CYBERSECURITY
SURVIVAL GUIDE FOR LANDSTAR AGENTS

THE ESSENTIALS YOU **MUST** KNOW TO PROTECT YOUR AGENCY!

- ATTACKED: ONE AGENT'S HARROWING EXPERIENCE
- CYBERATTACK: A SERIOUS THREAT TO YOUR AGENCY
- WHY YOU MUST PROTECT YOUR BUSINESS – NOW!
- YOUR SECURITY CHECKLIST: CREATING A CYBERSECURITY PLAN TO PREVENT DISASTER

SURVIVING AN ATTACK

How one Landstar agency kept freight moving when their business was under cyber-siege

One evening in March of 2021, independent Landstar agency Momentum Transportation USA received a call from its IT Management Service Provider (MSP), saying there was something impacting one of Momentum's servers, they were working on it, and should quickly have things back to normal.

Brian Putzke, president and CEO of Momentum, said his agency had systems in place to protect against hackings, but unfortunately, it wasn't enough. Hackers had found their way far beyond Momentum's one server, and were deep into the agency's entire IT system.

Early the next day, agency employees found some of their data and drives were seriously affected. By Noon, all of the agency's data – including backups – was encrypted. Immediately, all of Momentum's systems and servers were shut down, creating a total loss of access to all of the agency's files, email, and even the phone system. Momentum's business was nearly at a complete standstill.

> *"I wouldn't wish this on my worst enemy."*
>
> *Brian Putzke, Independent Landstar Agent*

The team was determined to do whatever it took to keep freight moving. "For some tasks, we went back to pre-computer days and did things by hand," Putzke said. "Luckily, we had use of our cell phones and purchased a few clean laptops from the store,"

As Landstar's systems weren't affected, the agency was able to

continued >

THIS GUIDE IS FOR EDUCATIONAL PURPOSES ONLY. INDEPENDENT AGENTS ARE ENCOURAGED TO CONTACT A CYBER SECURITY PROFESSIONAL FOR BETTER PROTECTING THEIR IT SYSTEMS.

LANDSTAR®

SURVIVING A CYBERATTACK

keep doing business because of Landstar's online platforms and mobile apps. The agency was able to access vital, real-time business information via their personal devices to keep freight moving.

"In our agency's case, I felt there was no guarantee the hackers would release our information back to us – or not use it for other purposes," Putzke said.

With more than a dozen IT engineers working around the clock for Momentum, the restoration of services and useable data was progressing.

The agency's recovery effort included every computer being individually rebuilt and restored, new servers installed, and a full evaluation by Momentum of everything that would have to be recreated.

It took several weeks to restore what information could be recovered, but some had to be completely recreated. More than 18 months of agency records were lost, resulting in Momentum having to research and re-enter as much information as possible. As a precaution, banking information had to be changed. It was an overwhelming amount of work, but it had to be done.

Once up and running, changes were immediately put in place to try and prevent another hacking. Backup strategies and configurations were strengthened, stronger email security was implemented, and multi-factor authentication was added.

> *We thought we were doing everything right in terms of cybersecurity, but it wasn't enough,*
>
> *Brian Putzke, Independent Landstar Agent*

Momentum's expense to recover from the hack was in the six figures, and their monthly operating expenses were doubled to provide the necessary protection from another attack. Last but certainly not least, the agency now has educational security videos that every employee is required to view.

"I wouldn't wish this on my worst enemy," Putzke said. "We thought we were doing everything right in terms of cybersecurity, but it wasn't enough. All we can do is heed the lesson we learned – simply make sure you're doing everything you possibly can do to protect your technology and your business."

Security experts say cyberattacks aren't going away anytime soon. Odds are, your business will be under an attack of some kind at some point. Stay ahead of the curve – reduce your chances by implementing the precautions suggested in this guide. While no one can promise you'll never have a breach, your chances of being a cyber statistic will be reduced dramatically.

THIS GUIDE IS FOR EDUCATIONAL PURPOSES ONLY. INDEPENDENT AGENTS ARE ENCOURAGED TO CONTACT A CYBER SECURITY PROFESSIONAL FOR BETTER PROTECTING THEIR IT SYSTEMS.

CYBERATTACK:
A SERIOUS THREAT TO YOUR AGENCY

Once you're in the clutches of a cyberattack, your data and your business are in for a world of trouble. Prevention is critical – it can save you untold hours of business downtime and a huge chunk of your hard-earned money.

