TechSage Solutions Newsletter October 2018

TECHSAGE TECH TALK

"Insider Tips To Make Your Business Run Faster, Easier, and More Profitably"

Your monthly newsletter provided by John Hill, President and CEO of TechSage Solutions

What's Inside:

How To Make Sure You Never Fall Victim To Ransomware

Late last March, the infrastructure of Atlanta was brought to its knees. More than a third of 424 programs used nearly every day by city officials of all types, including everyone from police officers to trash collectors to water management employees, were knocked out of commission. What's worse, close to 30% of these programs were considered "mission critical," according to Atlanta's Information Management head, Daphne Rackley.

The culprit wasn't some horrific natural disaster or mechanical collapse; it was a small package of code called SAMSAM, a virus that managed to penetrate the networks of a $371 billion city economy and wreak havoc on its systems. After the malicious software wormed its way into the network, locking hundreds of city employees out of their computers, hackers demanded a $50,000 Bitcoin ransom to release their grip on the data.

While officials remain quiet about the entry point of SAMSAM or their response to the ransom, within two weeks of the attack, total recovery costs already exceeded $2.6 million, and Rackley estimates they'll climb at least another $9.5 million over the coming year.

It's a disturbing cautionary tale not only for other city governments, but for organizations of all sizes with assets to protect. Atlanta wasn't the only entity to buckle under the siege of SAMSAM. According to a report from security software firm Sophos, SAMSAM has snatched almost $6 million since 2015, casting a wide net over more than 233 victims of all types. And, of course, SAMSAM is far from the only ransomware that can bring calamity to an organization.

If you're a business owner, these numbers should serve as a wake-up call. It's very simple: in 2018, lax, underfunded cyber security will not cut it. When hackers are

Continued on pg.2

Continued from pg.1

ganging up on city governments like villains in an action movie, that's your cue to batten down the hatches and protect your livelihood.

The question is, how? When ransomware is so abundant and pernicious, what's the best way to keep it from swallowing your organization whole?

1. BACK UP YOUR STUFF

If you've ever talked to anyone with even the slightest bit of IT knowledge, you've probably heard how vital it is that you regularly back up everything in your system, but it's true. If you don't have a real-time or file-sync backup strategy, one that will actually allow you to roll back everything in your network to before the infection happened, then once ransomware hits and encrypts your files, you're basically sunk. Preferably, you'll maintain several different copies of backup files in multiple locations, on different media that malware can't spread to from your primary network. Then, if it breaches your defenses, you can pinpoint the malware, delete it, then restore your network to a pre-virus state, drastically minimizing the damage and totally circumventing paying out a hefty ransom.

2. GET EDUCATED

We've written before that the biggest security flaw to your business isn't that free, outdated antivirus you've installed, but the hapless

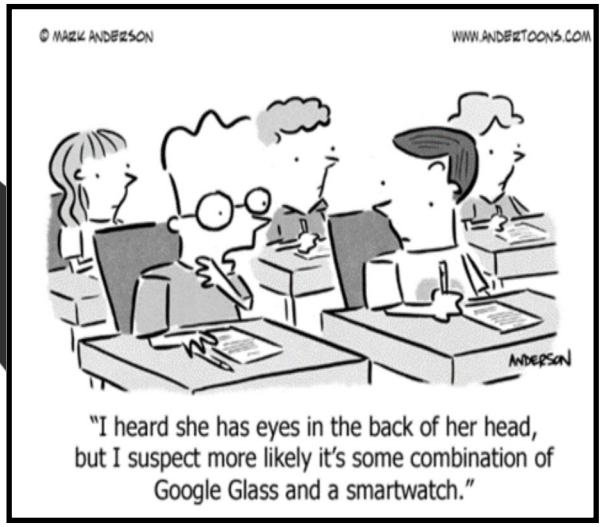
employees who sit down at their workstations each day. Ransomware can take on some extremely tricky forms to hoodwink its way into your network, but if your team can easily recognize social engineering strategies, shady clickbait links and the dangers of unvetted attachments, it will be much, much more difficult for ransomware to find a foothold. These are by far the most common ways that malware finds it way in.

