BSSi2 Innovations
Review Twice, Implement Once. Doing IT Right the First Time.

How To Make Cyber Security An Ingrained Part Of Your Company Culture

Your employees are your first line of defense when it comes to protecting your business from cyberthreats. Human error is one of the single biggest culprits behind cyber-attacks. It comes down to someone falling for a phishing scam, clicking an unknown link or downloading a file without realizing that it's malicious.

Because your team is so critical to protecting your business from cyberthreats, it's just as critical to keep your team informed and on top of today's dangers. One way to do that is to weave cyber security into your existing company culture.

How Do You Do That?

For many employees, cyber security is rarely an engaging topic. In truth, it can be dry at times, especially for people outside of the cyber security industry, but it can boil down to presentation. That isn't to say you need to make cyber security "fun," but make it interesting or engaging. It should be accessible and a normal part of the workday.

Bring It Home For Your Team. One of the reasons why people are often disconnected from topics related to cyber security is simply because they don't have firsthand experience with it. This is also one reason why many small businesses don't invest in cyber security in the first place – it hasn't happened to them, so they don't think it will. Following that logic, why invest in it at all?

The thing is that **it will eventually happen**. It's never a question of if, but **when**. Cyberthreats are more common than ever. Of course, this also means it's easier to find examples you can share with your team. Many major companies have been attacked. Millions of people have had their personal data stolen. Look for examples that employees can relate to, names they are familiar with, discuss the damage that's been done.

If possible, bring in personal examples. Maybe you or someone you know has been the victim of a cyber-attack, such as ransomware or a data breach. The closer you can bring it home to your employees, the more they can relate, which means they're listening.

Collaborate With Your Employees. Ask what your team needs from you in terms of cyber security. Maybe they have zero knowledge about data security and they could benefit from training. Or maybe they need access to better tools and resources. Make it a regular conversation with employees and respond to their concerns.

Continued on the next page...

...continued from the previous page.

Part of that can include transparency with employees. If Julie in accounting received a phishing e-mail, talk about it. Bring it up in the next weekly huddle or all-company meeting. Talk about what was in the e-mail and point out its identifying features. Do this every time phishing e-mails reach your employees.

Or, maybe Jared received a mysterious e-mail and made the mistake of clicking the link within that e-mail. Talk about that with everyone, as well. It's not about calling out Jared. It's about having a conversation and not placing blame. The focus should be on educating and filling in the gaps. Keep the conversation going and make it a normal part of your company's routine. The more you talk about it and the more open you are, the more it becomes a part of the company culture.

Keep Things Positive. Coming from that last point, you want employees to feel safe in bringing their concerns to their supervisors or managers. While there are many cyberthreats that can do serious damage to your business (and this should be stressed to employees), you want to create an environment where employees are willing to ask for help and are encouraged to learn more about these issues.

Basically, employees should know they won't get into trouble if something happens. Now, if an employee is blatantly not following your company's IT rules, that's a different matter. But for the day-to-day activities, creating a positive, educational, collaborative environment is the best way to make cyber security a normal part of your company culture.

Plus, taking this approach builds trust, and when you and your team have that trust, it becomes easier to tackle issues of data and network security – and to have necessary conversations.

Need help creating a cyber security company culture that's positive? Don't hesitate to reach out to your managed services provider or IT partner! They can help you lay the foundation for educating your team and ensure that everyone is on the same page when it comes to today's constant cyberthreats.

On the Lighter Side

A reporter asked Michael Jordan if his Bulls teams of the '90's could beat the NBA champs of today.

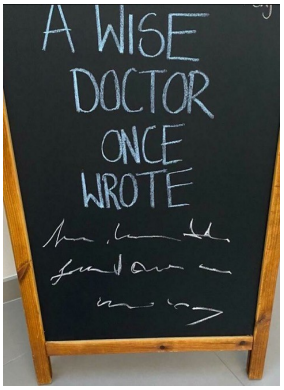
MJ replied, "Absolutely"!

"How much would you beat them by", the reporter asked?

MJ answered, "By 2 or 3 points".

The reporter queried, "Why so close"?

MJ snickered as he answered, "Well, most of us are close to 60 now"!



Recent Phishing Attacks Using PDF Files Have Skyrocketed More Than 1,000%

Phishing attacks using PDF files have spiked over the past year, according to researchers at Palo Alto Networks' Unit 42.

"From 2019-20, we noticed a dramatic 1,160% increase in malicious PDF files – from 411,800 malicious files to 5,224,056," the researchers write. "PDF files are an enticing phishing vector as they are cross-platform and allow attackers to engage with users, making their schemes more believable as opposed to a text-based email with just a plain link."

The most common form of PDF phishing lures used an image of a fake CAPTCHA to trick victims into clicking the "Continue" button, which led to a malicious site. Another variant used an image that purported to be a coupon, and told victims to click the image in order to get 50% off on a product.

A third type of PDF phishing attack used images that appeared to be paused videos, but led to a phishing site when users clicked on them.