Whether it's malware, ransomware, or other cybersecurity attacks, the goal is that malicious software is installed without the user's permission, and proceeds to attack data, backups, software, cloud storage, cell phone, email – or a combination thereof.

Highly feared by businesses of all kinds are ransomware attacks – a form of extortion where malicious software prevents access to the information on a computer system, usually by encryption, until the victim pays a ransom fee to the hijackers to get the "key" to unlock the encrypted stolen data. There's no guarantee they'll unlock the information, and often sensitive information is sold or released to the Internet or Dark Web – regardless.

Cyberattacks of all kinds are a serious and growing threat to any business of any size – small, medium or large. Most sources agree accurate numbers are difficult, as attacks are thought to be greatly under reported due to embarassment, not wanting to seem vulnerable to attack, or other personal or professional reasons. ITChronicles.com reports successful attack numbers are growing every year, with new methods created every day. Its reported estimates show that in 2020, a new attack was attempted very 40 seconds. Cybersecurity expert Sophos reports that 51 percent of businesses were targeted by ransomware alone in 2020. All in all, that's pretty good odds that at some point, you'll be hit.

Why do hackers bother? Because it's effective – and the payoff is HUGE. The Institute for Security and Technology estimates that in 2020, at least $350 million was paid to ransomware attackers. Even if data isn't held ransom, hackers can steal and sell the data or use it for other illegal activities.

Cyberattacks can be distributed for little to no cost to the hackers. Often, attacks are delivered through a simple "phishing" email, where an attacker sends a fake or "spoofed" message designed to trick recipients into unknowingly releasing the malware on the victim's system. These emails may look very real – email addresses that look to be from a legitimate business, subject lines with generic phrases such as "your Amazon order" or "verify your bank account." Other methods include web links, attachments disguised as videos or memes, and even surveys. Just one little click and an attack starts raging through your network.

Even scarier, cyberattacks get more sophisticated all the time. Some newer ones allow the criminal to transparently peek into your website and discover how to breach more security boundaries. Others dig for personal information that can be sold for identity theft scams. Some release critical, private company information.

Landstar has invested significantly in cybersecurity education, prevention, tools and processes in the last few years. And, Landstar is constantly monitoring for and preventing phishing scams, hacking, and cybersecurity attacks on its systems.

It is important that independent Landstar agencies also do their part to protect their businesses.

Cyberattacks are hard to trace, hard to fight against, and a financial and reputation hit that some businesses may never recover from. According to a study published by Deep Instinct, there were hundreds of millions of attempted cyberattacks in 2020. Compared to 2019, cyber attacks increased by 358 percent.

Only 57 percent of businesses conducted a data security risk assessment in 2020, according to Insight Enterprises's survey through IDG Research Services. Varnish's 2019 Global Data Risk Report says that on average, only 5 percent of companies' folders are properly protected. These statistics should frighten any business owner.

TAKEAWAYS

- **PREVENTING AN ATTACK IS SIGNIFICANTLY EASIER THAN BATTLING ONE**
- **THE NUMBER OF ATTACKS IS GROWING EVERY YEAR – YOU'RE LIKELY TO BE HIT**
- **EDUCATION AND AWARENESS ARE CRITICAL**
- **BEING CONSISTANTLY VIGILANT ABOUT PROTECTING YOUR DATA IS SMART BUSINESS**

THIS GUIDE IS FOR EDUCATIONAL PURPOSES ONLY. INDEPENDENT AGENTS ARE ENCOURAGED TO CONTACT A CYBER SECURITY PROFESSIONAL FOR BETTER PROTECTING THEIR IT SYSTEMS.

LANDSTAR®

CYBERSECURITY
SHOULD BE ONE OF THE TOP ELEMENTS OF YOUR BUSINESS PLAN

...according to a recent article in Inc. magazine by Neill Feather, Chief Innovation Officer for Sitelock.

WHY YOU MUST PROTECT YOUR BUSINESS

After Landstar Agent Brian Putzke's digital assets were hacked, he and his IT Management Service Provider (MSP) quickly re-evaluated what kind of protections would be best for his business. "We had a good IT service, backups were being done, we used a basic email filter, and we had service and support," Putzke said. "But it wasn't enough to keep up with the criminals. An attack at this level wasn't on our radar. We were doing things to protect ourselves, but not at the in-depth level we are now."

Now, Momentum and its team have a top-notch email filter specifically designed to catch a phishing attack – which, according to Infosec Resources cybersecurity blog, is how the vast majority of malware is delivered, and very likely how the attackers got in.

