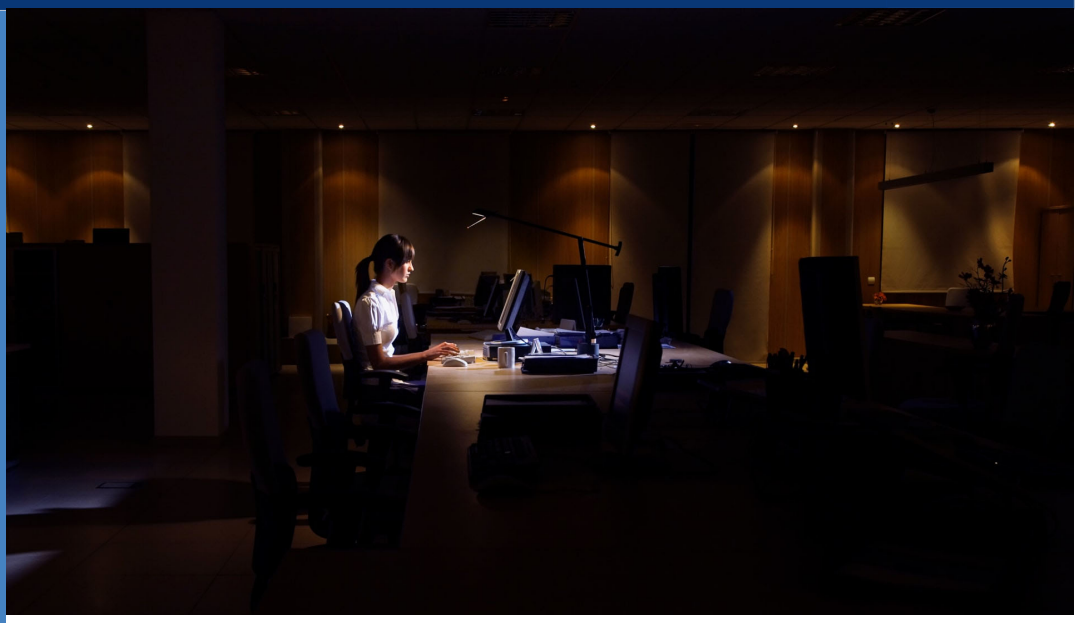
DTS DanTech Services
Computers under control!™

Technology Times August 2021 Issue

"With over 20 years of experience providing remote support to clients that rely on technology, I know what it takes to deliver business continuity. Add to that another 20 years of support in the service industry you'll not find another company that takes customer service to heart as I do. Find out for your business what a difference it makes. "

What's Inside:

Got IT Problem? - Click Here!



Cyber Insecurity Is a Big Problem for Small Business. This House Bill Seeks to Lessen the Impact

The legislation would boost information sharing among businesses and federal institutions.

Small businesses hit with cyberattacks may soon get a helping hand from the federal government.

A bipartisan bill introduced this week by House Small Business Committee Chairwoman Nydia M. Velázquez (D-NY) and Representative Byron Donalds (R-FL) is aimed at increasing information-sharing between small businesses and the federal government. While the full text of measure H.R. 4513 has not been made available, both of the bill's co-sponsors released statements that offer an early glimpse of what's to come.

The bill would allow the Small Business Administration's Small Business Development Centers (SBDC), which serve as local resource centers for entrepreneurs, to collect information from small businesses on cyberattacks. Under the measure, any business that shares information with an SBDC is entitled to the same protection as other entities under the law. Finally, the bill provides liability protections for small businesses that share information.

The bill has some urgency, given the rise of cyberattacks among small businesses in the last few months. The pandemic fueled the problem, as more people tended to work from home and vulnerabilities grew accordingly, a mid-year cybercrime report from security firm Sontiq shows. The study found that small, less widely reported data breaches resulted in the loss of the most significant levels of information, including personal identifiable information (PII) such as social security numbers and mailing addresses.

- Continued on page 4

SIX-STEPS PROBLEM SOLVING MODEL

If it is simplicity that you are after, the six-steps problem solving model is a great place to start. This is all about the basics of problem solving – each of the six steps will take you a bit closer to a positive outcome. This model might not be complex enough for your needs, but you may be surprised to find just how many times this technique is able to do the job.

To give you a better understanding of how the six-step problem solving model works, let's quickly walk through each of the six steps.