3. LOCK IT DOWN

By whitelisting applications, keeping everything updated with the latest patches and restricting administrative privileges for most users, you can drastically reduce the risk and impact of ransomware. But it's difficult to do this without an entire team on the case day by day. That's where a managed services provider becomes essential, proactively managing your network to plug up any security holes long before hackers can sniff them out.

The bad news is that ransomware is everywhere. The good news is that with a few fairly simple steps, you can secure your business against the large majority of threats.

"The question is, how? When ransomware is so abundant and pernicious, what's the best way to keep it from swallowing your organization whole?"



SHINY NEW GADGET OF THE MONTH

Clocky

The Alarm Clock On Wheels

Waking up can be difficult. Even the most driven people occasionally struggle to get out of bed in the morning, pounding the snooze button ad infinitum until we finally force ourselves upright, dazed and groggy from interrupted sleep.

That's where Clocky, the alarm clock on wheels, comes in. Clocky is an adorable little digital timekeeper to keep by your bed; it will be your best friend until it comes time to rise in the morning. By default, it'll give you a single press of the snooze for free, but once you hit snooze for the second time, it'll speed off and start wheeling around your room, beeping and making a racket until you catch it and send it back to sleep. If you or someone you know struggles to get out of bed in the morning, Clocky will be a trusted ally in your mission to start the day.

4 Ways To Keep Your Team Inspired

Entrepreneurs and business leaders often find that motivating team members is one of the most challenging parts of the job. Leaders seldom lack self-motivation — it's so second nature to them that they get frustrated when a team member doesn't appear to have the same level of drive and ambition.

One of the most frequently asked questions I hear from business leaders is "How can I motivate my team?" Imagine their surprise when I tell them, "You can't." My responsibility as a coach is to help company leaders grasp the underlying reasons for their own motivation and ensure that those reasons are consistent with the goals and objectives of their business. In the same way, leaders need to stop looking for ways to motivate and instead find ways to inspire team members to seek out their own motivation.

Business leaders must understand that team members will not always share their outlook or passion. Instead of forcing your will on others, use these four approaches to inspire motivation in your team.

1 Lead by example.
Show your team members how it's done, and dedicate yourself to showing your passion and motivation in everything you do. When your team members see your genuine excitement and enthusiasm, they'll be much more likely to increase their energy levels and get on board.

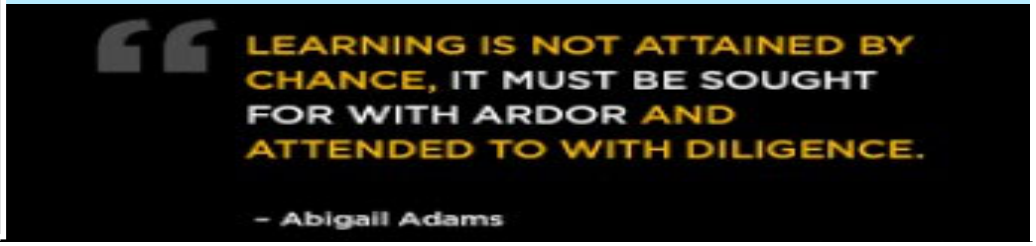
2 Honesty is the best policy.
It's vital that you be open and honest about the task at hand. You must get your team members to understand why the task is so important to you personally and to the company as a whole. Not every goal, task, or objective will foster the same amount of excitement and teamwork. If what you want is challenging or risky, let your team know. They'll respect your transparency and be more likely to trust you and your leadership.

3 Find balance.
There are two surefire ways to destroy motivation among team members. The first is micromanaging, and the second is being so hands-off that your team doesn't know what to do when problems arise. Give your team the freedom they need to feel empowered, but stay involved so that you can provide the necessary guidance when team members get discouraged.

4 Expect results and celebrate victories.
Before you give your team their marching orders, let them know you have confidence in their abilities. Take time to explain why a successful outcome is important to you and the business. They'll be more likely to meet your expectations, not because they're doing it for your sake, but because they're working harder for the benefit of the team as a whole.

It's crucial to celebrate wins with the team and to express your appreciation. An individual reward can be a great motivational tool, but it's just as important that you celebrate as a team.

