pchtechnologies

Unbeatable IT and Cybersecurity

KEEP YOUR BUSINESS PROTECTED WITH CYBERSECURITY

Stay one step ahead with PCH Technologies.

pchtechnologies

(844) 754-7500
info@pchtechnology.com
www.pchtechnologies.com

OUR COMPANY

"PCH" is the shortened version of our original company name, "PC Helpers." Since then, we have continually evolved and expanded – from our IT services, our personnel, and our capabilities as new technologies emerged. All to consistently meet the needs of our clients.

The thing that makes us different from other IT support options is simply this: we will make certain – once your network is up – it stays up. With the redundancies and offsite options available to us, our clients' downtime has quickly become a thing of the past.

We pride ourselves on keeping your systems safe and secure, and demonstrating consistent professionalism by being always on time and on budget.

TABLE OF CONTENTS

pch technologies

Section 01

STAY ONE STEP AHEAD WITH CYBERSECURITY

The security landscape is constantly changing. Within a cybersecurity environment, if CIOs and business teams alike are not evolving with those accelerating changes, then they are at risk. Headlines involving data breaches and successful ransomware attacks seem to be the norm these days, but they do not have to be normal for your company.

Contrary to popular belief, having the latest in network security technologies or software isn't what will ultimately protect you or your organization from a data breach or critical data loss. However, what will in fact help keep your organizatzion one step ahead of the latest cyber attack is first understanding the motivations behind those cyber attacks, and then becoming familiar withtype of attacks to look out for and how you counter those different attacks.

MOTIVATIONS BEHIND CYBER ATTACKS

The single biggest motivation behind any cyber attack is criminal in nature, according to information security website Hacksawed. And while all cyber attacks are considered criminal to some degree, it is cybercrime that is the biggest motivator – those individuals seeking to gain from their cyber activities either through direct or indirect monetary gain, or to cause great harm to an individual person or entire organization.

In nearly 78% of all cyber attacks, cybercrime is the primary motivation. Hacktivism is the second largest motivator at 13.5%, which is specifically carried out by individuals or groups fighting for a particular cause meant to bring awareness to the plight of a group of people, or attempts to highlight the perceived negative or unethical behavior of government or corporate misbehavior.

78%

IN NEARLY 78% OF ALL CYBER ATTACKS, CYBERCRIME IS THE PRIMARY MOTIVATION.

pch technologies

TYPES OF ATTACKS

Given the wide variety of options and tools cyber criminals have at their disposal to cause harm, It's certainly important to know and understand what some of the most common forms of attacks are. Used most often at 25.8% is malware, which is an umbrella term for just about any form of hostile software including computer viruses, ransomware, spyware, Trojans, and so on. This is the preferred method of delivering an attack because it's often the easiest to create and successfully pass the eye test with people who simply don't pay close attention to what they are clicking on or opening.

STAYING ONE STEP AHEAD

It shouldn't come as a surprise that cybercrime is the single greatest threat to individuals and companies all over the world. It is widely expected that cybercrime damages could cost in excess of $6 trillion annually by 2021. Cyber theft is the fastest growing crime in the United States, according to multiple FBI and U.S. Intelligence reports. In order to be prepared for this ever-expanding threat, there are two core areas in which a company must be extra vigilant: cybersecurity education for employees and avoiding alarm fatigue.

INVEST IN CYBERSECURITY EDUCATION FOR EMPLOYEES

The workforce of today isn't nearly as equipped to deal with the current cyber challenges as the cyber workforce of the near future should be. Research shows that investing in cybersecurity education for employees can reduce network security risk by as much as 70%. Additionally, organizations that offer the training and education resources to current and prospective employees create an environment where the majority of their workforce is better prepared to handle the the cyber demands of the digital economy.

AVOID ALARM FATIGUE

Everyone who has paid attention to the increasing number of cyber attacks and growing cyber threats remembers what happened to Target in 2014. The retail giant was the victim of, at the time, one of the largest data breaches in history. The issue wasn't that they didn't receive any alerts or red flags, the problem was that they receive so many alerts and false alarms on a daily basis that a legitimate threat was overlooked.

