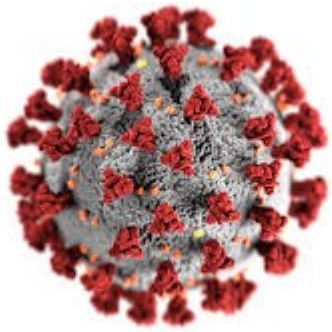
BSSi2

Innovations

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



Is COVID-19 Infecting the Internet?

By Scott Bernstein

I know what you are thinking "Are you nuts? How can COVID-19 infect the Internet? You cannot breathe on it." Hear me out, there's more to this than you think.

We have entered into a new era of work; **more people than ever are working from home**. Such a great perk (we agree, that is how BSSi2 has always operated). Companies can save money on office space, employees save money on commuting and oh yes, hackers will have a field day. You didn't think it was all roses did you?

When your staff is in an office, there is typically one single Internet Access Point. Your IT puts all their efforts and expertise in protecting that entry point, plus all the corporate controlled computers behind it. And as we well know, that is not always an easy task. But now that you have a larger remote workforce there is no single-entry point to protect; **it is every employees' home that needs protection**. As you can well imagine, that is more than a nightmare for the average IT person, who often is not a cybersecurity expert.

But it does not end there. IT departments do their best to put security measures in place but are often fighting a difficult battle. **Too many companies allow employees to use personal computers, not business class corporate controlled computers**, so there is some loss of security control. Those companies that take security seriously will put extra layers of protection in place. But guess what, **54% of employees will find workarounds when they feel security policies get in the way of them doing their jobs**. According to the Digital Guardian report, covering financial services, manufacturing, healthcare, and other businesses, **employees copied company data to USB drives 123% more than before the pandemic's onset**, with 74% of that data marked as "classified." Data egress over email, USB, and cloud services leaped 80%, with more than 50% of that data marked as "classified." And that is YOUR DATA.

Why does this happen? According to email security company Tessian in their The State of Data Loss Report, **some of the top reasons employees aren't completely following the same safe data practices** as usual include **working from their own device, rather than a company issued one, as well as feeling as if they can take additional risks because they're not being watched by IT and security**. In some cases, employees aren't purposefully ignoring security practices, but **distractions while working from home** – such as childcare, roommates and not having a desk set up like they would at the office – are having an impact on how people operate.

Meanwhile, some employees say they're being forced to cut security corners because they're under pressure to get work done quickly. "**People will cut corners on security best practices when working remotely and find workarounds if security policies disrupt their productivity in these new working conditions**," said Tim Salder, CEO of Tessian. "But **all it takes is one** misdirected email, incorrectly stored data file, or weak password, before a business faces a severe data breach that results in the wrath of regulations and financial turmoil." There is a saying from Dustin Dykes, founder of the Dallas Hackers Association: "**Security systems have to win every time, the attacker only has to win once.**"

People are working from home more, they have no one looking over their shoulders, they miss conversing with their cohorts so they take to doing more on the Internet, and not necessarily corporate approved activities. According to the Pew Research Center, 53% of Americans say the Internet was essential for them during the COVID-19 crisis and 34% said it was important (87% total). A little more YouTube here, a few more tweets there and a little more keeping up with friends on Facebook. And let's not forget about checking our personal email more often. Free offers, new apps to try, a few more new links to follow. What could possibly go wrong? **People are "sick" and tired of being cooped up and their primary relief comes via the Internet**. Welcome to the feeding ground of hackers and cyber criminals.

So where does COVID-19 come into play? Bored, unentertained or unemployed people result in more

Continue on the next page...

...continue from the previous page.

web surfacing, more malicious web sites waiting for you, more phishing attacks that are getting to people (less stringent protection), more chances for catching a computer virus. **There is an increase in COVID-19 related phishing attacks on home WiFi networks on personal computers that are typically not as secure as office computers** that are accessing corporate data that may contain confidential and personal information. This can be a feeding ground for the bad guys. And remember what I said earlier, it only takes one person to be hacked to help gain access to the corporate server and files. ONE.

In a recent article in Forbes by Stephen McBride (5/14/20), he is predicting the largest cyberattack in history will take place within 6 months. Some people say he is just spreading FUD (Fear Uncertainty Doubt) but many are not arguing. With growing numbers of not-so-well-protected home computers, you can see the chances have increased for breaches. Hackers breached the network of the USA's largest defense contractor, Lockheed Martin, by going after remote work-at-home employees.

Before you throw your hands up in the air and go running out of the room screaming what's the point, let me give you a few tips to help protect your staff. Nothing is 100% guaranteed but the more barriers you put in front of hackers, the more likely they will move on to easier targets.

- Insist on using corporate controlled and protected computers. It may mean buying more equipment, but the cost is far cheaper than a data breach.
- Do not use the corporate computer for anything but work (and keeps the kids off).
- Install business-class (i.e., paid) endpoint protection that is centrally monitored.
- Upgrade your firewall. Do not rely on the cable modem or retail purchased firewalls.
- Implement two-factor authentication (2FA) wherever possible.
- **PROVIDE YOUR STAFF WITH SECURITY AWARENESS TRAINING (online, critical point)**

There are more security steps to be taken but I did not want the list to be overwhelming and hard to follow. These protections add a little inconvenience but **how inconvenienced will you be if your servers and workstations are hit with ransomware or your bank account is emptied?** There is a trade-off.

