'NETWORKINGS

SUMMER 2022

A PUBLICATION OF LOCKNET MANAGED IT SERVICES

locknetmanagedit.com
844-365-4968

A Message from Kris Kilgard, Locknet Division President

Summer is here and for those of us in the Midwest who have survived a long winter, we think about taking a break, enjoying some vacation, and finding time to relax in the nice weather. Wouldn't it be great if all the cyber criminals and bad actors out there took vacations too? Unfortunately, we know that isn't the case. Instead, it's more important than ever to be vigilant. Over the last few years, we are seeing more activity from bad actors during national holidays and other normal vacation times.

Of particular concern to me is the approximately 40% uptick in published rates of ransomware activity in the first half of 2022. We continue to stress the importance of having the right technology and employee training in place to recognize threats. As your trusted partner, we continually monitor feeds and make sure your network is resilient, but everyone plays a role in knowing what to look for and maintaining vigilance.

Take a minute to think about how your business has likely changed already in only the first half of the year. Do you have new employees? Are you expanding? Do you have a new location? Is your workforce at home? Did you add new technology for your customers? Most of our clients have experienced some level of change this year and it is rewarding for us to help facilitate that change by leveraging technology to make sure the change is implemented securely.

There are a lot of good takeaways in this issue of our newsletter, but I'm sure it can also seem overwhelming. Penetration testing, email security, dark web monitoring, employee training, breach detection—all of them are important. And for most small to midsized businesses, we understand it's too much to tackle on your own. Over the last few months, I have noticed our team working with clients on prioritizing some of these items. Whether it's budget or time constraints, it can be difficult to implement everything at once. I am proud of how our team works on long-term plans with our clients to constantly improve their security position.

Lastly, I'm honored to say we were recognized this year by the Better Business Bureau with the Torch Award for Ethics (see pg. 6), and trust is at the heart of this recognition. The growth Locknet has experienced so far this year is a combination of the trusted partnerships we have with our current clients, the trust new clients have put in us, and the trust our clients have in the superior customer service experience provided by our amazing team.

I hope you can relax and enjoy this summer with the peace of mind that your network security is in good hands. We know what we do is critical to your business, and we thank you for putting your trust in us.

No one wants to be a victim of a ransomware attack. Understand how an attack starts, the demands, and the security solutions needed to guard your data.

WHAT'S **INSIDE**

LOCKNET
AN EOJOHNSON COMPANY

The Path to a Ransomware Attack and the Consequences

No one wants to deal with a ransomware attack in their organization. If it's successful, the attack will not only be a major drain on company resources but will also create complications that could reverberate for ages. Even worse, it could put an organization out of business. According to the National Cyber Security Alliance, 60% of small and midsized companies will go out of business.

1 Behind the scenes

Stopping cybercrime is difficult because new ransomware gangs crop up constantly. They can form organically, spawn from other groups, or emerge as a new version of another big player. No matter how the group develops, a ransomware attack starts with the formation of a squad of attackers. And even cybercriminals are outsourcing these days. Most ransomware gangs recruit affiliates to conduct the actual attacks. It's standard practice for big ransomware outfits to hire help and acquire resources in dark web forums.

2 How it starts

Ransomware is almost always the poisonous cargo of a phishing attack. Cybercriminals use the information they gathered from the dark web and other sources to carefully craft a phishing email that will be especially appealing to your employees. The email makes it past your security and lands in your employees' inboxes. One of your employees takes the bait, opens the email, and interacts with it by visiting a poisoned website or opening a tainted attachment. The malicious payload infects the computer, and the computer then establishes a connection with the cybercriminals' network to encrypt your data, and in some instances, publish your data on the internet for all to see.

3 The bad guys demand payment

If the attack is successful, the cybercriminals will demand payment. The bad actors may demand payment for a decryption key to unlock systems and data or for the safe return or destruction of the stolen data. The most common type of attack now involves double extortion. In this scenario, the cybercriminals demand two payments from the victim—typically one payment for the decryptor and a second payment to stay quiet about the victim's security failure.

The U.S. Federal Bureau of Investigation Internet Crime Compliant Center (IC3) broke down the cybercrimes recorded by the Bureau in 2021. IC3 received 847,376 complaints in 2021, a record number that's up 7% from 2020. Even more alarming was the dollar amount. The total amount of loss reported hit a new record high in 2021 of $6.9 billion, a 48% increase from 2020.

4 The payment fallout

Unfortunately, many who fall victim to ransomware choose to pay the extortionists. This brings negative consequences for everyone. When the bad guys receive a pay out, the scheme works, and they continue to use it. But paying up doesn't usually solve the problem for the victim. Even if a ransomware victim pays, the data may have already been copied or the bad actors may have left a backdoor into your system to return later.

It's also illegal. In October 2020, The U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) announced that paying ransom to cybercriminals is unlawful.

5 Businesses suffer negative consequences

The outcome of a ransomware attack can vary by organization. A snapshot of what companies might expect after a ransomware incident include data loss, downtime, lost profits, reputation damage, and compliance failure. The expense of a ransomware incident also snowballs in the aftermath, leaving a variety of challenges in any organization.

6 Smart solutions to avoid ransomware

The best offense is a good defense. Instead of paying extortionists, invest in strong security measures now to prevent future attacks.

Since phishing is the most likely way for a ransomware attack to start, phishing simulations through Security Education and Awareness Training are effective at reducing an organization's risk by making employees better at spotting and stopping phishing.

Locknet Managed IT's Security Education and Awareness Training program is the ideal solution for businesses of any size.