According to the Ponemon Institute, by 2015 only 4% of all malware alerts were investigated. Organizations were receiving an average of over 17,000 malware alerts per week, but less than 20% of those were considered reliable and actionable. While those numbers have likely increased, this information tells us is that organizations either typically do not have the resources to detect and block legitimate malware attacks, or simply lack the in-house expertise to recognize the threats.

pchtechnologies

Section 02

WITH INTERNAL NETWORK SECURITY TRAINING, STOP THE THREAT FROM WITHIN

What's the best way to combat network security threats? Is it the crème de la crème of next-gen security software? Or, is it top of the line CIA-grade encryption on your data centers? Nope. Believe it or not, the most effective way to combat cyber attacks against your company is to train your employees on modern network security.

THE DANGERS OF UNKNOWN SECURITY RISKS

With so many network security risks out there, if internal teams aren't aware they exist and don't know what to look for – how could you expect them to help the company combat them?

The reality of the digital workplace is that employees unknowingly pose the biggest security risks to the company they work for simply because they don't know any better.

Unknown security risks your employees should be educated on take on many forms, but here are some of the most common:

01 **Social engineering attacks designed to gain confidential information from an unsuspecting employee**

02 **Downloading files from the internet from unknown sources**

03 **Failure to properly secure and inventory company devices such as laptops, smartphones, and tablets**

WITH THE RIGHT TRAINING, ALL OF THESE NETWORK SECURITY THREATS SUDDENLY BECOME A NON-ISSUE, BECAUSE EMPLOYEES CAN WATCH FOR THEM AS A COHESIVE TEAM AND WORK WITH DEDICATED NETWORK SECURITY PROFESSIONALS, AS OPPOSED TO AGAINST THEM.

pch technologies

TRAINING APPROACHES

When it comes to actually educating employees on the dos and don'ts of network security, where should you begin? Each person in the organization will have varying degrees of network security experience and knowledge – and some may have none at all. Security awareness training can be implemented in a number of ways, whether in a one-on-one setting or in a classroom environment, depending on the resources available to conduct such specialized education.

Regardless of resources, there are three approaches to training that practically any organization can implement:

01

Provide access and materials to trusted and certified security awareness programs existing online.

02

Set up a "Helpful Hints" system that provides pop-ups and feedback when an individual tries accessing certain sections of company data, or simply when they login to their computers.

03

Use visual aids and informational flyers by in common areas and handouts in meetings, common areas and workspaces during normal working hours.

HOW TO IMPLEMENT THE RIGHT TRAINING PROGRAMS

There is never just one particular area where an organization is lacking in network security. The vast majority of systems are interconnected and if one device, if one piece of software is vulnerable then the entire IT ecosystem is vulnerable. As such, the success of any security awareness training program is generally based entirely on how well the information is delivered and reinforced.

First and foremost, network security training must absolutely be incorporated into new employee orientation. By doing so your organization not only makes it clear just how seriously network security is taken, but the expectation is set for all new employees to be mindful of and share responsibility for it.

Taking things a step further, training should be developed for specialty roles where certain employees are responsible for critical niche operations within an organization. After all, if an IT professional is hired to monitor any and all incoming and outgoing internet connections for the organizations, it doesn't do much good to have them spend time troubleshooting general computer issues for other employees like tickets for lost passwords.

REINFORCING NETWORK SECURITY TRAINING & RE-EDUCATION

Once you have a plan in place for implementing the right network security training programs for your employees and organizations, how do you keep everyone's knowledge base and skills fresh and up-to-date?

To choose the right approach, you must understand the company culture and what is deemed acceptable and unacceptable. One way to reinforce network security training education is through positive feedback. Seems simple enough, yet it may not be enough for some employees to internalize and maintain that critical knowledge. You can take a step further with rewards such as gift cards or company gear of some kind, based on scores in follow-up surveys or modules.

