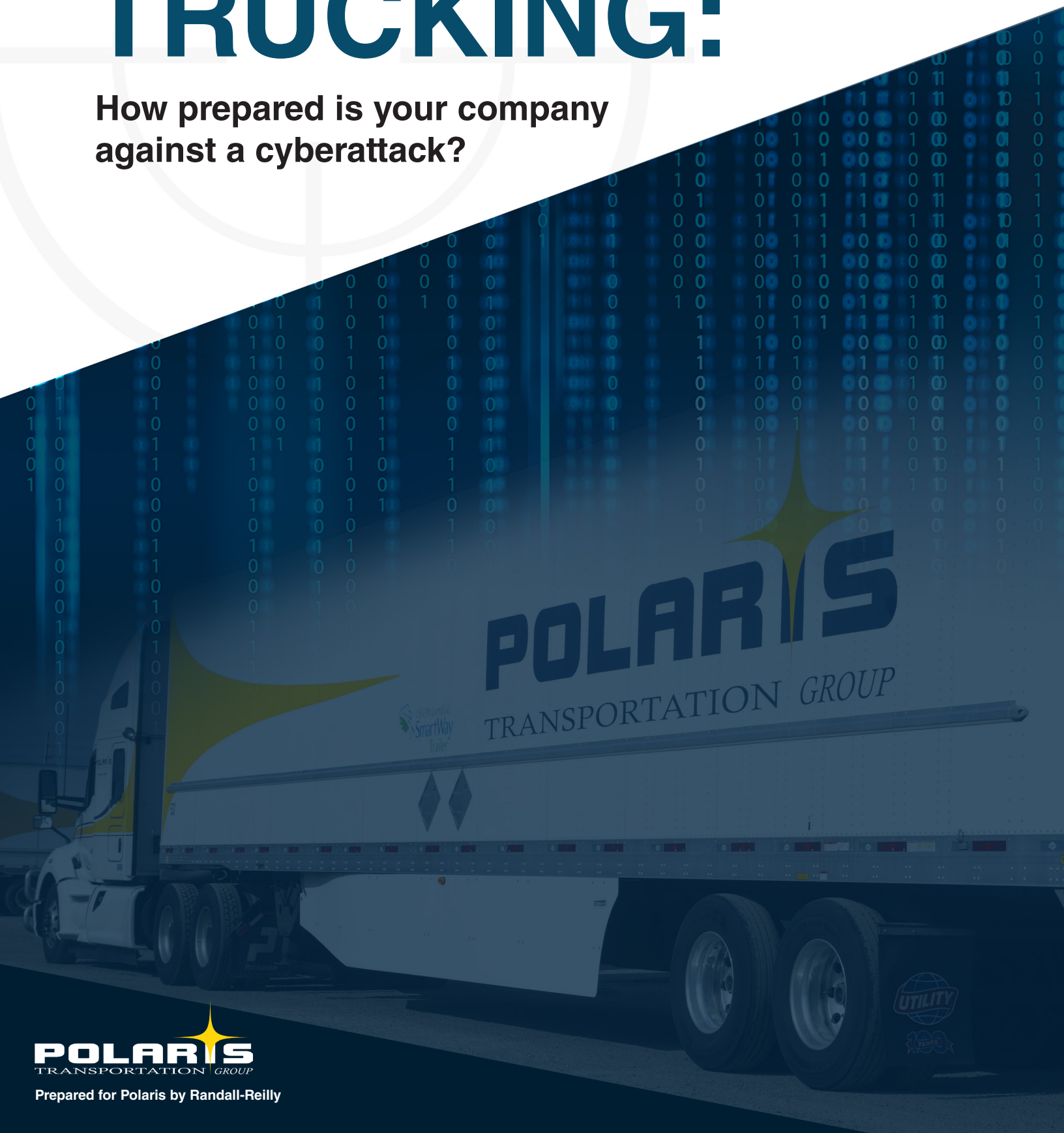
TARGETING TRUCKING:

How prepared is your company against a cyberattack?



POLARIS TRANSPORTATION GROUP

Prepared for Polaris by Randall-Reilly

It shouldn't take the shutdown of America's largest gasoline pipeline, a resulting shock in infrastructure and a $5 million payout to hackers to warn businesses that cyberattacks are credible threats that can have devastating consequences.

The U.S. Department of Homeland Security estimates that as of early May 2021, there'd been a nearly threefold increase in ransomware attacks within the past year — a majority of those targeting smaller businesses — and many instances go unreported. As companies continue to conduct more business digitally, these kinds of attacks are expected to be more prevalent.

