The Tech chronicle

It happens to all

Retailers, hospitals and financial institutions tend to be the targets; however, any company can find itself in the cross hairs of a hacker.

The latest victim is a motherboard manufacturer, Gigabyte.

This attack shut down operations and took a number of the company's web-based systems along with the attack.

Anyone can be a target, protect yourself and your systems, no matter who you are.

Read the August 23rd blog post on our website.

September 2021

This monthly publication provided courtesy of Carlos Soto. Franchise owner since 2005.

Our Mission: To build a community of successful-minded entrepreneurs that inspires excellence, encourages collaboration and expands the capacity of all members to achieve great things.

A Flexible Partnership With IT Professionals

It's hard to see how investing in your company's IT services would be as incentivizing as other investments that might deliver a more tangible ROI. However, ensuring that your IT department has a competent team that's up-to-date on the latest cyber security knowledge and has access to the latest software to allow them to do their jobs well is a sounder investment than you might think.

Investing in your IT services is a little like buckling your seat belt before you drive to work in the morning. You're certainly not planning on getting in a crash that day, but you know that if you do, the seat belt will keep you safe, or at least mitigate the bodily damage the crash could cause.

We live in a world where it pays for companies to be on the forefront of cyber security. Even in just the past few years, ransomware and other cyber-attacks have become increasingly common, and they target antiquated IT systems that have yet to get with the times. If hackers can infiltrate your company's servers and hold that data hostage, it could financially cripple your company to try to get it back – or shut it down entirely. It could also destroy your company's reputation and hurt your clients and customers.

You need an IT team that you can depend on to keep your company safe, but that still leaves the problem of cost. We get it: keeping your IT up-to-date is expensive, whether because you can't afford to hire the right number of IT professionals or because you can't afford the software necessary for keeping your

Continued on pg.2

Continued from pg.1

company from getting hacked. That's why we believe co-managed IT is the best option for companies looking to protect their employees and their customers' sensitive data.

Co-managed IT is a means by which growing companies can have access to all the tools and knowledge necessary to protect their data without paying the full cost. It won't replace your current IT team, and it's more than just a one-off project-based relationship with an outside IT service – it's a flexible partnership between your business and IT services that you can trust.

Say your existing IT team does a stellar job of putting out the little fires that inevitably happen throughout the workday, but they struggle to find time for building and updating company security systems and protocols that will keep your data safe in the event of a cyber-attack. Or your company is going through a period of rapid expansion, and you can't hire enough people for your IT department quickly enough to secure your ever-growing databases. Or perhaps your IT team does a stellar job of finding balance between the daily tasks and preventive maintenance, but they lack the software tools to do so efficiently. In all these scenarios, co-managed IT can ensure that those gaps your IT team just can't fill on their own get filled through a collaborative effort.

"Co-managed IT is a means by which growing companies can have access to all the tools and knowledge necessary to protect their data without paying the full cost."

Co-managed IT can be a great solution for a burnt-out, potentially disgruntled IT team. If you don't know whether your IT team is getting burnt out or not, you can look for a few different signs. If they're constantly working late or on weekends, they're not getting projects done on time or correctly, they aren't creating any new security measures or they're showing signs of aggression or frustration at their job, you might be burdened with a burnt-out IT team.

Ideally, a burnt-out IT team would welcome help with their responsibilities and see the benefits of the collaborative effort between them and another group of experienced IT professionals. Together, we can protect your company from hackers, if you're willing to invest in your IT infrastructure. Even though you might think that keeping things the way they are won't cost you a dime, with how common cyber-attacks are becoming, it could only be a matter of time before hackers hold your data for ransom and cost you everything.

With all this in mind, we strongly encourage you and your IT lead to come to a diagnostic consultation with us. We'll help you understand how, moving forward, co-managed IT can save your company a boatload of money and trouble.

