INSIGHTful DISCUSSIONS

Sponsors' Content Distributed By Greater Wilmington Business Journal

MANAGING CYBERSECURITY FOR YOUR BUSINESS

LARRY BLUMENFELD
President/Security Consultant, Cyber Security Integration

JESUS SHELBY
Cloud Solutions Architect, eGroup

CHRISSY COOR
Director of Service & Business Development, Fluid IT Services

SHAUN OLSEN
Founder, CloudWyze

Today, technology is not only a helpful tool for a business' day-to-day operations, it is crucial to that business' overall success. But with the benefits of technological advancements come the increased threat of data breaches and other cyberattacks. We asked four local experts to share their advice on how to effectively utilize technology in business while minimizing its risks.

How can a small business keep pace with ever-changing and more sophisticated hacking methods?

SHAUN OLSEN: Small businesses need to hire trusted technology specialists who stay abreast of the latest threats and the ways to thwart them.

There are about 74,000 pages in the tax code that change every year. Small businesses rely on their CPAs to exercise all available tax strategies to minimize their financial outlay, while keeping them compliant. Security should be viewed in the exact same way.

CHRISSY COOR: Be knowledgeable on the subject. Business owners don't need to read every article published about cybersecurity, but they do need to have a base understanding of the kinds of information that are targeted, and that even the smallest business is at risk.

The security options owners put in place may need to be tweaked throughout the year, and these owners need to budget for this. Having a trusted resource that provides proactive security is extremely helpful.

Discuss your concerns with your IT provider. They are seeing things on a higher level and should be included in security discussions, research and solutions for any business.

JESUS SHELBY: It's difficult not just for small businesses; it's difficult for enterprises and governments, as we've seen from breaches in the news. Nobody is able to stay completely secure, so the best you can do is stay aware.

If you have an IT department, it's best that they are staying up to date and watching for news articles, especially with their vendors.

And, then, just getting the basics right – not installing things that you shouldn't be installing on your work

INSIGHTful DISCUSSIONS

Sponsors' Content Distributed By Greater Wilmington Business Journal

> "Nobody is able to stay completely secure, so the best you can do is stay aware."

JESUS SHELBY
Cloud Solutions Architect,
eGroup

> "Budget for not only an attack on your business, but proactive maintenance to try and avoid it."

CHRISSY COOR
Director of Service & Business Development,
Fluid IT Services

PCs, not running things on servers that shouldn't be run there – so you can really reduce the threat factors you're exposed to.

I don't think you can do it alone. If you have an internal IT staff and it's small or if it's just one person, you're almost assuredly going to have to reach out at some point to an external vendor to get some help in some area, whether it's initial setup, auditing or providing extra hands at some point.

> "Cybercrimes cost CEOs their jobs, consumers their identities, governments their secrets and companies their customers.
>
> – Larry Blumenfeld

LARRY BLUMENFELD: It is important to pick a trusted advisor on the future-changing environment in physical security and IT emerging threats.

We, as industry professionals, attend technology conferences, trade shows and webinars - hosted by the top manufactures in our industries - that discuss comprehensive sessions on IoT, cybersecurity and unique challenges and opportunities we face. We also receive vulnerability alerts and white papers on best practices we can supply to our customers. There are local educational events, like the recent lunch and learn seminar, "Cyber Security Issues for Your Small Business," sponsored by Cape Fear Community College and Wilmington Chamber of Commerce.

There are many sites that can be researched on the internet, like the Department of Homeland Security (DHS) and research and education organization, SANS (Sys Admin, Audit, Network, Security). One of the most popular set of so-called "best practices" is "The CIS Critical Security Controls for Effective Cyber Defense," also known as "SANS Top 20." Many states recommend "best practices" as part of a good or reasonable security program and refer to the "SANS Top 20" as an example of "best practices."

Cybersecurity education is critical for all businesses, including manufacturers of consumer technology products. Cybercrimes cost CEOs their jobs, consumers their identities, governments their secrets and companies their customers. Cybersecurity is everybody's business.

What specific security issues does the Internet of Things (IoT) present, and how can businesses protect against them?

SHELBY: The Internet of Things is a very broad term; it's basically anything that has a sensor and a network connection. So, it's difficult to say how you protect against something so broad. Overall, the idea behind it is, just don't bring them into your business networks. Unfortunately, they are being flooded into the market now, and security is almost an afterthought. When these products come out with small sensors - like a smart lightbulb, for instance - they have very small capacity. It's not like a laptop. So, they have to really economize what they put into these devices, and right now security has kind of taken a back seat.