- Define the problem. Obviously, you aren't going to get far if you don't know what the problem is that you are trying to solve. Take some time at this first step to understand the problem on a deeper level so you will be able to take logical action later on.
- Determine the root cause. This is an important step that is frequently missed when individuals or teams are trying to solve problems. What is it that is causing you to wind up in this situation? Is there just one root cause, or is it a combination of issues coming together negatively?
- Develop alternative solutions. At this point, you aren't trying to find the single answer to the problem – instead, you are trying to find all possible answers. Anything which you believe may be able to help you solve this issue should be on the table at this point.
- Select a solution. Now that you have a list of possible solutions to consider, you can pare them down and wind up picking out the one which you believe will resolve the matter.
- Implement the solution. With your choice made, it's now time to put that choice into action and see what happens. Of course, implementation itself can be a complex process which may require its own methods and tools to work through successfully.
- Evaluate the outcome. This is important. Once you implement a solution, you need to follow through with that solution to make sure it actually worked. If not, you may need to go back and consider one of your other potential solutions that was identified in step three.

There is nothing particularly complex about the six-step problem solving method, but that is exactly what makes it so effective. Take your time on each step, seek out collaboration as necessary, and trust the model to lead you to a wise choice.

The Lost Art of Keeping Your Word

By Mark Sanborn

The chasm between "promises made" and "promises kept" seems to keep widening. Consider:

- How many times have you unsubscribed from emails and continued to receive them?

I've noticed that a high number of "unsubscribes" are illusionary.

- How often have you met with a vendor who promised a quote or proposal that you never heard from again?

We've all had that experience of wasted time, for me, more than I care to remember.

- When was the last time somebody said, "I'll get that to you," and then didn't?

Recently? It happens too often.

- A company uses a pre-recorded message to explain their commitment to customers when you reach their automated customer help system.

But the system wears you out with prompts, takes an egregiously long time and then cuts you off before you get the needed help.

- A prospect requests a product be overnighted but when you call to make sure they received it, they don't return your call.

How hard is it to say, "Got it, thanks"?

- Another potential client asks you to tentatively hold a date for an engagement. As the date approaches you call and email to confirm that they still want the date yet you can't get a response of any kind.

A simple email saying, "No thanks, we've changed our mind," would have prevented much aggravation and wasted time.

If someone starts to talk about people not keeping their word, they sound like prehistoric throwbacks. Yet while I've not seen hard data, I'd wager that the keeping of one's word is ill if not on life support. If I tally the number of times people I encounter don't do what they say they will, I get nearly depressed.

Some behaviors go out of style or become displaced by better options. Keeping your word isn't one of them. Integrity as I like to remind myself and others is the distance between your lips and your life. **Don't make promises you can't or won't keep.** Dedicate yourself to saying what you will do and then doing it. Keeping your word has always mattered, still matters and always will.

Shiny New Gadget Of The Month:

Belkin Magnetic Phone Mount with Face Tracking

Snap your iPhone 12 onto this magnetic phone mount with face recognition tracking that rotates and adjusts to shoot content from any angle. The accompanying app follows your movements while you record and links directly to your social media channels.

This motorized phone stand will pair with your iPhone 12's face-tracking to follow you around a room while you strut your stuff on TikTok (no? Us neither), film a YouTube video or make a Zoom call.

It capitalizes on the iPhone 12's MagSafe tech, so you can just magnetically snap the phone into place and get going.

Are You're Worried About Safety Of Your Business Data?

HOW TO PROTECT YOUR SMALL BUSINESS FROM HACKERS

What would happen if a hacker decided to launch a cyber attack against your business? Would they be successful? Would your company information be safe? Are you confident in the security you have in place? While you might think cyber security is just a concern for large businesses, small businesses are more at risk and susceptible to cyber crime. In fact, 43% of cyber attacks target small businesses.

If you're a small business owner, you can't ignore these statistics. Many believe their business is too small to deal with cyber security issues, but hackers target small businesses, too. Your business might not be as big as Starbucks, but you have something hackers want — employee and customer payment information. Here are some ways to take control of your business' information and fight off hackers.

GET INSURANCE* It's not just for your home and car — your business needs cyber security insurance, too. Cyber liability insurance is designed to protect your business from various cyber security threats. If there's a breach and your company is held liable, you may end up having to pay thousands of dollars in a lawsuit. This can significantly harm your business financially. However, if you have the right type of insurance, your legal costs will be covered.

DEVELOP A PASSWORD STRATEGY* One way hackers can intrude your system is through employee passwords. Often times, many passwords are way too simple. It's important to educate your team on the proper way to use passwords to avoid a cyber attack. While you may not be able to avoid every single hacker, you can slow them down by creating a secure system to discourage a hacker.