Free Report Download: If You Are Considering Cloud Computing For Your Company, DON'T, Until You Read This…

If you are considering cloud computing or Office 365 to save money and simplify IT, it is extremely important that you get and read this special report: **"5 Critical Facts Every Business Owner Must Know Before Moving Their Network To The Cloud."**

This report discusses in simple, nontechnical terms the pros and cons of cloud computing, data security, how to choose a cloud provider and three little-known facts that most IT consultants don't know or won't tell you about cloud computing that could end up causing you MORE problems and costing you more money than you anticipated. **Even if you aren't ready to move to the cloud yet**, this report will give you the right information and questions to ask when the time comes.

Get your FREE copy today
https://go.ctmaryland.com/cloudreport

ThreatLocker

- Application whitelisting that gives you complete control over what software is running and blocks everything else, including ransomware, viruses, and other malicious software
- Ringfence applications for post-execution protection, stopping attackers from using trusted software (living off the land)

Full visibility of every program, library, or script that is running on your endpoints or servers

- Control which hard drives can connect to your endpoints regardless of type, connection method, or location
- Audit all file access, including reads, writes, moves, and deletes from local drives, external storage, and network shares
- Control application access to your files, preventing misuse of data and ransomware from encrypting your network shares

Put restrictions on individual file types, e.g., permit only jpeg files to be copied from a camera device.

Take control of your computer systems and stop hackers from causing havoc on your computer systems

Call us today!

What Is The #1 Key To Success?

Dr. Geoff Smart: The Key To Success Is Building A Talented Team

To start off, I'll tell you what the key to lasting success isn't. It isn't financially savvy, competitiveness, humility or even hard work. Lots of people embody those traits, so they won't cause you to stand out from the crowd. No, what it really takes to be successful is hiring a talented team.

Successful leaders aren't successful just because of the things that they do on their own. They find success in hiring the right people for the right jobs. That's ultimately what leaders do: they assemble talent and allocate it toward a worthy goal. They have to understand a person's strengths and weaknesses and perceive if and how that person will further the mission of the team, whatever that may be. With a stellar team in place, the decisions of one person become less and less important.

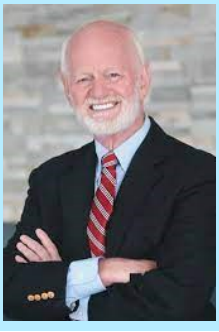
If you don't think that hiring a talented team is the ultimate sign of your success as a business leader, then maybe I can convince you if I approach my point from a different angle. In my book *Who*, which I wrote with Randy Street, one of the first things we established was that one of the biggest problems facing companies today is unsuccessful hiring. At the time, it cost companies $1.5 million per year, and the average company had a success rate of just 50%. Wouldn't it make sense that solving this problem, which is arguably the most important problem many companies face, would be the key to lasting success?

Marshall Goldsmith: The Key To Success Is Creating Lasting Positive Change In Yourself And Others

I would agree with Geoff that success isn't dependent on any of the common, pithy traits like trust, passion, honesty or engagement, but I don't think it necessarily has to do so much with a leader's team. I think that lasting success still starts when one person commits to make the most useful change that will bring about the most good for their business.

So, while having a talented team is important, at the end of the day, if you're not committed to changing yourself, then you won't be able to enact positive change in others when needed either. Your lasting success can only start with you, no matter how much talent you surround yourself with.

That's why in my book, *What Got You Here Won't Get You There*, I emphasize so many different "behavior derailers," like passing judgment, making destructive comments, telling the world how smart you are, etc. Changing these things within yourself where lasting success begins.



Dr. Geoff Smart is the chairman and founder of ghSMART, which serves Fortune 500 companies and helps their CEOs make impactful, successful decisions. He is also the author of the New York Times *best-selling book,* Who, *and many others.*

Marshall Goldsmith is one of the most successful leadership coaches currently working. He is the only two-time #1 Leadership Thinker in the world, as ranked by Thinkers 50. He has written 42 books, many of which are best-sellers.