Andy Bailey is the founder, CEO and lead business coach at Petra, an organization dedicated to helping business owners across the world achieve levels of success they never thought possible. With personal experience founding an Inc. 500 multimillion-dollar company that he then sold and exited, Bailey founded Petra to pass on the principles and practices he learned along the way. As his clients can attest, he can cut through organizational BS faster than a hot knife through butter.



Why Upskilling Is The Future Of Business

Although your top performers may have been with your company for years, that doesn't necessarily mean they're equipped to steer your business into the future and transform the organization from the ground up. It's tempting, when you're looking at under skilled employees to consider hiring a team of fresh new faces. But, in most cases, that's a mistake.

Today, instead of relying on new hires, savvy companies like Cognizant and AT&T are turning to upskilling to deepen the talent and loyalty of key employees. The use personalized, engaging educational programs with specialized training modules to grow each employee's skill set. By using modern technology like Artificial Intelligence to sharpen training programs, you can tailor training techniques to the individual, instead of using a one-size fits all approach.

Forbes.com, 7/25/2018

All Businesses Should Have This In Place

All businesses are at risk especially small businesses. Cyber criminals know that small businesses think they would not be a victim of a cyber incident, which makes them a huge target.

The National Institute of Standards and Technology (NIST) is a federal agency charged with leading the development of technology standards with public and private sector. NIST developed a cybersecurity framework for organizations to better manage and reduce cybersecurity risk.

The cybersecurity framework is based on five categories.

Credit: N. Hanacek/NIST

1) Identify– Determine what assets are to be protected. Is this documented?
2) Protect—Access controls in place, cyber security training, security processes and procedures, maintenance.
3) Detect—Do you have a way to detect a cyber incident? What is your procedure once it is detected?
4) Respond—Every business, regardless of size, needs to have a respond plan in place before an event happens. Most businesses have plans to continue business if there is lost of electricity or weather conditions, how about if your data is compromised.
5) Recover—The goal is to quickly go back to normal operations from a security incident. Do you have multiple monitoring devices to prevent the hacker from returning (which is not uncommon)? Does the business have cyber insurance?

I will expand on more of the five categories in the future newsletters.

Refer a friend from now through December 31, 2018 Get a $25 Gift Card & You'll Be Eligible to WIN a

How the Contest Works:

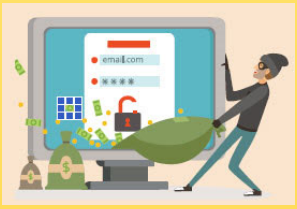
1) Call or email us with your referral information and receive $25 gift card.
2) We will call your friend to schedule an appointment. If an appointment is made, we will send you a $50 gift card.
3) After the appointment we will add your name into the drawing for Sonos-PLAY3: Wireless Speaker for Streaming Music.
4) If your friend becomes a client and spends $1,000 or more, we'll send you a check for $100. As a bonus, we'll also give your friend a $100 discount off our services!

What makes a good referral for TechSage Solutions?

A business owner who has 5 or more PC's and needs help with their network, data backups, phones, email, data security, etc. or is just interested in having a second opinion on how they are doing things now. We provide service to the San Antonio area and surrounding cities.

Send email to info@techsagesolutions.com or call (210)-582-5814

2 Sneaky Ways Hackers Rob You Blind



We've said it before, and we'll say it again: cyber-attacks aren't limited to big corporations and government organizations. Verizon's 2018 Data Breach Investigations Report states that 58%of data breaches in 2017 occurred at small businesses. And according to Verizon's data, there are two specific hacking techniques on the rise today that small businesses should know about.

The first technique is point-of-sale (POS) system hacking. If you're in the hospitality industry, this should definitely be on your radar. Verizon recorded 368 POS incidents in 2017, most instigated by hackers penetrating the system rather than employees making mistakes that opened up vulnerabilities. Usually, hackers will steal credentials directly from a POS service provider, which enables them to exploit the POS systems used by that provider's customers.

The second is called financial pretexting. Instead of phishing a business and installing malware, attackers impersonate a high-level employee within an organization - often using a legitimate but compromised e-mail account - to steal funds or sensitive information from the company's finance or HR department.

As always, forewarned is forearmed. Equip your teams with the know-how to avoid these scams, and you will be ahead of the game. *SmallBizTrends.com, 5/1/2018*