This creates all kinds of scenarios in which you can have issues. We've seen some broad breaches now where smart sensors and smart lightbulbs, for example, have been compromised and end up being used for Distributed Denial of Service of Attacks. We saw that when the Dyn Network was targeted, and there have recently been some others. And nobody really saw those coming.

So, you just have to keep those off your business network. Segregate those things and make it easy, so if there is an issue with them, you can just flip one switch and turn everything off.

BLUMENFELD: IP camera security and access control are a big part of the buzz about the Internet of Things. There should be more concern about how the industry has possibly left the customer vulnerable.

Today, more and more physical security systems are connected to communication networks for security monitoring, safety and control. These connections leave systems vulnerable to cyberattack. Increasing numbers of attacks on physical security systems and companies' networks deployed in critical infrastructure facilities and corporations must be addressed with a solution that can defend against a broad range of both physical and cyber threats.

Surveillance cameras, access control systems, sensors and controllers are connected using ethernet, IP and other technologies, and rely on unsecured communication networks deployed across the site, as well as in the field. The use of these unsecured networks exposes the site to combined cyber and physical threats.

With the studies and concern brought about by the IoT, these problems were brought to light. Hardening of devices was not stressed and in most cases, camera settings were left open to hacking by improper setup.

> "Security is the responsibility of all employees. If something looks wrong or seems out of place, it probably is.
>
> – Shaun Olsen

The common factor in most of data breach class-action lawsuits, as well as investigations by regulatory agencies, is the allegation that the breached company failed to implement "reasonable security or protections" to prevent the breach.

Logically, then, if you implement "reasonable security and protections," you should be able to confidently defend your security practices and actions.

OLSEN: The two biggest security issues with IoT are that you cannot install anti-virus on them and their OS [Operating System] is not updated to plug

INSIGHTful DISCUSSIONS
Sponsors' Content Distributed By Greater Wilmington Business Journal

security flaws, so they become what is known as a potential honey-pot.

Firewalls, which offer Stateful Packet Inspection (SPI), such as those made by our partners at Sophos, are able to shut down network traffic by device when it sees they are possibly compromised and self-mitigate the threat.

What potential security threats do Artificial Intelligence (AI) and other growing tech trends, such as smart homes, create?

OLSEN: People forget that while AI can be used nefariously, it can also be used to learn to adapt and block intrusion attempts. With smart homes, it brings a virtual threat to a real-life security concern.

SHELBY: We've got all these devices and sensors and this data, and AI is a great benefit for going over that data.

But there is a downside there that we're seeing, too, in that the algorithms that push these things can actually be biased. Us as people are biased. People program these algorithms and they program their own biases into these algorithms. We have seen that recently with Facebook and Twitter, where they're filtering news stories; they're determining who is going to see what.

Another example is how AI is used in the judicial system. When you go to court now, your profile is going through some closed-source system that is giving you a score that a judge will use to help determine sentencing or fines. These are things we have no visibility into, but they are controlling aspects of our lives. So, there is a huge threat there that we could lose control as a society, and within businesses, too.

What is the most common mistake you see businesses making in terms of cybersecurity?

COOR: Not being prepared. Knowing what to do - and when - is critical. Each business, no matter the size, needs to have a plan in place.

Many businesses feel they are not at risk because of their size. This couldn't be further from the truth. It's these businesses that are highest targets because they have access to the larger entities.

Each business needs to have a documented approach to any type of data breach or cybersecurity attack.

> "Locking your door after a burglary serves no purpose. If one is not proactive by updating and monitoring firewalls, anti-virus and security policies, then it isn't a matter of if but when."
>
> **SHAUN OLSEN**
> Founder,
> CloudWyze

Employees should be familiar with the company's security policy and response plan and be offered ongoing training, whether from an in-house contact or a third party.

BLUMENFELD: Ninety-one percent of all targeted attacks begin with phishing email, so education of your employees on how to spot suspicious emails with attachments that should not be opened is the key. Spear phishing leads to ransomware attacks, which, according to the FBI was a $1-billion-dollar problem in 2016.

Use of poor passwords are also a major problem. Most IP-based devices are shipped with default passwords and default settings. This is the most common way a cybercriminal can gain unauthorized access to your system. Change passwords from the default, have strong unique passwords or use passphrases, and change your passwords on a regular basis.

Most companies do not have a documented plan for installing and maintaining all your network-attached devices. It is important to deploy and install devices using best practices supplied by the vendor. Companies need to be more careful of product manufacturers and installers of devices on your company network.