Why Cyber-Attacks Are Getting So Dangerous

Cyber-attacks on companies are becoming increasingly common. As many companies adapted to the work-from-home culture that came about during the pandemic, they left their systems vulnerable to hackers who could steal their valuable data or hold it for ransom.

Some companies have been able to recover most of their data through the use of backup copies, but all too often, companies see massive interruptions to their operations and make enormous ransom payments. In fact, in the first quarter of 2021, 41% of insurance claims in Europe were related to ransomware.

If it happened to them, it can happen to your organization too. Create a security-conscious work culture, create backups for your data, keep your systems up-to-date and hire security consultants to help you patch up any holes. Cyber-attacks can happen to you, but they don't have to.

How Do You Build Client Trust?

Building trust between yourself and your clients or customers is critical for making sales. If you have a client's trust, they'll work with you regardless of any other hurdles they have to clear to maintain their relationship with you. If you get the impression that potential clients and customers don't trust you, try these two methods for gaining their trust.

Share Client Case Studies With Them. If you can show customers how you benefited someone else's life with your business, they might be more inclined to see you as someone who can help them as well. Find a customer who you've successfully helped in the past. Then, with their permission, map out their struggles and how your services helped them overcome those struggles. New customers will see themselves reflected in those case studies and be more willing to trust you.

Share Video Testimonials With Them. While serving the same basic function as a case study, videos of client success stories help new clients "see it to believe it." These can capture tone and emotion like written words cannot, thus making them a potentially more effective tool for establishing trust in your business.

Building A Virtual Team That Spans The Country

As many businesses found out this past year and a half, miscommunications happen all the time when any team is working virtually. Most of how we communicate with one another is nonverbal, so it would make sense that things would get lost in translation when just chatting through Slack. Nevertheless, there are a few key ways that businesses can learn to communicate well and build a great virtual team.

Create Spaces For Personal Stories. Whether this looks like a group call where the team talks about non-work-related things or you have a virtual "coffee break" every morning, talking about your personal life will help you build trust with your fellow team members.

Make Communication Simple. Make sure the communication channels are clear, then use them correctly. If everyone knows where to find instructions for their workload, then miscommunications will be kept to a minimum.

Set Clear, Attainable Goals. When something needs to get done, don't make general statements about how you'll get there. When you communicate the task to others, mention dates, times and specific steps for getting the task done.

Small and Medium-Sized Business
Cybersecurity Trends in 2021

Cybercriminals do not discriminate based on company size. That's why you can depend on Computer Troubleshooters to ensure your systems are taken care of, data is kept secure, and help is at hand when you need it.

Cyberattacks do not only affect large enterprises. In fact, 55% of SMBs reported suffering from a cyberattack over the last two years and the average cost of an attack has risen to $200,000. Unfortunately, these numbers are expected to continue to climb into 2022.

If that isn't alarming enough, 60% of SMBs that are hit with cyber attacks go out of business within 6 months.

The purpose of this document is to help educate you on the cyber landscape today so that you understand why solutions like ThreatLocker will help keep your business safe.

National Cyber Security Alliance Research

60% of SMBs in the U.S hit with cyber attacks go out of business within 6 months.

How ThreatLocker Protects Your Business

Small to medium-sized businesses are constantly buying into the latest technologies such as next-gen antivirus software and threat detection solutions that use machine learning, artificial intelligence, advanced heuristics, blockchain, and more.

However, none of these solutions protect against the latest cyber threats, including ransomware and other forms of malware. Millions of dollars are spent on cybersecurity annually, yet companies that rely on threat detection are still getting compromised.

Most cybersecurity protections are based on looking for, finding, and stopping threats. The problem is, cybercriminals are getting smarter and entering networks undetected.

End-users are constantly inviting threats through actions such as downloading various applications without Computer Troubleshooters' approval, clicking on links they shouldn't, and opening attachments in e-mails.