Malware can be designed to quickly obtain complete administrative privileges. It can encrypt working files and backups, putting you right where the hackers want you – at their mercy. Adding two-step authentication, risk-aware passwords, role-based access, alerting and reporting software that detects and notifies suspect activity, and immutable storage (storage capable of writing data so it cannot be altered or deleted) are some of the simplest ways to prevent an attack, states Veritas Technologies in its 2020 "5 Ways to Defend Data from Ransomware" checklist.

"It might be inconvenient when you are hurrying through your day and want quick access," Putzke said. "Time-sensitive emails sometimes take longer to get through, because they're being scanned before delivery to our inboxes. But after going through an attack, we feel it is well worth the little bit of inconvenience."

Additional investment in security enhancements could save not only your data, but your business.

It is critical for agencies' business technologies to be properly configured to protect against cyberattacks. Additional investment in security enhancements could save not only your data, but your business. Ask your independent IT company for an evaluation of all of your system protections, then determine what options are best for your business – and your budget.

"The lesson learned from this is to simply make sure we're doing everything we possibly can do to protect ourselves," Putzke said. "There's so much protection you can buy that you can price yourself into bankruptcy. Of course, you can't afford to do it all, but do whatever you can afford."

His best advice after going through what he says is the worst experience in business in his life? Create secure offsite backups on a daily basis. "No agency should ever leave for the day without a full backup of its system going into a protected space," Putzke said. "It is a whole lot easier to recover from there than going back a year or two like we had to."

He added it was the last thing in the world his agency expected. "We're a little tiny business compared to all the really big dollar companies you'd think hackers would target," Putzke said. "An attack could have wiped us out. The expense and headaches were massive, and we're still sorting through some of it. We thought we had protection, but it wasn't enough. I hope sharing our story can prevent another agent in the Landstar family from experiencing this nightmare."

THIS GUIDE IS FOR EDUCATIONAL PURPOSES ONLY. INDEPENDENT AGENTS ARE ENCOURAGED TO CONTACT A CYBER SECURITY PROFESSIONAL FOR BETTER PROTECTING THEIR IT SYSTEMS.

SECURITY CHECKLIST:

While nothing is foolproof, there are some effective ways to prevent a cyberattack – and they're relatively easy to implement for most businesses.

ASSUME YOU WILL BE HIT.

No one is immune to a cyberattack – and a single attack can quickly cripple an organization. It's a thousand times better to be prepared and not hit, than hit and unprepared.

STAY VIGILANT.

Hackers are continually improving their software and their tactics.

PLAN AHEAD.

Have a comprehensive plan ahead of time and know what to do if you suspect a breach. Contact names and numbers should be readily available to everyone in your organization who may need them in case of emergency. Know your IT provider's regular and after-hours schedules, and make sure your provider knows who to contact at your agency in case of an issue – days, nights, and weekends.

STAY CURRENT ON SOFTWARE/PATCHING.

Cyberattacks often sneak in through system and software vulnerabilities. Current updates are often readily available to patch system holes. Keeping current on updates is critical to keeping your tech safe. Consult with your IT specialists as to who will be responsible for discovering and implementing updates – your web developer, email system manager, computer server host – they can all help you with establishing effective procedures.

- Most applications, browsers, and operating systems can be set to notify you of current updates, or even download and install them automatically. While this is relatively easy for most users to do themselves, often there are more vulnerabilities than are covered by basic updates, and sometimes incompatibilities can shut down a system you're trying to update. Talk with your IT team about the most effective tools and update plan for your system.

REMEMBER TO COVER WORK FROM HOME.

Now more than ever, people are working from home. If you have off-site computers and devices interacting with your agency's network, they must have appropriate security protection, too.

- Any sensitive or critical data should be stored in a secure location, like a cloud or off-site server, just as your other data is stored.
- If employees are using their personal computers and devices to connect to your network, it is critical to have malware endpoint protection software set to automatically update. Never depend on employees storing company data on their own devices – work with your IT specialists on how to set up their systems to best work with yours. Remember – it's your information that's on the line.

EDUCATE, EDUCATE!

You know the saying an ounce of prevention is worth a pound of cure? That ounce of prevention is education. It is vital that you are vigilant about educating your team on cyber-safety procedures. This includes how to spot phishing email, identifying malware, and what to do if an attack is suspected. Stopping a cyberattack before it starts beats dealing with it by a million miles.