In reality, repetition is likely the best and most widely successful reinforcement of network security training education. Create and distribute announcements throughout the organization via email and regular company newsletters or flyers. Only by incorporating security into the culture of the company with clear expectations and direction will employees keep it top of mind.

I'm so confident now with PCH Technologies….that we are protected because of the layers of security that are now in place. Even if we do manage to download a virus, which your system would prevent, we would have a backup that is not contaminated. We never had anything like this before. Now PCH Security Plus is on all of our systems and devices, all are protected — it's just brilliant.

– Team Builders Plus / Take Flight Learning

Section 03

KEEP YOUR FILES EXRA-SAFE IN A DATA CENTER

The reasons for a change in how we store and access our data boil down to cost, security and ease of use. If something were to go wrong on site – such as your brick-and-mortar storefront burning to the ground – all of your customer data would otherwise go up in smoke with it. Except none of it will because you wisely stored it in a remote data center in the Andes and didn't lose any billing or customer information, and you won't be required to start from scratch to rebuild your business.

BUSINESS BENEFITS OF STORING FILES WITHIN A DATA CENTER

Storing files remotely as opposed to locally on your physical property has pretty clear benefits across your operation, when you lay it all out. From lowering costs, in many cases, to completely automating your data storage activities and saving your company many, many hours of work and time, to increasing security and improving scalability.

COST BENEFITS OF STORING FILES WITHIN A DATA CENTER

Storing and backing up critical data isn't cheap. As a matter of fact, according to Search Data Backup the average total cost to maintain a high-quality tape backup checks in at over $600,000 over a five-year period. The average five-year cost to handle local backup on disk checks in at over $2 million. Of course, this depends on the amount of data you need to secure and backup, but the fact remains local backup is incredibly cost-prohibitive.

Since your data is being stored off-site and backed up in multiple secure facilities, your company now has additional free space for new operations or employees that can help drive sales and increase customer satisfaction.

$600k

THE AVERAGE TOTAL COST TO MAINTAIN A HIGH-QUALITY TAPE BACKUP CHECKS IN AT OVER $600,000 OVER A FIVE-YEAR PERIOD.

pch technologies

Security Benefits of Storing Files within a Data Center

Data stored remotely in a secure data center provides the added benefit of end-to-end encryption, both during transmission and while at rest. This means unauthorized users will not have any access to your files and information. And when your data is always available to you, there's no need to go downstairs, try three times to correctly remember the entry code, make sure no one is following to gain unauthorized access, and so on.

Additionally, servers securely storing your data remain in an environment set up with multiple layers of security and emergency power. Your data is completely secure, yet you maintain constant and immediate access to it.

Backup and Recovery Benefits of Storing Files within a Data Center

Manually backing up and/or recovering your company data after critical data loss can be a disaster in and of itself. Not only would it take excessive physical labor and man-shours, there's no guarantee you'd recover everything given the inherent human error in such large undertakings. When securely storing files within a data center, your backups are handled automatically and on a set schedule that you determine.

When it comes to recovering lost data, whether all data was compromised or just a small portion, the right controls in place typically have most companies back up and running within 30 minutes. Downtime isn't just expensive and disruptive, it also means causing concern for clients and employees who otherwise wouldn't have noticed there was an issue.

Section 04

STANDING SENTRY OVER YOUR DATA WITH NETWORK MONITORING

Imagine there's a door that no one is supposed to enter that says, "Private — Secure Personnel Only." Now imagine someone always there guarding that door, making sure no unauthorized person enters that room to potentially bring down your entire network or take the opportunity to cause irreparable damage. That's why it's important to consistently stand sentry over your data with proactive network monitoring.

PROACTIVE NETWORK MONITORING OPTIMIZES PERFORMANCE

Think of network availability as having open and available connections when you try to connect to and retrieve a file from your server. Or, when you're trying to access and respond to email, or simply trying to connect to the internet in general. Monitoring the quality and status of your network connection matters, as inefficiencies or errors here can severely degrade your entire network performance and your ability to access critical information in a timely manner. Optimizing the performance of your network can also help increase productivity when every piece of hardware and software within your network infrastructure is updated and working as expected.

