Waging War: What St. Louis Experts Say About Cybercrime

Safeguarding St. Louis Against Cyber Threats

Managed IT | Co-Managed IT | Cybersecurity

ANDERSON TECHNOLOGIES

An Ebook by Anderson Technologies, a St. Louis IT Company
info@andersontech.com | andersontech.com | 314.394.3001 | © 2021 Anderson Technologies

ANDERSON TECHNOLOGIES

Securing St. Louis

Cybersecurity attacks devastate businesses and organizations all over the globe. **St. Louis is no exception**. And yet, investing beyond basic protections might feel too expensive when current needs are more pressing. . . until you become the target.

It's hard to imagine just how important business cybersecurity is until the worst happens to you. Business cybersecurity is essential because **cybercrime is happening** in our St. Louis community—but thankfully, **so are the solutions**.

According to **Forbes**,

57%

of small business owners feel they won't be targeted for cyberattacks.

Of all data breaches,

43%

were small businesses, the #1 target of cybercriminals. (**2019 Verizon Data Breach Investigations Report**)

Small businesses aren't immune from attack. In fact, smaller prey are often easier to catch, making small businesses a prime target for cybercriminals.

Meet the Experts

When St. Louis' small businesses have questions about cybersecurity, they can look to experts across major industries. Four knowledgeable local figures weigh in on the elephant in every server room.

"Cybersecurity and protecting your assets and your data is no longer optional."

—Erica Wilson, Vice President, Global Security & Privacy Risk Management, Reinsurance Group of America

"People don't know what they don't know. A business doesn't want you to know that they were breached or they may be compromised."

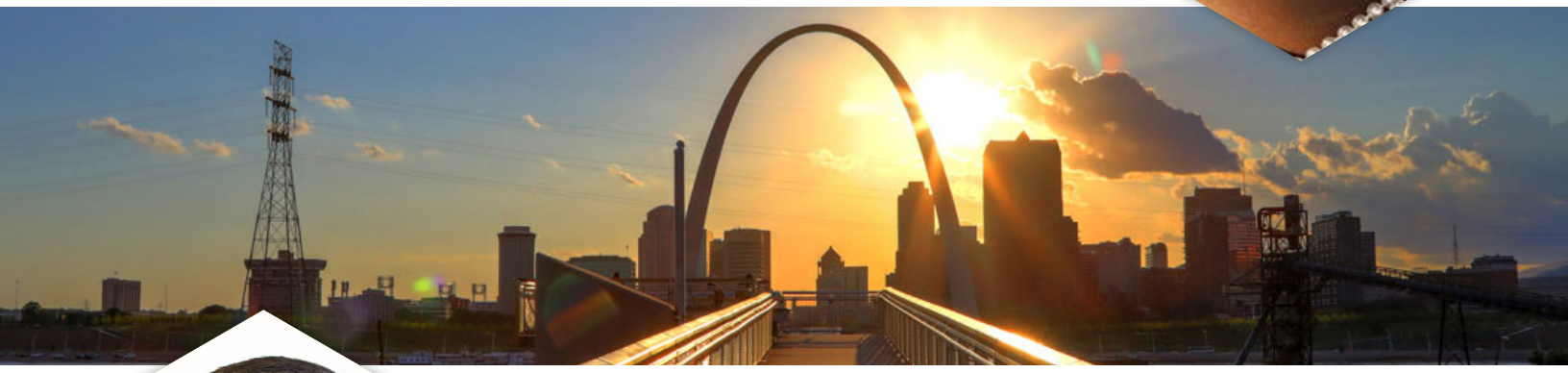
—Derek Pounds, Multicloud Consultant, World Wide Technology, Information Technology

World Wide Technology

Meet the Experts

"It's not a matter of if you get penetrated, it's when. Because [the threat] can be anywhere, it can happen to any of us. None of us are outside of the scope of a threat actor."

—Paris Forest, Senior Director of Information Technology, Boeing, Aerospace



"You need to be prepared for your username and password to be for sale on the dark web. Over time, it's pretty likely."

—Bob Rein, Director of Information Security, Computer Software Firm

Who Are the Targets?

Who needs to think about cyber-security? What type of businesses are being targeted by criminals?