Remember the Target breach? The release of the malware, known as Mirai, gave cybercriminals with minimal skills a new tool to launch cyberattacks. Camera hacks like the Mirai exposed the threat of unsecured devices being used in an attack that involved the whole group of major websites, including Twitter, Spotify, Amazon, Reddit, Yelp, Netflix and The New York Times.

OLSEN: Lack of patching and applying security updates. Some companies will invest in a quality firewall but then never update the firmware, or they allow protection subscriptions to lapse. Therefore, cybersecurity requires ongoing management and monitoring by a certified and trusted technology partner.

SHELBY: I think there are two big ones early on. One is a lack of resources - either they don't have the people, or they don't have the money. In some cases, it may just be the allocation of resources – the resources are there, but they don't determine that security is a high-enough priority for them to implement it. They look at the risks and think, I'm just too small; I'm not a factor.

Actually, the opposite is true. Now, with all the controls and defenses, it's a lot harder to go after the Fortune 500 companies. Granted, those are like the gold chests. But most of the hackers are going to go after the little guys, where there is less security. They just want to be able to click a button and get in. They don't want to have to do surveillance on you for months and use social engineering and phishing to target you.

So, small- and medium-sized businesses are probably at greater risk than larger organizations. Not realizing that and not dedicating resources to security increases their vulnerability. If you don't have cybersecurity insurance, which is still fairly new, and other assets to protect you, you could literally go out of business overnight.

The other mistake is the failure for businesses to adapt their thinking about resources. A lot of businesses still think all they need is anti-virus software and a firewall in front of their server. But today, the problem is much more complex than that. Failing to realize that there is no real boundary anymore has also held back businesses from putting in the proper controls.

How can business owners ensure staff is safely accessing data, networks and servers, onsite and while working remotely?

SHELBY: It's a combination of policy and technical services. You have to educate your staff members on how to do their work properly and safely and what tools to use.

You also need to know what you're actually protecting to give them the proper tools to do so. It may not be critical for me to worry about your laptop and how you're accessing a Word document with information on it because if that gets out in the public, I may not care. So, in that

> "Many businesses feel they are not at risk because of their size. This couldn't be further from the truth. It's these businesses that are highest targets because they have access to the larger entities."
>
> – Chrissy Coor

> One of the things I see people do that is counterintuitive is disabling security controls.
>
> – Jesus Shelby

case, controls don't have to be that strict.

But if I have really sensitive information or if I travel a lot, for instance, and go back across the borders and worry about laptops being seized, I may need to implement a remote-desktop solution that keeps data completely off my machine, so if I lose the machine, I don't lose the data.

OLSEN: It all starts with education. Security is the responsibility of all employees. If something looks wrong or seems out of place, it probably is.

Question everything. Ask your IT department before you click on that link, and let them know if you did click something you shouldn't have before it gets worse.

COOR: Access to all data, whether onsite, remote or to a third party (e.g. Dropbox) should be encrypted. Strict guidelines for employees on who and what can and cannot be accessed should be clearly defined. Not every employee needs access to every company system or data.

Define and enforce a policy of strong passwords and two-step authentication to mitigate risk. Ensure all devices have adequate anti-virus and remote monitoring software to mitigate incidents. Define a policy of company-owned devices versus employee-owned devices. Employee-owned devices - especially those used remotely, like a home computer - are not easily managed and thus more prone to security incidents.

What initial steps should businesses take in the event of a data breach?

COOR: Management should immediately initiate your Incident Response Plan, which should document all the steps to take internally, as well as with your customers, vendors and other third parties. Confirm the scope - what data was breached, the volume and contents (billing, account info, social security numbers, data, etc.). Communicate with employees, then impacted parties (customers, vendors, etc.), notifying them of what occurred, the plan to remediate, and any action item they should take, such as resetting passwords and confirming data integrity.

OLSEN: First, change all passwords, and unplug the connection to the internet and any wireless access points until you determine what was stolen and how.

Next, find a solution to your problem to prevent future issues and, depending on what federal laws apply, such as HIPAA and SOX, you may have to disclose this information.

BLUMENFELD: I will share advice from my colleague, David Willson, JD, CISSP cybersecurity attorney on this subject:

> IP camera security and access control are a big part of the buzz about the Internet of Things. There should be more concern about how the industry has possibly left the customer vulnerable.