- Make sure everyone on your team knows what might indicate a breach – such as inability to connect, files that suddenly aren't accessible, or strange email activity.
- All the need-to-know members of your team should understand your backup and restore process and exactly what to do if something unusual happens.
- Schedule ongoing training and awareness for everyone on your team. Consider it an essential part of your

continued >

THIS GUIDE IS FOR EDUCATIONAL PURPOSES ONLY. INDEPENDENT AGENTS ARE ENCOURAGED TO CONTACT A CYBER SECURITY PROFESSIONAL FOR BETTER PROTECTING THEIR IT SYSTEMS.

LANDSTAR®

budget. It's too easy for someone to forget or get careless – and then you're exposed. Experts recommend that new hires be trained immediately upon hire, and refresher training be provided for everyone at least once a year. Ask your independent IT professional about training programs and materials.

LIMIT PRIVILEGE. ADD PROTECTION.

Limiting administrative and escalated privileges for most accounts will help prevent the spread of malware. Do not use shared accounts or passwords for accessing any applications or email.

• Since nearly all malware attacks begin with phishing, adding at least one additional layer of advanced email filtering can greatly help detect and block malicious messages and embedded links. Consult your email provider or IT specialist for advice about what is currently most effective for your service.

• Multi-factor authentication (MFA) is highly recommended. It requires users to provide at least two verification factors to access an account, making break-ins more difficult and seriously decreasing the likelihood of a successful cyberattack.

• Endpoint security protection (endpoint means devices such as desktops, laptops, and mobile devices) can also lessen the risk of being invaded by those with malicious intent. Usually, this kind of security is installed on a network or in the cloud. This includes anti-malware protection, spyware protection, and anomaly detection.

Resources:

Ransomware Statistics, Trends and Facts for 2020 and Beyond - cloudwards.net
How to Protect Backups from Ransomware - CSO Online
Top five ways backup can protect against ransomware - Computer Weekly
JBS Paid $11 Million to Resolve Ransomware Attack, June 9, 2021 - The Wall Street Journal
Alarming Cybersecurity Stats: What You Need To Know For 2021 - Forbes
2019 Global Data Risk Report - Varnish
IDG Research Services Survey - Insight Enterprises
Ransomware Attacks, Explained, July 13, 2021 - CNN Business
Ransomware Victim Every 10 Seconds in 2020 - Infosecurity-magazine.com
Institute for Security and Technology
Global State of the Channel Ransomware Report 2020 - Datto
Malware increased by 358% in 2020, helpnetsecurity.com
The State of Ransomware 2021, Sophos
U.S. Department of the Treasury, Ransomware Advisory
This Year in Ransomware Payouts, Heimdal Security

BACKUP & RESTORATION STRATEGIES

Frequency is key. Backing up data on a regular basis is highly recommended. Most IT pros recommend backing up at least daily – preferably to an offsite server or cloud – with backups going back multiple days or weeks. That way, if you are attacked, your losses are minimized and you can restore the data you've saved offsite, saving untold hours and dollars.

Timing matters. When setting backup schedules, determine the balance between how long it takes to run a backup for the amount of time you are covering versus how long it would take to rebuild any data lost between backups. Whether it's a day, a half day, or just hours, work with your independent IT company to decide what schedule works best for your business.

Speed counts. The ability to quickly restore your data from a current backup is vital to continuing daily operations. Ask your IT company about restoration timeframes – both partial and complete. You want a short enough time span to keep your business going while doing a data rebuild, which could take hours, days, weeks, or even longer – valuable time you could spend running your business instead of re-creating information you already had.

Location, location, location. It's highly recommended to secure backups off-site and in one-direction-only systems. Store your information so it cannot be altered or encrypted during an event such as a ransomware attack. Most cloud-based storage and backup services provide various levels of backup protection. Talk with providers about your options.

Don't procrastinate! It's easy to put off, but it is extremely important to test your backup and restore procedures on a regular schedule, so you know the process works. Test often enough so you have confidence in your ability to recover if your data was wiped out tomorrow. Work with your IT provider to determine what changes might affect the effectiveness of backups, including system changes, new drives, additional users, or new upgrades.

Don't skimp. If you decide to create your backup and restoration plan yourself, consider having a professional review your plan for steps you may have missed.

Check your work. Regularly review your plans with your IT provider for possible issues and thoroughness. The last thing you want is to discover you thought your backups were working – and find out after a hack that they're not.

THIS GUIDE IS FOR EDUCATIONAL PURPOSES ONLY. INDEPENDENT AGENTS ARE ENCOURAGED TO CONTACT A CYBER SECURITY PROFESSIONAL FOR BETTER PROTECTING THEIR IT SYSTEMS.

LANDSTAR®