Major headlines have highlighted recent attacks to healthcare, government, an oil pipeline, transportation, and a meat processor. But we don't see the millions of attacks that aren't big enough to make the news.

Smaller businesses and institutions are prime targets not only for their data, but for their ability to connect to larger, more lucrative targets that the business serves. Business email compromise is a way for cybercriminals to infiltrate organizations that they otherwise wouldn't be able to reach. **Bad actors don't even need to directly access an organization's systems to make a profit from them.** With access to a supply chain vendor's email or network, the cybercriminal can mimic legitimate invoices to the client company and tell them to send payment to a new bank account, leaving both businesses at a loss.

"What we saw at the onset of the pandemic, and we continue to see, is the bad actors being more focused on some industries, like government agencies. Even universities and hospitals were a huge target. But even more, I think **what it showed us is that no one is off limits**. Now, because the end users, the employees, everyone who has the ability to connect in are really the target. Anyone can be the target."

—Erica Wilson

"All organizations should be fighting against becoming the next topic in the news. I mean, **we see it over and over** and over and over and over and over again. And it is just a matter of time before the focus gets off of the very large, very public entities and into the very small entities where there [is] easy access, especially those who may be on a business growth trajectory."

—Paris Forest

"Cloud changes the dynamic for a small company to act as a big company, because it gives them the same abilities, from a tech perspective, to run their business the same way. Often, they're not investing in IT, instead they're focused on their business not trying to build and secure everything in the datacenter."

—Derek Pounds

What Is the "The Perimeter"?

You know the steps (if any) you've taken to secure your company's digital walls—firewalls, passwords, and web filtering. . . . But even if those digital walls are protected, the breadth of your business stretches beyond just *your business*.

Go In-Depth with Erica Wilson

"There's a term in security that we call **the perimeter**, which is basically the outer layer of your corporate network. That really doesn't exist anymore. With people working from anywhere, whether it's home, different remote locations, when they connect in and they're using foreign networks, it essentially becomes an extension of your network now.

The moment there's a new type of device that can connect to the network, connect to the internet, the cloud, what have you, that's another vector. You've got to figure out how to protect it, what can be done. There's the issue in that a lot of these manufacturers aren't truly security or technology companies, so they're just coming up with the next cool thing. Not that security isn't in mind for them at all, but it's definitely not at the core of what they do.

Think about [the Internet of Things] and all the different devices that are out there; items like refrigerators and vacuum cleaners and thermostats, all of those devices become an attack vector. That's pretty scary, because we used to have what I would say is a little bit more control. You've got to really have visibility into devices and identities and normal traffic patterns. You have to know all of that so you can see if there's anomalies and be able to respond quickly if you need to."

The global pandemic of 2020 was characterized by an entire segment of the nation's workforce moving to working from home. This sudden shift opened many business owners' eyes to the concept that their perimeter, or the digital walls of their business, stretched further than they could imagine or could control. The interconnected methods of business and technology in the modern day allowed for this, but it also revealed a lot of the vulnerabilities that this inherent interconnectedness allows for.

What Is the "The Perimeter"?

According to Aim Point Group's 2021 State of IT Operations: The Rise of the Remote Workforce, "half of all survey participants expect that over 60% of their organizations' employees will be working remotely in 2021/2022. . . . Close to 80% of those surveyed agree that the process of managing endpoints has become harder as a result of the shift to more employees operating remotely."

Go In-Depth with Paris Forest

"[With 130,000 employees,] there are 130,000 opportunities for the Boeing Company to be attacked in some way, shape, or form . . . .

We're responsible to make sure that our customers and our teammates are aware of how they play into the overall.

It's not just us who has to be concerned, . . . because we become a network. And I think that's the broader implication. If they want to do business with some of these bigger companies, . . . it's critical. But it's because they don't realize that that they are prime [targets]. They think that the prime are the people like the Boeings and other larger firms, so they don't think that anybody is looking at little old them, but little old them is very high on the list, especially if [criminals] have access and someone can get in through them to one of the other bigger targets. That has absolutely happened countless times where the infiltration is through a partner or supplier.