LARRY BLUMENFELD
President/Security Consultant,
Cyber Security Integration

Assuming you can't prevent the breach, prepare a message in anticipation of a breach. Owners, CEOs, executives, managers and others - what would you do and say if you found out tomorrow your organization was breached?

Remember, most companies find out they have been breached from an individual or entity outside of the company. Normally, you will have very little time to react and put out a statement once a breach is identified.

Once a breach occurs or a potential breach is identified, if you or anyone from the company is asked to or makes a statement, don't admit to anything. It is likely, once you are notified of the breach or potential breach, that you have no idea what may have occurred, how much data was lost or stolen, if any, or impacted, etc. These situations are usually fluid, so generally any prepared message will likely have to be modified depending on the facts. But it is much better to be prepared and have a sense of what you will say versus trying to develop a statement as you are being pressured. If you are not sure what to do, find an expert who can help.

SHELBY: Hopefully you have a response plan already and you can open that up and follow it.

But I know the reality is that many businesses probably don't have a plan in place, so, once you have discovered a breach, you really want to minimize that exposure. You don't want data to continue to leak out. But you also want to do that in a way that is not going to compromise the ability to find out what is going on. So, in most cases, you should reach out to a firm that specializes in this, so they can walk you through the steps to submit information for investigation.

Once the technical part is underway, you really need to look at who may be affected, such as your consumers and business partners. You have to devise a way to communicate that out. You probably should refer to a legal team initially, but you definitely want to get that out and let them know as soon as possible. You don't want to wait and have something happen because you waited.

In what ways – or in what industries – could the European Union's General Data Protection Regulation (GDPR) impact U.S. businesses?

SHELBY: To be quite honest, the whole reason we have GDPR has more to do with the U.S. than with the European Union. It's about how we handle data, and we've had different agreements with them as far as how data about European citizens is handled and transferred. They didn't feel we were honoring the agreements in place. And then, of course, the whole NSA and spying issue on top of that, it all tipped over and the EU decided to develop stronger regulations.

So, if you do any business at all in the EU, you're affected by GDPR. If you don't comply, there are some substantial fines, and if you can't pay those fines, you may be blocked from access to the largest market in the world.

That's difficult to do, though, because the EU and the U.S. have very opposite stances on data. GDPR says that European citizens own their data. If you have information on them, it's theirs, not yours. You are a steward of that information and are expected to comply with that in a respectful and reliable manner. In the U.S., whoever has the data owns it.

In the EU, they're trying to limit what they need. If I only need your email address and do business with you, I should only have your email address and when we're done doing business, I should get rid of it. But in the U.S., I may only need your email address, but I'm going to get as much information as you're willing to give me. Then I'm going to store it and keep it forever. Of course, the longer I have the data, the more increased the chance is that someone will get it.

So, it's a big shift in how you have to think about it, and we don't have a lot of tools available. But I do think eventually, it's going to affect even people who aren't doing business in the EU, because the tools we use are going to be affected.

That will trickle down to us because we'll all be using those tools from the big vendors and hopefully that will benefit us all.

OLSEN: GDPR is a great step towards

protecting consumers. Many believe that its impact and ability to enforce on U.S. businesses is not yet known.

How can businesses be proactive about security?

BLUMENFELD: Like physical security, effective cybersecurity is an ongoing cycle of identifying vulnerabilities, assessing threats and implementing appropriate measures. The need to strongly secure your network becomes more evident every day.

To ensure a strong defense, consider the hardening of not only the network but also all the devices attached to it.

Physical installation (of an IP surveillance camera or any other network device) and maintenance problems can also be cause for concern when it comes to cybersecurity. Installers sometimes do not understand the specific needs that you require at the time of installation. With so many vendors, it's possible the installer missed any or all their security best practices. Most IP-based devices are shipped with default passwords and default settings. Sometimes, these passwords are easy to guess and even published online. This is the most common way a cybercriminal can gain unauthorized access to your system. This should be the first thing you change. After all, passwords are the gateway to the entire network.

Many vendors publicly post common vulnerabilities and exposure reports that document solutions or workarounds to a specific vulnerability. Immediately react and follow security vulnerability alerts instructions from vendors.

COOR: Education. All high-level executives and business owners need to educate themselves on the potential threats.

Owners should keep all their systems up to date, and ensure manufacture warranties and support are still intact. Run security scans to find any gaps with current hardware/software in place. Fill these gaps. Determine how long your business can run via "paper" and budget for appropriate back-up resources.