BACKUP YOUR FILES* No system is completely secure, so creating offline backups of sensitive files is vital. That way, if your computer is hacked, you'll still have access to your files. It's recommended to backup your online data with a program that uses "versioning." This allows you to see different versions of files, and most crypto viruses and malware look for local devices.

PROTECT YOUR WIRELESS NETWORK* If your small business has a wireless network, your access point is probably a cable or modem connected to a wireless router. This directs traffic between your local network and the internet. Any devices within range can pull the signal and access the internet, which is when hackers gain easy access to information. To prevent this, change the name of your router from default to something unique that only you know. In addition, it's imperative to keep your router's software up to date. To do this, visit the manufacturer's website to see if there is a new version of the software available for download. Once you've set up your router, log out as the administrator to lessen to risk of a stranger gaining control of your device.

PLAN AHEAD* Knowing what to do if something goes wrong is a necessary precaution to prepare before a hacker gets into your business' system. Planning ahead on what steps to take before a crisis happens can help minimize the damage if you discover malware on your computer, find out your email has been hacked or if there is a data breach. In addition to these steps, test your security. Check your software for viruses and other malicious programs and consider installing a network firewall to control incoming and outgoing network traffic. Talk to an IT expert and seek advice on what tools best suit your small business to ensure safety. While there's no bulletproof way to prevent a hacker from gaining valuable information from your company, there are many ways to slow down and avoid a hacker attack. Training employees on the importance of cyber security can prevent miscommunications and fixable mistakes. It can be easy to overlook the simple steps but keeping cyber security top of mind can reduce the risk of a data breach. Is your sensitive information safe now?

*** DanTech Services has services and solutions. Call 907-885-0500 x 1**

- "Cyber Insecurity Is a Big Problem for Small Business"

- Continued from Page 1

"Small businesses, in particular, were not as well-equipped to fend off cyberattacks," Jim Van Dyke, senior vice-president of financial wellness at Sontiq, said in a statement. "Most people do not realize how dangerous these small-scale data breaches can be."

Velázquez would echo that sentiment. "Unfortunately, small businesses often lack the resources needed to develop adequate cybersecurity strategies and are reluctant to report cyber threats to the federal government," she said in a statement. "This bill will encourage collaboration and information sharing between small businesses and the federal government, helping to protect small firms that are vulnerable to cyber-attacks."

The bill has been referred to the House Committee on Small Business, which will eventually debate the proposal, adopt any amendments, and vote on approval. A markup date has yet to be scheduled.

By Amrita Khalid, www.inc.com

Patch Management Software and Tools

NEED REMOTE IT SUPPORT AT YOUR HOME?

Call us about our residential service offering.

907-885-0500

Next Level of Informational Security For Your Business

SIEM stands for security information and event management and provides organizations with next-generation detection, analytics and response. SIEM software combines security information management (SIM) and security event management (SEM) to provide real-time analysis of security alerts generated by applications and network hardware.

SIEM software matches events against rules and analytics engines and indexes them for sub-second search to detect and analyze advanced threats using globally gathered intelligence.

This gives security teams both insight into and a track record of the activities within their IT environment by providing data analysis, event correlation, aggregation, reporting and log management.

SIEM software can have a number of features and benefits, including:

- Consolidation of multiple data points
- Custom dashboards and alert workflow management
- Integration with other products

How does SIEM work? SIEM software works by collecting log and event data generated by an organizations applications, security devices and host systems and bringing it together into a single centralized platform. SIEM gathers data from antivirus events, firewall logs and other locations; it sorts this data into categories, for example: malware activity and failed and successful logins. When SIEM identifies a threat through network security monitoring, it generates an alert and defines a threat level based on predetermined rules.

For example, someone trying to log into an account 10 times in 10 minutes is ok, while 100 times in 10 minutes might be flagged as an attempted attack. In this way it detects threats and creates security alerts.

SIEM use in compliance. Tighter compliance regulations are pushing businesses to invest more heavily in IT security and SIEM plays an important role, helping organizations comply with PCI DSS, GDPR, HIPAA and SOX standards.

IoT security. The Internet of Things (IoT) market is growing. Most IoT solution vendors provide API and external data repositories that can be easily integrated into SIEM solutions.

Prevention of insider threats. External threats aren't the only things that make organizations vulnerable, insider threats pose a considerable risk, especially considering the ease of access. SIEM software allows organizations to continuously monitor employee actions and create alerts for irregular events based on 'normal' activity.

Find out what Dantech Services, Inc SIEM could do for you over HERE