We cannot believe that because we've secured our perimeter that the full perimeter is secure, until the perimeter extends as far out as whoever we do business with. That's why it's extremely important, especially for boutique-type vendors who may do something very niche that could be very valuable to these large corporate entities.

You have to make sure you are protected because you become a part of that perimeter, which means that you can come under the scrutiny of the organizations with which you do business."

What Can You Do to Protect Your Business?

The Basics of Protection

If you care about your business's cybersecurity, you'll need to prepare more than the bare minimum protections.

"Make sure that employees have what they need. Basic things like antivirus, everybody's running the standard up-to-date antivirus/anti-malware protection, because that's kind of the first base level step to preventing some things from coming in."

"When I think about small businesses and even nonprofit organizations, certainly it's to be expected and understood that they have limited funding, right? So using their funding wisely when it comes to technology and security is very important."

—Erica Wilson

"Update your computers and phones. Set them to automatically update the operating system, and when it prompts you to update it, go ahead and update it. **You have time.** That's the greatest enemy of the scammers is you saying, 'You know what, I'm just gonna take a step back here for a minute.'"

—Bob Rein

If you have nothing else, consider:

- Two-Factor Authentication, also known as Multi-Factor Authentication
- Reliable and secure password manager
- Enterprise-grade antivirus/anti-malware on all devices
- A regular update schedule for all hardware and software

What Can You Do to Protect Your Business?

Email: The Simplest Attack Gateway

Email is possibly the most frequently used vector of cyberattack for the modern business, and for good reason. Each of your employees' inboxes is a fresh opportunity for that end user to click a link or open a dangerous attachment, meaning the protections around that inbox needs to be your business's first line of defense.

The Human Factor

On average, every employee has access to 11 million files. Access to a single employee's account could mean access to your entire business.—Varonis

"They will research your company . . .

they will know about projects that are going on, and they'll send very believable emails sometimes. **You've got to have that agreement up front—any kind of financial transaction has to be approved outside of email like through a website or via a phone call."**

—Bob Rein

"It's just a really good practice . . .

to always remind individuals, if you're not sure of the source or if it looks suspicious, hover over the hyperlink, **pay attention**, and make sure it's really going to a site that you would expect before you click, because a lot of times you could prevent so much from people just avoiding those malicious links."

—Erica Wilson

ANDERSON TECHNOLOGIES

What Can You Do to Protect Your Business?

Email: The Simplest Attack Gateway

"If a company that you do business with emails you and you're confident it's actually that company, you still don't interact with them through that email, because the fakes are so good these days . . . and they can absolutely guess information about you and figure out information about you with a little bit of effort. They can know that it's your bank, and they can say, 'Hey, based on your recent activity . . . ' They can make it sound very, very believable. Just have a general practice: if you emailed me that, I'm not going to interact with it through that email."

—Bob Rein

Phishing by the Numbers

- **10.7%** of users in a phishing simulation fell for the phish. That means in a real attack almost 11 users of 100 will likely click. —2021 Annual State of Phishing Report, Confense
- **74%** of US organizations experienced a successful phishing attack in 2020. —2021 State of the Phish, Proofpoint
- Compared to 2019, successful phishing attacks were **13%** more likely to lead to data loss, and 11% more likely to lead to credential compromise. —2021 State of the Phish, Proofpoint
- **48%** of malicious email attachments are Microsoft Office files. —"Few Phish in a Sea: Protected with Email Threat Isolation," Sunil Choudrie, Symantec
- Smaller organizations (1–250 employees) have the highest targeted malicious email rate at **1 in 323**. —Symantec, ISTR Volume 24, February 2019

Want to protect your business? Engage in ongoing phishing training and utilize tools that decrease the number of phishing emails that reach an inbox in the first place.

What Can You Do to Protect Your Business?

