Rotary Club of Charlotte

THIS WEEK'S PROGRAM

September 9, 2025

Cyber Crime & Tech Trends: Joel Sosebee

Director of Client Success, AT-NET Services

by **Susie Masotti**

The Charlotte Rotary Club was pleased to have Joel Sosebee, Director of Sales for AT-NET Services, serve as our speaker this week.

Dena Diorio, Retired Mecklenburg County Manager, introduced Joel. She shared that Joe has 25 years of experience building managed technology solutions with a focus on Cyber Security. His programs provide proactive models with more efficiency. His speaking partner, Michael Sylvester, Chief Strategy Officer at AT-NET Services, focuses on growth, innovation, and success while staying within industry compliance standards.

Joel began by asking how confident you are that you are protected from a cyber attack scam. He advised that there are more opportunities every day for bad actors to try to work their way into your business or your personal information. In Charlotte, AT-NET Managed IT Services focuses primarily on efficiency and protecting companies from cybercrime.

Cybercrime is expected to increase to $10 billion by the end of the decade, growing at a very fast pace. When technology first started, you may have imagined an individual trying to hack into your system. Today, there are highly effective businesses whose only job is to look for targets that are vulnerable. A business is cyber-attacked every 39 seconds in the US. Joel warned not to be

fooled – these are organizations that are well funded and very good at what they do.

There are 3 types of attacks:

- Business e-mail compromise – they are making their Trojan horse more believable.
- Invoice fraud – they look for ways to submit invoices to you and your suppliers by hacking into your business and finding who you do business with, hoping that when you (or they) receive an invoice, you don't know the difference.
- Ransom and Data Extortion – they enter and take over your system, then demand a ransom for the return of your system. Even Google was attacked by an internal mole.

Almost all cybercrimes begin with malware that you likely don't know is on your device.

What solutions do you use as a business owner or individual to protect yourself? It starts with the basics. Statistically, people and companies use the same password for more than half their accounts. You may have noticed many companies are now using multi-factor authorization for everything (even e-mail). While this is an additional (and annoying) extra step, it is a vital step. Manage your system-wide vulnerabilities – accept all the Microsoft Updates when they arrive, as they include updates to help prevent cybercrime. Back up often and in different ways – if a criminal is in your device, they likely have access to your iCloud back-up – separate hardware back-ups are key! If you receive an alert for a threat detection from outside (i.e., identity protection software), take it seriously.

Make sure you train ALL users of your systems and keep training. If you use a shared network, then it just takes one person making a misstep for your entire system to be targeted. Purchase cyber liability insurance – review your insurance policies – what little protection is included in "standard" policies is simply not enough. There is a lot of money at stake – more pop up each day. The threat is not if it's when, but you can reduce your risk.

Joel and Michael then took questions from Rotary members and guests.

One member asked if small or large businesses are more at risk. They answered that they are equally at risk, but small businesses are targeted specifically because they really don't have cybersecurity protection.

Another member asked about employees who travel, work remotely, etc. – should they be connecting company (or individual) devices to unknown Wi-Fi? Do you have any recommendations for protection? Michael answered that having a VPN is key. It is better to connect to a well-known Wi-Fi Source if not at your secure location (examples being hotels, banks, etc.), but beware of small businesses as they may not have protection for you. The primary thing that you must do is to answer "No" to any pop-up on a Wi-Fi spot that asks if you will allow your device to be seen on a Wi-Fi network – it is literally opening a door that you don't know who is on the other side of the door.

Dena Diorio was asked about the Mecklenburg County cyberattack in 2017. She stated that they were able to restore some of the system, but others had to be rebuilt. Ultimately, it was decided not

to pay the ransom as there was no guarantee that they would not continue to be targeted. Mecklenburg County learned a lot from the attack and increased its cyber protection.

A member then asked why it is so hard to catch them. The answer is that they are very good at what they do and are experts at masking. Both the FBI and Homeland Security have tracked some, but most are out of their jurisdiction, so they must work with entities around the world – it is a difficult task.

It was asked if personal homeowners' insurance covers cyber-attacks, and if you are, what do you do? The best way to know is to check your policy and speak with your insurance company. In either case, notifying your insurance company and the police as soon as possible, so that there is early detection – it is key to catching someone. As soon as there is detection, then protection can start. Don't be afraid or embarrassed to report!

When they come in, what do they do? They are looking for your information, whether it is banking, social security information, your contact list, or your social media – they are looking for anything they can use against you. If you think something is spam, then it likely is. Delete it right away. In the case of e-mail, don't unsubscribe, just move it to spam. Delete and then block the phone number of anything you're worried about on text. Unsubscribing to a scammer lets them know they've hit a real person. Don't give them that opportunity.

A member asked if they had any recommendations for non-profits specifically to lower cost (such as banding together)? Do you recommend moving from Windows to Mac? The answer was surprising – it's not as expensive as you think, but banding together could help. Windows is the larger target today, but that's coming for Mac. They suggested that you team up with a strategic partner to help you prioritize how to use and protect your capital. They may not be after your donations necessarily; they may be after your donors. Generally, making it difficult for them as they are focused on numbers, and the harder it is to get in, the faster they'll move on.

The question was asked about services that can predict or foresee when someone has put something in your system. Some software can predict a threat, but it can't identify. LifeLock is a good product that monitors your credit. You can also freeze your credit with all 3 agencies – you can turn it back on when you need to, but that way no one can open any new credit in your name.

One guest who works for the Panthers asked about mobile tickets and sharing them – Is that an opening? The answer is yes. You protect yourself at the start by having a different password for each of your logins (i.e., Ticketmaster, etc.). Using simple and repetitive passwords is very dangerous. Michael shared that if possible, use different passwords for everything and make them LONG and complicated. Michael himself creates his own passwords using 26 characters with a mixture of letters, numbers, and characters. He only changes them when someone can't take that many characters. Use a password manager to keep up with your passwords.

The last question of the day was shopping online, when your browser asks if you want it to remember your password, what should you answer? The answer was an absolutely “no” – don’t create an easily hacked, less secure environment.

A recording of the meeting can be found here:
With Slides: https://vimeo.com/1117610617?fl=pl&fe=sh
Without Slides: https://vimeo.com/1117614912?fl=pl&fe=sh
The speaker’s introduction begins at approximately 25 minutes and 20 seconds.