That's why a new approach of blocking everything that is not trusted and only allowing those applications that are approved, is a far cleaner and more comprehensive approach to ensuring malware does not end up on your networks.

ThreatLocker combines Application Whitelisting with Ringfencing and Storage Control in ways that make security simple. By combining these three techniques, your applications will not be exploited.

What is Application Whitelisting?

Application Whitelisting is the gold standard in protecting against ransomware, viruses, and other malicious software. The ThreatLocker solution implements a default-deny approach, which means all applications are blocked unless they are on the whitelist.

Traditionally, businesses have relied on antivirus to protect their business. The problem is, antivirus software only attempts to block the bad stuff and oftentimes, it fails.

Antivirus relies on existing signatures and known behavior. As a result, it cannot distinguish between malware and a legitimate piece of software like Dropbox.

In the past, application whitelisting was too complex to manage and maintain for non-enterprise businesses. ThreatLocker has addressed this issue head-on, making the solution feasbile for SMBs.

The ThreatLocker solution combines advanced software and service, allowing Computer Troubleshooters to deploy application whitelisting in a few hours.

The ThreatLocker 24-hour operations center continuously monitors for application and operating system updates, so Computer Troubleshooters does not have to worry about adding a new file to the application whitelist every time Microsoft, Google, or another vendor releases an update.

What is Ringfencing?

ThreatLocker's proprietary Ringfencing solution enables Computer Troubleshooters to go beyond permitting what software can run and control how applications can behave after they have been opened.

This solution adds controlled, firewall-like boundaries around your applications, stopping them from interacting with other applications, accessing network resources, registry keys, and even your files.

This approach is extremely effective at stopping fileless malware and exploits, and makes sure software does not step out of its lane and steal your data.

For example, earlier this year, a vulnerability was discovered in Zoom, putting millions of users at risk of a cyber attack. If you aren't familiar with this tool, it is one of the leading video conferencing software applications on the market, which many have grown accustomed to over the last few months.

By using Ringfencing, you can stop applications like Zoom from accessing your files and launching other applications that could be used against you - even if it isn't on your whitelist, even it's a trusted application, and even if it's malware.

Whitelisting blocks all untrusted applications, however, it will not stop an attacker from weaponizing tools and applications against you. That's why Ringfencing is critical when blocking these attacks.

We highly recommend you combine Ringencing with Whitelisting. By combining these techniques, untrusted applications are not going to be permitted, regardless of how the payload is delivered to you.

What is Storage Control?

It is critical that you configure file shares, USB devices, and other policies to restrict access to files not only at the user level but also at the application level.

With ThreatLocker, you can control device access down to the most granular level, including file type, user or group, application, and serial number - regardless of whether or not the device has been encrypted.

ThreatLocker not only protects you from USB drives, it protects all of your files, including those on your local hard drives and file servers.

Types of Malware

Malware is a piece of malicious software desgined by cybercriminals to steal your data and carry out other nefarious behaviors. Malware can be spread in many ways, including phishing, malicious URLs, downloads, browser extensions, and more.

Ransomware

Ransomware is a type of malware that infects your computer network and other devices. Once infected, your data is locked and encrypted, making it unusable and inaccessible until a ransom payment is received.

Virus

A Virus is another form of malware that, when executed, replicates itself by modifying other computer programs and inserting its own code.

Worms

Like viruses, worms replicate in order to spread to other computers over a network. In the process, they cause harm by detroying files and data.

Trojan

A Trojan is a form of malware that can be used to steal financial information or install ransomware. This is one of the most dangerous forms of malware, as it is often disguised as legitimate software.

Keylogger

This malware records all of the keystrokes on your keyboard. This sends all of your sensitive information, including credit cards, passwords and other user credientials to a cybercriminal.

Spyware

Spyware is malicious software designed to enter your device, gather your information, and forward it to a third-party without your consent. This software is used to profit from stolen data.