Multi-Factor Authentication (MFA/2FA)

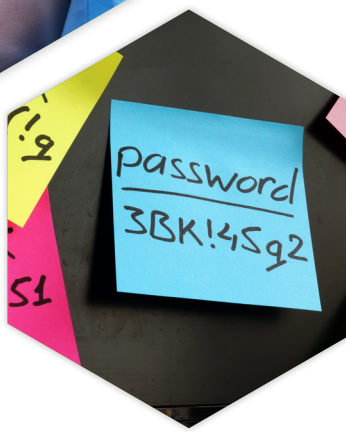
Go In-Depth with Bob Rein

"Require two-factor authentication on anything you care about. Going to that level where you're required to use it is by far **the number one thing you need to do.**

It's so much harder for a bad guy to hack an account if it's two-factor than if it's single-factor. There are **three different types of factors** that one can present in order to prove that he is who he says he is, to be authenticated. The first one is **something you know**, like a password or PIN. Second is **something you have**. That could be your phone, could be a key, could be a little key fob. The third thing is something biological about your body [or **something you are**]. That could be your thumbprint, could be to your facial scan, it could be a retina scan.

In order to have two-factor authentication, you need to have at least one from two of the groups. If you have a username and a password, that's group one, something you know. If you add in another password, that's still just something you know, so it's still single-factor authentication. And then when you add in something you have, like your phone, now you've got two-factor authentication.

The simplest thing is going to be to have [employees] do something on their phone, either receive a text or they'll have an authenticator app on their phone and type in a code. They also have authenticators where you can just tap something on your phone, or thumbprint on your phone.



It's not that bad a user experience. I don't think it's very costly, and it is the number one thing you should do. This idea of breaking into people's accounts is happening. It's rampant—happens all the time. **Two-factor authentication is a pretty clean way to dramatically lower that risk. Require two factor authentication. It is not optional."**

Preparing for Risk

Ransomware

Ransomware is one of the biggest cybersecurity concerns for businesses near and far. It seems like every day brings news of yet another organization falling victim to these kinds of attacks, leading to financial and reputational ruin. When you read stories like that of the Colonial Pipeline, it's easy to ask, "What did they do wrong to let this happen?"

"Ransomware is probably the top concern for so many organizations. Once the compromise occurs, critical data is encrypted, it can't be accessed, and if you don't have back-ups, you're really at a loss. And the ransom amounts are upwards of hundreds of thousands [and] could take some organizations totally under. That's a pretty scary place. In years past, . . . somebody gets infected, their machine, you pull them off the network, you clean it up, you just reinstall everything, and you're good to go. We're way beyond that. It's so much more sophisticated."

—Erica Wilson

Paying the ransom doesn't solve the problem

- 68% of US organizations said they paid a ransom in 2020. —2021 State of the Phish, Proofpoint
- In 2020, organizations who paid ransoms were 9% **less likely** to receive their data after the agreed-upon first payment. Requests for additional ransoms increased more than 320% in 2020. 32% made additional payments and eventually received their data. —2021 State of the Phish, Proofpoint

Should You Move to the Cloud?

Risks and Rewards

More businesses than ever are moving to cloud-based platforms, and for good reason. Cloud applications allow for greater accessibility, collaboration, and innovation. But they also create new vulnerabilities that businesses have to be aware of.

"Are you able to wait two or three days in a 24/7 business environment for your data to get restored?"

—Derek Pounds

Cloud backups are great alternatives . . .

or additions to other methods, but like any backups they should be regularly monitored and tested. If your business has been holding back from moving to the cloud, know that it may not be a large investment upfront but only when you need to move all the data.

19% of malicious breaches were caused by cloud misconfiguration . . .

so be sure you are partnering with an expert when you venture into the cloud. Assure your cloud systems are well-monitored and configured by an IT expert. —Data Breach Report, IBM

"They still need to understand what the business needs to take changes rapidly, and allow for the business to change and grow using the new technology. . . . I look at cloud solutions, some combination of offering public cloud solutions and software, to help you manage your business to put more time and understanding your customer. There's all kinds of things that they put in place from a secure management perspective that you can manage on prem, as well as in the cloud."

—Derek Pounds

ANDERSON TECHNOLOGIES

Don't Skip Your Risk Assessment

Go In-Depth with Bob Rein

"I think security professionals have to be a little bit careful because there are things that people need to do in order to secure themselves, but they're not all equally important. We run the risk of saying, 'You got to do this' and crying the sky is falling. 'If you don't encrypt communications over the network, then people can steal it' and all this stuff.

