



Regular updates on IT for modern growing organizations

March 2017

IN THIS ISSUE...

- INCS News
- Value of Trust
- 11 Foot Ladder
- Your Best Defense
- The Corner Office
- Patching the Holes
- Did you know?

INCS NEWS

Welcome to our new clients, we're thrilled to have you as part of the growing INCS family! We always feel honored to have another organization put their trust in us to serve their technology needs. We see that as a fulfilment of our mission: To bring affordable, safe and reliable IT to modern growing organizations.

We also welcome our newest employee, Danielle Hoff-Black. Danielle will be splitting her time between the help desk and running our social media, including LinkedIn, Twitter and Facebook. She's also going to make it more likely that when you call us, you'll get to speak to a live human being! It may be old-fashioned, but we believe that it's important, especially when you need help with your technology. So, come on in and see what's up—thanks for being with us!

VALUE OF TRUST *JIM BRENDLE, INCS PRESIDENT*

Why do our clients do business with INCS?

In my opinion, it all boils down to *Trust*. Our clients *trust* us because:

- We know our industry and stay current with proven IT solutions
- We take the time to comprehend all pieces of the IT puzzle as it relates to our client's network and applications
- We serve our client's best interest first and foremost
- We have an expert understanding of compliance regulations, cyber- security, business continuity, disaster recovery and more
- We provide an account manager that knows our client's business
- We employ certified and experienced IT architects, engineers and support personnel so we can provide fast and accurate support
- We will not over-charge and will always be fair
- We will make the tough decisions, keep organized, profitable and in business so we can continue to serve our client's needs

These are just to name a few.

"Trust" from an IT company? Are you kidding? (continued next page)



Trust is the bedrock of every client relationship we are privileged to enjoy

Value of trust (continued)

There are a lot of IT companies out there to choose from. How do you know when you have chosen the right company to support your business? Many business owners simply choose by price alone, while others will pick someone (usually a sales person) that they like, or maybe a company that was referred by someone. Over time, business owners will learn if there is *trust* or doubt. Sometimes these hard lessons learned can cost a business more than they even know. Stick with a company that is focused on being your trusted partner.

"If you don't have trust inside your company, then you can't transfer it to your customers." --Roger Staubach

THE 11-FOOT LADDER BRIAN ALLISON, SALES AND MARKETING MANAGER

81%

of the hackers we interviewed said they could identify and exfiltrate your data in less than 12 hours.

The cyber security firm Nuix prepared a recent report where they did live interviews with so-called "White Hat" hackers at an infamous annual hacking convention. More than 4 out of 5 of those interviewed said they could penetrate any network, find and extract the most valuable information and



be out and done in 12 hours. "White Hats," work legally, being paid by the target to penetrate their own network. Here is what these interviews revealed:

It's essentially a re-statement of the age-old sentiment, you can pay me now or pay me (much more) later. Not to be too alarmist, but clearly attacks are increasing across the board. No data is completely safe.

Some of the other important findings are:

1. 50% of the hackers used a different technique for every attack
2. 84% use social engineering—compromising people to get the target to help with the attack
3. 69% say they are almost never caught by the existing security team

"The only difference between me and a terrorist is a piece of paper. The attacks, the tools, the methodology; it's all the same. Besides, I'm far too pretty to be in jail."

Read the rest of the article on our blog: www.incsNOW.com/blog.

"Every time we build a 10-foot wall, the bad guys build an 11-foot ladder." (Silicon Valley police)

"ENCRYPTION IS YOUR BEST DEFENSE" SAYS FEDERAL HHS

Clinicians and other healthcare professionals don't want to be encumbered by security processes that detract from the time they spend with patients. Safeguarding protected health information is a provider's responsibility; unfortunately, more than 81 percent of providers acknowledged their organization was attacked within the past two years. A weak state of security jeopardizes patients' physical and digital security, but healthcare organizations can now protect patients and their own reputation with easy-to-use security.