PROACTIVE NETWORK MONITORING MINIMIZES RISK

Minimizing risk is the sole purpose of any capable network monitoring strategy. It requires a proactive approach to all things network security, as well as staying current on the evolving security threats.

PROACTIVE NETWORK MONITORING MINIMIZES RISK BY:

01 **Managing all updates for timely and proper installation**

02 **Examining firewall activity, hacking attempts and spikes in traffic for relevance vs. risk**

03 **Confirming proper operation of all application services such as Exchange, HTTP, file sharing, etc.**

04 **Tracking and reporting all backup and recovery status**

05 **Providing remote support for the majority of issues**

pchtechnologies

PROACTIVE NETWORK MONITORING IMPROVES PRODUCTIVITY

Wouldn't it be nice to be able to monitor and manage every piece of hardware and software within your network infrastructure? Connecting all the components to and through the network would make it possible to determine which assets are being used and for what purposes — and prevent the potential for one piece failing and causing problems across the network.

A survey conducted by CenturyLink indicated that the most popular benefit of proactive network monitoring is how much time it frees up for internal staff. The reason is that proactively monitoring your network through a network management system is can detect and resolve most issues before you even notice they are there.

The most popular benefit of proactive monitoring is how much time it frees up for internal staff.

pchtechnologies

PROACTIVE NETWORK MONITORING SAVES TIME AND MONEY

We know by now that the single greatest threat to a secure network is the human beings managing it. Inattention to detail, ignoring security alerts as a result of alert fatigue, and visiting risky websites all contribute to data breaches and some nasty downtime. Proactively monitoring your security network gives you the opportunity to identify issues well before they get out of hand – limiting downtime and saving money in the process.

The importance of early detection of data breaches is highlighted in the latest report from FireEye, which states that it can take well over 140 days, and in some cases upwards of 500, to recognize that a security breach has occurred. That's several months of a cyber-criminal poking around in your sensitive data, stealing bits and pieces undetected. In major corporate data breaches at Home Depot, Sony or even the Trump Hotels over the past few years, it took internal security teams 5 months to a full year to realize they had been breached. By then, the damage had been done.

IMB and the Ponemon Institute partnered on a recent study highlighting the average cost of a data breach, which discovered that the average cost of a single data breach is $4 million, and the average cost incurred for each lost record increased to nearly $160.

When it comes to unplanned downtime, companies have begun to invest in high-availability clusters and complex fault-tolerance servers, but demand is still outpacing what is currently available. The average outage, or unplanned downtime, due to data breaches, human error or simply an act of nature is nearly 3.5 hours. To make matters worse, businesses are losing more than $108,000 per hour of IT network downtime.

$4,000,000

THE AVERAGE COST OF A SINGLE DATA BREACH IS $4 MILLION, AND THE AVERAGE COST INCURRED FOR EACH LOST RECORD INCREASED TO NEARLY $160.