A computer and information technology security posture can be compared to a person's physical posture. A weak, slouched physical posture can be like waving a red flag in front of a bull. Those with harmful or malicious intent instantly spot weaknesses and peg the person as an easy target for a crime, like assault or robbery. On the other hand, an upright, steady physical posture projects strength and prominence, making that person a more difficult target and thus less likely to fall victim to an attack. In the world of digital ecosystems, a weak IT security posture is a flashing light to technical professionals who may have malicious intent. By the time you recognize the issue, it could be too late.

5 immediate questions your company will face:

What was stolen?
Sensitive data is often the target of cyberattacks, and hackers may threaten to make it public, for example, unless a ransom is paid.

What systems are down?
Cybercriminals can lock down a business's operations and hold it in limbo, preventing it from carrying out day-to-day functions and causing instant, hemorrhagic losses. For companies in transportation and infrastructure, the repercussions of downed systems can be even more pronounced.

How much will it cost to fix?
What are the hackers demanding, and how much must be paid in the scramble to get out? Along with the uptick in ransomware attacks, Homeland Security has tracked a sizeable increase in average amounts paid to fix cybersecurity breaches.

What social impact will it have?
An IT security breach can be damaging to a business's image and reputation. This may not be an immediately tangible loss, but it's often persistent and difficult to repair.

What are the legal implications?
If sensitive data such as financial or personal information is made public, there could be legal ramifications for the business that has fallen victim. That could mean additional business losses or restrictions going forward, perhaps for years.

NORTHSTAR
DIGITAL SOLUTIONS

Dave Brajkovich, CTO Polaris Transportation Group + COO NorthStar Digital Solutions (left), Dave Cox, President + CEO Polaris Transportation Group (right).

Polaris Transportation Group, a cross-border transportation and supply chain solutions company based in Ontario, Canada, has taken the lead in mitigating risk. In recent years they worked to automate previously manual processes like order entry and customs form management — resulting in more digital-based freight transactions. The company started its own IT-focused firm, NorthStar Digital Solutions, to handle its growing IT security needs and those of other similar clients. NorthStar aims to address this question: What are the real costs and impact of IT downtime?

The cost of IT downtime isn't limited to specific loss of files or megabits of data. The real costs of IT downtime can include damage to client relations, finances, employee retention, business growth and more. It's common sense that not meeting business obligations in any way will have an impact on your bottom line.

Most business leaders today are aware of these issues, but what are they doing to minimize risk? Many of the current IT security breaches are "silent killers" with sophisticated technology that penetrates a company's systems before anyone is even aware they've been attacked. Even so, there are solid techniques, training programs and system infrastructures that afford some protection and will help deter hackers from penetrating poor organizational IT security.

Organizations like financial and health care institutions handle sensitive data and have spent millions of dollars to proactively secure their platforms and networks. Organizations that have not invested so heavily in security are the ones that present vulnerable security postures and are likelier to become opportune targets for professional hackers.

Hackers have recently discovered weak IT security postures in transportation and supply chain verticals. They are now targeting these organizations to steal data, ransom systems operations, use phishing campaigns to extract funds through fraudulent accounts, or steal passwords and commit identity theft. Once data is captured, hackers can use it on the dark web to do a lot of damage. The threat is substantial and ongoing. All the targeted organizations in IT security breaches have one thing in common: the need for digital capabilities to conduct their business transactions. Today, having the right IT security in place is no different than having adequate insurance or disaster recovery plans, with continuous testing and monitoring.

5 signs you've been hacked

Your software vendor has been attacked.
The Texas-based Solar Winds attack by Russia's foreign intelligence service had a ripple effect that impacted the transportation industry.

Your system begins to degrade.
When employees start to say their software systems are running slow, it can mean you've been compromised.

An employee clicks on a suspicious email.
A phishing email that collects an employee's password is one of the easiest ways for a hacker to access the company's data, including online banking.

There is suspicious network activity.
Cybercriminals are using sophisticated artificial intelligence to infiltrate servers and launch an attack. Many of the attacks come from China and Russia.

Company files are encrypted.
If you get a message saying files are encrypted, you are facing a ransomware situation.

Source: www.CCJdigital.com

Upgrading IT security measures

Gone are the days of antivirus protection providing sufficient security. There is much more to IT security now in the world of digital integrations, like privacy regulations and elevated protection needs due to connection complexities, coupled with accompanying security and preventive tools and measures.