The need for more security comes at a time when healthcare professionals increasingly rely on more digital data flowing from cloud, mobile, patient monitoring, and other sources. "Encryption is one of the most powerful tools available to security professionals seeking to protect sensitive information from unauthorized disclosure," according to Certification Magazine. (continued next page)

Encryption (continued)

“Our message to these organizations is simple: Encryption is your best defense against these incidents,” said Susan McAndrews, Deputy Director of Privacy on HHS.gov

Susan McAndrews is the Deputy Director of health information privacy at the Office of Civil Rights, quoted above from HHS.gov (the U.S. Department of Health and Human Services). HHS has also announced that, absent convincing proof otherwise, any successful ransomware encryption attack will be considered a breach of patient records - the medical practice has lost control of patient information. Breaches of patient records can invoke rules on patient and public notification, with a flurry of difficult media attention. Providers must now document and explain their decision not to implement encryption, according to HealthITSecurity.com.

Because of our security-first approach, INCS is a leading provider of certified Sophos solutions in our area. Sophos lets us give you a complete range of security solutions that actively work together to keep you safe.

THE CORNER OFFICE - CEO TO CEO COMMUNICATION *JIM BRENDLE, PRESIDENT*

As I was playing a friendly game of 7-card stud poker in the MGM hotel in Las Vegas, a popular player told me, “You don’t have to be giant to be big in your own or other people’s eyes.” I didn’t understand. I was young and thought bigger was better. We had our IT solution and it was great for our customers. Gradually I realized that to be a big success, in my industry or personally, required both industry knowledge and a focus on other skills like: Relationships, trust, caring, consistency and dependability. My personal life taught me to be a better business man and vice versa. Different people have different levels of success. To me, someone that can balance “happy” with their business and their personal life has accomplished something gigantic. By the way, this “popular player” was Mel Gibson, soon after his film *Maverick* was released (he is a very short person in stature, but a giant in other ways—just not a very good poker player).



“Chris and INCS have been fantastic for our firm. The expertise, responsiveness, foresight and professionalism are unmatched. We’ve been with them for over 15 years now and it’s been a great relationship” (Dozier Miller Pollard & Murphy law)

PATCHING THE HOLES *DENNIS ESSELMAN, SENIOR ACCOUNT EXECUTIVE*

You hear a lot about “patching,” but what is it and what gets patched and why? A modern computer with an office suite is running about 100 million lines of computer code, providing hundreds of hidden services just from booting. All that software, all the way down to the firmware running on the circuit boards, needs to be updated to make improvements and fix mistakes—that’s what patching is.

Patches are applied generally to improve the performance of the system, but many of them are specific to security. A flaw may have been found in the way the code was written, and these flaws are routinely fixed by every reputable software company. The problem now is that security holes are widely known, and the bad guys can figure out how to attack them. A patch can make the attack fail, but it only provides protection if it’s actually installed on your system. Most attacks are against a known and fixed hole—but the patch was never applied. There are all kinds of nasty malware in the world, and they want to crawl through that hole and break things.

(continued next page, bottom)



3743 Latrobe Drive
Charlotte, NC 28211

Recipient Name
Street Address
City, ST ZIP Code

Find out how the affordable security-first services from INCS keep your data and your reputation safe. Call us at 704-362-1682, or on the web at www.incsNOW.com

Patching the Holes (continued)

To be effective, patching must be both systemized and screened. Having an automated way to do this for all the most popular packages is the most effective way to see that patching is always current. Because of the complexity of all the different software programs working together, some patches break things. This is why patches need to be tested and screened across different vendors before they are installed.

If you need help with this, INCS can identify issues within your current computer technology. We provide a service that quickly screens patches as they become available, and then applies them to every system you have. It's automated and ensures systems are not riddled with the kind of holes the bad guys are looking for.

Read more on our blog: www.incsNOW.com/blog

DID YOU KNOW?

INCS can provide telephone systems, internet connectivity and voice circuits? Large scale warranty and maintenance solutions? Cloud and other storage solutions? Consulting and resource management? Business continuity and disaster recovery? Hardware, networking and software solutions? All this and more...

Whatever your technology needs are, we know how to find a great fit for your business. Let our experts help!