Let BSSi2 help you with this strategy. **We are more than IT people; we are Security Fanatics.**

BSSi2 Employee Spotlight

We're happy to announce another new addition to the BSSi2 team:

Nykole Gault | Procurement Support

Hi! Nykole here. I've lived in the Chicago land area my entire life and furthest I've ever lived away is when I went to NIU. I graduated with a degree in Interactive Marketing from there and after jumping around different places I've found myself in IT. My family always said that I was a Jack-of-all-Trades but seemed to take to Photography and Software quicker then anyone they know. I'm personally a very timid person, but you would never guess as much if you saw me with people I trust. In my spare time I do Photography, Board Games, video games, and Duct Tape Crafts.

On the Lighter Side

June is already over? Julying

You should cut people born between June 21st and July 22nd out of your life… They're Cancer.

My wife and I just had a daughter and named her Junejulyaugust. We call her Summer for short.

How do we know that the ocean is friendly?
It waves!

Are people born with a photographic memory?
Or does it take time to develop?

A coworker named Celsius recently retired at my work, so they hired a guy named Kelvin to replace him.
He's the new temp. Seems like a cool guy.

Has anyone else's gardening skills improved during this quarantine like mine have?
I planted myself on the sofa at the start of April and I've grown bigger ever since.

The Many Faces of Corporate Leaders

Employees' happiness at work is more important in the workforce than ever before, and that feeling of fulfillment and engagement often comes from the top. If you are aware of what type of leader you are and how your leadership affects employees and clients, you can mitigate your weaknesses and discover your strengths to ultimately lead more effectively. Let's take a look at a few leadership personas I've witnessed while coaching and what works best for each.

In-The-Weeds Leaders

Leaders who are "in the weeds" tend to spend too much time in the day-to-day. They get bogged down with what's in front of them and don't think outside the box. Without innovation, the company runs the risk of coming to a grinding halt.

These leaders need to delegate current tasks to their team members. They can then focus on finding new ways to drive the business forward. In-the-weeds leaders may even need an outside party to hold them accountable for setting and reaching these new goals.

Frustrated Leaders

These leaders know their companies can be better, but they're upset because they can't scale at the rate they want. They bottle up their grievances and aren't sure where the disconnect is with their teams.

These leaders could seek guidance from a third party, whether that's a friend or colleague. An outside perspective can help identify problem areas. They also need to hear out their team members and get firsthand accounts on what's not working. Both perspectives can help turn frustration into focus.

Mindful Leaders

These leaders recognize that rapid growth is positive as long as they scale appropriately with formal organization and efficient processes. They are careful to avoid pushing forward blindly and losing essential parts of their culture and values along the way. However, they may take too long to think things through and miss new opportunities that come along because they couldn't act quickly enough.

These leaders should make sure they are sticking to the systems they have in place while remaining open to new opportunities and evaluating them in a timely manner. It's important to constantly reevaluate and adapt as the company grows and changes shape.

Control Freaks

These leaders can't seem to let go of the wheel. They micromanage and don't trust their team to get the job done, which fosters an atmosphere of frustration and mistrust. In this atmosphere, they can no longer lead effectively.

They should work with their teams to identify why the company exists, what motivates team members and why their work is important. That will not only help the leader and the team establish a better dynamic, but it will also help them

both understand where the company is now and where it's going.

When evaluating your leadership style, be honest with yourself. If you can pinpoint where you are on the leadership spectrum, then you'll better account for your challenges and capitalize on your assets. And that's how you become more self-aware and, in turn, a much stronger leader.

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.

Business Tidbit

Use These Steps To Protect Your Smartphone From Hackers

Update Your Phone And Apps

Just like you update your computer, you need to update your phone. Developers constantly update security patches. Like you, they want to stay ahead of the threats.

Lock Your Phone

Every smartphone comes with a bevy of security options to keep people out — except for you. Whether you use a passcode (the more complicated the password or PIN, the better) or biometrics (fingerprint or face recognition), you need to use something.

Avoid Public WiFi

Just as you wouldn't connect your laptop or tablet to unsecured public WiFi, you shouldn't connect your phone. If given the chance, hackers can and will try to access your phone and sensitive data. Consider using a VPN if you need to access public networks.

~ Digital Trends, Nov. 23, 2019

June 2020

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

ScreenKlean

"Welcome to the future of screen-cleaning."

Our lives are full of screens: phones, tablets, computers, TVs and even watches. These screens can be a pain to clean, especially if they are touchscreen. It seems like you look away for a second and they're covered in dust and fingerprints. It gets aggravating.

ScreenKlean solves this problem. This device removes fingerprints, smudges, dust and other particles in seconds. ScreenKlean uses electrically charged carbon molecules to clean just about any screen you have. It even works on mirrors!

ScreenKlean doesn't scratch or smudge, making it safe to use on your expensive devices. It's nontoxic and chemical-free, as it only uses special carbon pads, which last for hundreds of uses. You don't have to worry about dirty screens anymore! See GetScreenKlean.io for complete details!

Stay up-to-date

Follow BSSi2 at:

www.facebook.com/bssi2

twitter.com/BSSi2llc

The Pets of BSSi2

Last month you met Kurt's cat Bytes. This month here is his other kitty, Spas: a beautiful black house panther.