With IT security enhancements, NorthStar Digital Solutions points out that companies may hear one comment frequently from employees: "Why can't I connect to this website I used to be able to?" The answer is simply that new security measures had to be applied, and firewalls and whitelisting needed to be enabled.

There is now pressure on digitally enabled companies to be proficient and effective with security knowledge and experience. That means having a chief information security officer and an IT security group that works hand-in-hand with the IT and operations side of the business. The IT security team needs authority to refuse connections that it thinks will add risk to the organization and its clients. All this will cost money and add layers to system processes, but it should be considered a "must have" in some capacity.

Here are some baseline recommendations for strengthening IT security postures:

- Add in solid SIEM (security information event management) protection for current system foundations.
- Hire dedicated IT security management staff and services for monitoring and proactive/counteractive measures. These personnel can be considered your organization's IT asset security guards.
- Use end-user training programs for cybersecurity awareness, protection and proactive password management. This goes for all employees.
- Use two-factor authentication solutions — if not for the entire organization, at least for senior-level executives and decision makers.
- Combine security efforts with your cloud hosting solutions providers, which can provide additional levels of protection. The catch is that you'll need to know what to ask for and what you want to spend.
- Set appropriate policies for privacy and systems usage so that these are part of your code of conduct and expectations set for your employees — and again, this goes for all employees.
- Establish a disaster recovery plan for IT security that incorporates a return point objective and a return to operations plan. This should include a fully manual contingency in case all systems fail — i.e., how will you do business with no email, no transactional systems, no billing and/or limited communications? Write, test and deploy a playbook for the organization.

Call in the experts

Every organization needs to determine their own potential risks and security gaps. If those risks and gaps are difficult to identify, consider enlisting the services of a highly rated cybersecurity consulting team. NorthStar Digital Solutions notes there are many ex-law enforcement and forensic experts who offer IT security services. They can provide an IT security overview of your company, listing what's sufficient and what's not sufficient, with recommendations to close the doors on the biggest, most immediate risks.

How would your IT personnel answer these questions if your company's IT infrastructure were attacked?

Can we still commit to our client obligations?

Can we keep selling?

Can we deposit money + pay bills?

Can our staff continue to work?

Don't get overwhelmed, and keep in mind you don't have to fix everything at once. NorthStar Digital advises organizations to take incremental steps to address the whole system after you fill in the most critical security holes.

The value proposition is that you will know your risks, get the right pieces in place for foundational protection and focus on being proactive and educated. Remember that hackers are unforgiving, and the penalties of falling victim are considerable and long lasting. By the time your organization makes headlines, as a growing number have, it's too late. The reputational hit can take a long time to repair and customers will remember an IT security breach.

Remember that ignorance is not a defense. Once bitten, cautions NorthStar Digital, you will be on your own to deal with the mess that comes from all directions — and fast.

Back it up with the 3-2-1 rule

Still, NorthStar Digital says you can limit the impact, should an unplanned IT security event occur. Technology personnel often cite the "3-2-1 rule" for system backups: Store three copies of your data on two different mediums and keep one copy offsite. But when was the last time your business tested the integrity of its backups, and how would you recover if your backup platform were compromised? Do you have a plan for that, and does that plan have a person's name associated with it?

The problem with most IT disaster recovery plans or business continuity plans is that they are static processes with only vague procedures to back them. They're tested perhaps once a year by the person who wrote them, if that.

According to NorthStar, it's wise to move your infrastructure offsite and sign a hosting contract with teeth. Also, know that old technology is more susceptible to risk, in part because it's harder to patch. It's typically installed on a single server with slow recovery times. With old technology, it's likelier that holes in security have been added over the years without being documented. And old battery backups may not last long enough, among other problems.

There are some caveats to moving your infrastructure offsite. Organizations may hire a cloud architect, believing that company will make things safe and secure, but it won't, cautions NorthStar — that's a separate role. A cloud architect also won't maintain the cloud platform, since they're project-focused; they'll finish the job and move on. A cloud architect will also build your cloud platform with no regard for cost.

Arriving at this point, many businesses are confused about what to do next. As an IT security partner, NorthStar aims to gain an understanding of your IT business objectives, build a migration plan, ensure your cloud systems are resilient with multilocation availability, secure your systems, and maintain those systems 24/7, 365 days a year. NorthStar says it builds business relationships on trust. Whether on your premises or its private cloud, NorthStar can maintain your organization's technology, migrate it and secure it — and back that up contractually. Further, the company has the experience to know what to ask and how to deliver the service, ensuring everything needed is in scope. ■