Budget for not only an attack on your business, but proactive maintenance to try and avoid it. Understand there is no 100-percent foolproof way to avoid an attack, but that proactive awareness can save a lot of time and money. Ultimately, the security of your business is a budget decision. How long can you afford to be down and/or not working?

Business owners should understand that employees are the number-one cybersecurity "attackers" - whether malicious or not. Ensure all employees are aware and understand implications of their actions dealing with cyberattacks and/or breaches.

Have the appropriate security hardware, software, solutions and processes in place based on your business requirements, regulatory, compliance and risk tolerance.

SHELBY: It can start easy and get very difficult. One of the things I see people do that is counterintuitive is disabling security controls. When you get a new computer, don't start turning things off because they are annoying; learn to work with those controls.

Make sure you secure outbound connections with the internet; make sure you understand what's going in and out. Don't listen to those articles that say you don't need anti-virus.

Make sure everything stays up to date. That's across everything, not just your Windows applications.

Those are just the basics but if you do those, you're well ahead of the curve.

OLSEN: Locking your door after a burglary serves no purpose. If one is not proactive by updating and monitoring firewalls, anti-virus and security policies, then it isn't a matter of if but when.

Additionally, services such as DNS [Domain Name System] protection and web filtering can be a great proactive mechanism if deployed and managed properly.

What advice do you have for companies processing credit card payments and/or managing an online retail component?

COOR: Make sure you are compliant. There are industry standards in place for reasons. Using cloud applications offers encrypted data. Do not store customers' data. Educate employees on appropriate use of the systems. Run at least annual PCI [Payment Card Industry] scans, where necessary, to identify any failures and remediate risks.

SHELBY: Ensure that you stay compliant. From a risk standpoint, you're at a great risk if you're not compliant with PCI or don't stay in compliance. If you go through the first round of compliance but don't keep up with yearly audits, and a breach happens, Visa and MasterCard can charge you not only for the fraud that occurs but also any cost that they incur from sending a team in. So, it would be very easy, especially if you're small, to end up out of business by not being compliant.

OLSEN: PCI compliance is serious, but one shouldn't let that fear prevent them from online commerce. Small businesses should partner with a merchant company and a reputable shopping cart service that accept the responsibility of security. These are specialists that focus on proper and compliant ways of accepting electronic payments.

What questions should a business owner ask when shopping for an offsite cybersecurity service?

BLUMENFELD: Companies should look for help to provide the solutions, education, resources and reasons why they should invest in their cybersecurity maturing process.

The goal will be to assist companies to reach the minimal level of being reasonably secure and state, federal and international laws require businesses to protect the personally identifiable information of employees, vendors and customers.

It's reported that increasing employee knowledge on cybersecurity practices can cause a 30 percent decrease to security risks.

Some questions to ask include:

- How can you help build and maintain a culture for cybersecurity?
- How can we better invest in employee health training?
- What plan could we put on place to educate new employees on the processes as they onboard?
- What programs can we put in place to encourage senior leaders to enforce the importance of cybersecurity, continuously learning about the evolving cyber threats as they emerge and communicating known threats to appropriate members of the organization?
- How will you help in examining cybersecurity as a requirement when choosing new network equipment?
- Can you write policy for implementing a BYOD (bring your own device) policy?
- Can you assist in creating and applying a cybersecurity incident response strategy for when a breach occurs?

SHELBY: Before you ever call anyone, do your homework on the vendors. Go to their website, look at the case studies they're presenting, read the reviews. Nowadays, with Google and Bing you can find out things pretty quickly. I would even consider looking at the case studies they published and calling the companies to follow up.

If we're talking specifically in terms of compliance or breach assistance, make sure that's what they do. You don't want somebody who kind of does it sometimes. When it's that important, you want that to be their business, so I would look for somebody very specific. It may cost a little more, but you can generally be sure it's going to be done right since it's all that they do.

COOR: The business owner should first do some basic research on the "layers" of security they believe they need. Security has many layers, from the end-point anti-virus and office firewall to wireless access points and application and cloud-based security and encryption. Ideally, the cybersecurity service will cover as many layers as possible to centralize security and simplify management and ongoing reporting and remediation.

Any business should also understand the role their employees play in security, and that no matter how much security is put in place, there is always the possibility and likelihood of an incident or breach. They should understand what they are responsible for and what the vendor is responsible for, and have a company security policy and response plan.

OLSEN: Whenever I need a professional service such as an attorney or a CPA, I always ask individuals I trust who they use and why. Referrals are a safer bet than trying to Google for one. An established company with a solid reputation speaks volumes.