pchtechnologies

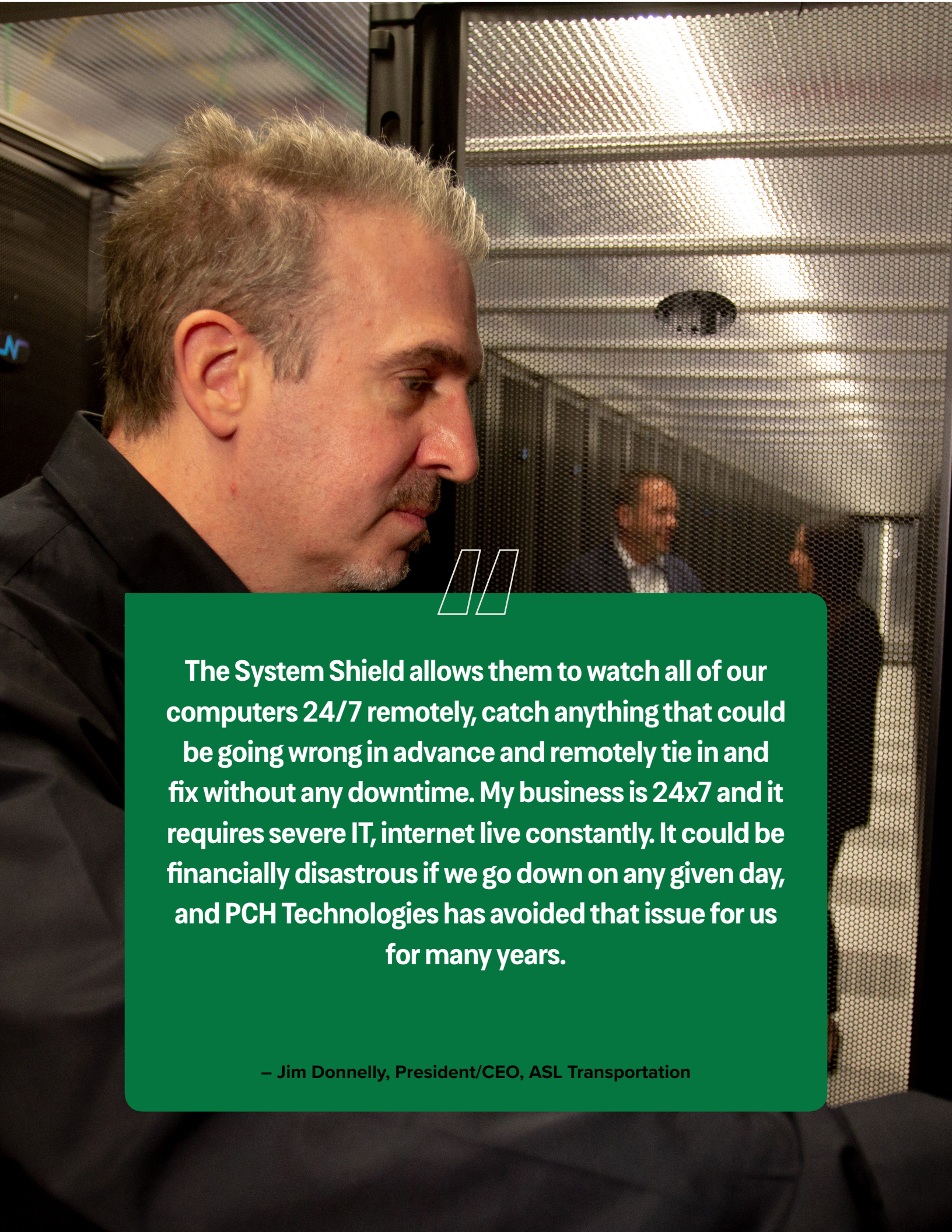
IT'S TIME TO TAKE NETWORK SECURITY SERIOUSLY AND TAKE ACTION

To take network security seriously, companies must invest in the internal teams and resources necessary to stay ahead of the cyber terrorists always waiting, always planning to strike at any given moment. Smaller organizations must often entrust protecting their business to an outside expert for network security management.

If you don't have the internal team to provide a comprehensive network security defense, you are not alone. Finding and employing the right team of well-trained and well-educated IT professionals to protect your organization from cyber crime around the clock could be quite expensive. Outsourcing your IT and network security needs is often the most cost-effective, efficient and responsible solution.

PCH Technologies has been working with clients like you who are serious about network security for over a decade – and our proven team of IT professionals are dedicated to protecting businesses and the information they value most. We make certain that once your network is up, and meets our strict PCH Technologies standards – it stays up, no matter what.

When you're ready for a serious conversation about your unique business network security needs, a dedicated PCH Technologies professional will be ready to talk.



> The System Shield allows them to watch all of our computers 24/7 remotely, catch anything that could be going wrong in advance and remotely tie in and fix without any downtime. My business is 24x7 and it requires severe IT, internet live constantly. It could be financially disastrous if we go down on any given day, and PCH Technologies has avoided that issue for us for many years.

– Jim Donnelly, President/CEO, ASL Transportation

www.pchtechnologies.com