Chicago, and now in Manteno, IL.

Check out our blog at goleadingit.com/blog