"These phishing files do not necessarily carry a specific message, as they are mostly static images with a picture of a play button ingrained in them," Unit 42 says. "Although we observed several categories of images, a significant portion of them either used nudity or followed specific monetary themes such as Bitcoin, stock charts and the like to lure users into clicking the play button."

The researchers conclude that users need to pause and think when they receive a suspicious file.

"Data from recent years demonstrates that the amount of phishing attacks continues to increase and social engineering is the main vector for attackers to take advantage of users," the researchers write. "Prior research has shown that large-scale phishing can have a click-through rate of up to 8%.

Thus, it is important to verify and double check the files you receive unexpectedly, even if they are from an entity that you know and trust. For example, why was your account locked out of nowhere, or why did someone share a file with you when you least expected it?"

New-school security awareness training can give your employees a healthy sense of skepticism so they can avoid falling for these attacks.

Blog post with links:
https://blog.knowbe4.com/phishing-attacks-using-pdf-files-have-skyrocketed

Business Tidbit

How To Know It's Time To Start Scaling Your Business

Creating a business that is scalable isn't easy, but it's necessary if you intend to grow – and grow some more. There are three simple ways to tell if you've created a business that is scalable.

You Have Positive Cash Flow Figured Out. You've successfully built a reliable month-to-month revenue stream. It's money that you can use to invest further into your business – whether it's to pay for additional employees, technology, systems and processes or all of the above.

Everything Has Been Delegated. Delegating is hard for many entrepreneurs. You want to have a hand in everything. But when your team keeps everything running – and everything runs even when you're not there – you're in a great place to scale up.

You Have More Control Over The People You Get To Work With. Basically, you can start to shape your client base. If there is someone you want to say no to (say you don't have the full resources to fulfill their needs or they're just not a great fit), you can move on guilt-free.

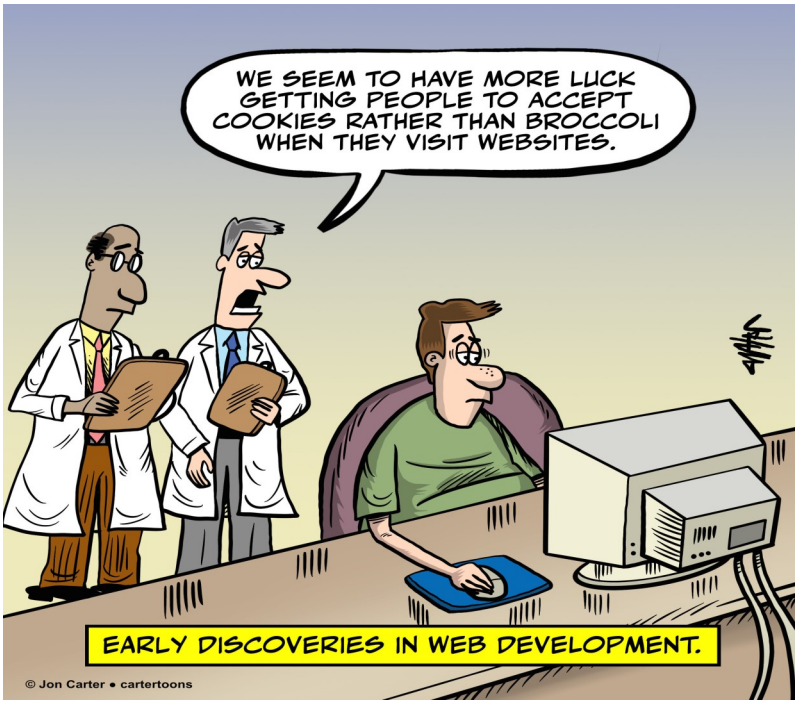
If you have these three things in place, you have the foundation to scale up safely and to create the business you've always wanted.

Forbes, Feb. 11, 2021

May 2021

35 Aztec Court
South Barrington, IL 60010
(312) 752-4679
www.bssi2.com

"We make all of your computer problems go away without the cost of a full-time I.T. staff"



Shiny New Gadget of the Month

The Pocket Translator: MUAMA ENENCE

It used to be science fiction, but not anymore! Now, you can translate languages on the go! The Muama Enence is the device that makes it possible. This handheld "listener" is capable of real-time translation of over 36 common languages from around the globe. Smaller than a smartphone, the Muama Enence breaks language barriers and makes travel easier than ever before, whether you're traveling for business or for vacation.

The Muama Enence is super-easy to use and ultra-portable. All you need to do is press a button, and it does the rest. Plus, with excellent audio quality, you'll be able to hear the translation, even when things get busy around you. Learn more – and get your own – at **bit.ly/37hhn8R**.

Stay up-to-date with the latest Cybersecurity News!

Follow our Chief Security Fanatic and CIO, Nick Espinosa, on social media for cybersecurity videos and articles:

f www.facebook.com/NickAEsp

twitter.com/NickAEsp

in www.linkedin.com/in/nickespinosa/

Follow BSSi2 at:

f www.facebook.com/bssi2

twitter.com/BSSi2llc