But we need to be grounded in reality and in risk management. **Is that a high risk? Is that a medium risk? Is that a low risk? How likely is that?** There are some things that are fairly low risk, and they take a lot of effort to try and protect against. That's probably not a good first step. I'm thinking particularly in my industry, the security industry, we have to be careful that we're not trying to get people to do things that are like priority 18 when we haven't gotten them to do priority one and two first."

A Weapon in the Cyber War You Cannot Ignore

Employee Training

In the end, cybersecurity still comes down to the human factor. All the defenses in the world can't stop an attacker who is invited in by an unwitting employee. That's why comprehensive and ongoing employee training is essential to the success of your cybersecurity plan.

Never assume your employees know what to look out for. Malicious emails are no longer easily identified by broken English or outrageous requests. They look like credible companies you work with daily. They could be a trusted contact whose email was compromised first. What looks like a message from one of your vendors trying to update their account information could actually be an imposter tricking you for credentials—all without the original vendor even knowing they've been compromised

"The number one sign of a scam is that they put tight time constraints on you. The number one thing to know in a scam is take your time, step back, maybe call somebody else that you trust. This is one common thing, though, the idea that they don't want you to take your time. They don't want you to step back, they don't want you to seek a second opinion. They want you to act as quickly as possible."

— Bob Rein

"You have to be able to stay on what's going on. The industry is changing so quickly. 5G is going to change things dramatically. It opens up the door for businesses to change their model, but if you're so focused on technology, you're going to miss that."

— Derek Pounds

Employee Training

Go In-Depth with Erica Wilson

"Keep yourself and your employees on the watch for new trends in phishing emails and put in place policies that safeguard against BEC scams. **It's always better to prepare defenses beforehand**, so that if unusual requests occur, everyone knows what to do to verify it is a legitimate request.

I would suggest that people as much as possible do as much education as they can, even if it's just a matter of saying, 'Hey, here's something that happened in the news,' sharing a real-life scenario, and helping people to understand. Then the next level is providing training, which should be required. These are the basic practices that should be in place prior to additional investments in technology.

We do regular communications about things that are happening in the news, trends we're seeing, if we've got an entity or vendor or a customer that's been impacted by something, making sure that our employees are aware. We do our own phishing exercises, so **test our employees just to make sure they're paying attention**. It gives us a level we can kind of gauge to see how on-edge or close people are paying attention.

If we start seeing those click rates go up, it's an indicator. 'Okay, people aren't getting it anymore. We've got to do something else.' We do training on our policies, the dos and don'ts for handling data, sending data, using personal email for work-related things, we try to provide some type of training around what's acceptable and what's not acceptable. And then lastly, one of the things that's gone a long way is to acknowledge when someone's doing something right."

"... there are scams out there and you can be a target of those scams even though you're a small business. You need to teach your people, especially people who have the ability to transfer money, we have a process. Don't ever transfer money based on an email."

— Bob Rein

ANDERSON TECHNOLOGIES

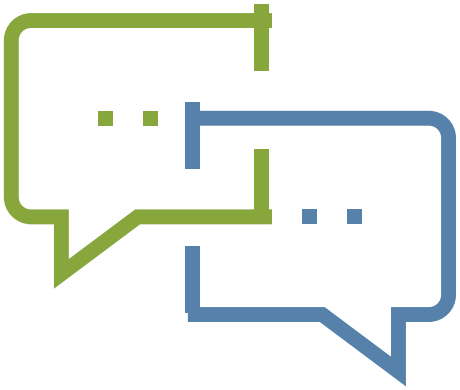
About Anderson Technologies

We hope you found this ebook useful. Educating yourself and your team is an integral and often overlooked component of cybersecurity.

Don't miss out on the peace of mind that comes with employees trained in cybersecurity and phishing. Contact Anderson Technologies' team of experts to schedule a **free cybersecurity training session** for your employees, and know that your business is one step closer to preventing a cyberattack.

Click to Schedule a Free Consultation

Click to View All Our Free Resources



Have Any Questions?

The team at Anderson Technologies is happy to discuss any questions you have or schedule a time to help educate your employees about best practices. Give us a call today at **314.394.3001.**

Managed IT | Co-Managed IT | Cybersecurity