- Bolster your defense by creating a "human firewall."
- Pre-test simulated phishing attacks to identify how phish-prone your organization is currently.

Continued on next page.

- Employees will learn how to identify common threat tactics such as social engineering, phishing, spoofing, and ransomware.
- 36-month online training program includes case studies, live demonstration videos, and final tests to ensure employees retain the information.

As employees are armed with the necessary cybersecurity knowledge, the stronger your first line of defense will become. However, human error happens and you should always have a plan B in place.

Locknet Managed IT's Managed Detection and Response Service can help protect your business with monitoring and detection if threats like Ransomware slip past your "human firewall."

- 24/7/365 monitoring
- Stops hidden threats that sneak past other security tools
- Detects, analyzes, and responds to attacks through both human intelligence and automated technology

Partnering with Locknet's team of trusted professionals can provide businesses with smart solutions to help avoid ransomware.

By instituting proper education practices along with a vigilant monitoring and detection solution, you can help prevent security threats from happening and quickly mitigate any damage if they do. Contact your local Locknet Account Executive for more information.

locknetmanagedit.com/it-support-services

A Message from our Owner and CEO

Our cornerstone core values of caring, customer vision, trustworthy, and resilient haven't varied much since my dad, Emery O. Johnson, founded the company in 1957. Over 65 years, we have grown from a single office in Wausau, WI to be in our second generation of family ownership, woman-owned, and with seven offices throughout the Midwest. Throughout that growth, we have remained committed to caring for the clients and communities we serve.

Our decision to acquire Locknet Managed IT 10 years ago is an important part of EO Johnson's history. It made us an even better partner to the business community. While we were confident in our expertise as a printing, copying and scanning business resource, acquiring Locknet Managed IT made the entire company more knowledgeable about security. We are always looking for what's new and what's coming next—adapting to the changing technology trends. Many of those changes are positive. But in the world of IT network management, it also means recognizing new risks and identifying the best security strategies to keep the bad guys out. Today, everything in your business is connected—from your copier, to scanning, to document management, to computers, to firewalls, to at-home workers, to the cloud. We listen, help with your business needs today, and prepare you for the workplace of the future.

Locknet Managed IT takes on additional compliance scrutiny knowing it will not only make our company better, but it will also make our clients better. Very few in our industry can state they are SOC 2 Type II certified and FFIEC examined. No matter the industry, our clients benefit from the commitment we make to meeting these additional compliance standards.

We are grateful for the businesses that have understood the value of our expertise, allowed us into their company's vision, and trusted us to keep their businesses secure. Thank you. Thank you for your partnership. Thank you for your trust. Thank you for being part of our family.

Mary Jo Johnson
CEO/Owner

NEW SERVICE AVAILABLE

Penetration Testing: Next Level Cybersecurity

Here's what you need to know about pen test and your network security

Penetration testing, or pen test, is the latest addition to the arsenal of network security strategies here at Locknet Managed IT. But what is penetration testing? Is it suitable for small and medium-sized businesses? And how does it protect your organization from cybersecurity threats? Let's explore.

What is penetration testing, or pen test?

Imagine letting someone hack into your network, someone who knows how to find the weakest link in your system that can be exploited. It sounds unthinkable, right? After all, preventing intrusion by hackers is why you have a cybersecurity strategy in place. Well, penetration testing does just that—but with a hacker who is here to help, not hurt.

Penetration testing leverages ethical hackers to identify, breach, and fix vulnerabilities in your business's network, website and more, before cybercriminals take advantage of these weaknesses. This process allows for evaluation of an app or network, so that issues can be flagged, ranging from login-related weaknesses to configurations to user vulnerabilities. It also can allow for evaluation of your security strategies and other cybersecurity efforts in place. Once our cybersleuths identify your system's weaknesses, we develop a penetration testing report detailing what we've found, the associated risks, and our recommendations for addressing these vulnerabilities. The overriding goal is to shore up your protections so hackers don't have a chance at conducting a security breach.

Penetration testing versus vulnerability assessments

We've talked in the past about the importance of vulnerability assessments to your organization's cybersecurity. And while pen test and vulnerability assessments may sound similar, there are distinct differences between the two. Here are a few noteworthy differences.

- Vulnerability assessments are primarily automated; pen test includes both automated scanning and manual testing
- Penetration testing includes exploiting weaknesses to learn from them, while vulnerability assessments are primarily about detecting and categorizing any system vulnerabilities.
- Pen test can find logic errors that a vulnerability assessment can miss. This is due to the added manual testing.
- The investment in penetration testing is greater, as it takes considerably more time and resources. Vulnerability assessment takes less time and money, but isn't as comprehensive; it simply identifies vulnerabilities. Pen test identifies those vulnerabilities, ranks them and explains how easily exploited they are, enabling them to be addressed in alignment with organizational priorities and goals.
- A vulnerability assessment locates security flaws. A pen test exploits those vulnerabilities so you have a clear idea of what's at stake, and how much damage your organization could suffer in a cyberattack.

Note that the terms penetration testing and vulnerability assessment are not interchangeable; though they can be employed in tandem with one another. Both can play an important role in evaluating your security and strengthening your network protections.

Penetration testing leverages ethical hackers to identify, breach, and fix vulnerabilities in your business's network, website and more, before cybercriminals take advantage of these weaknesses.

Are you ready for a pen test, or penetration testing? We can help.

When you're ready to put a pen test to work for your business, the in-house experts at Locknet Managed IT can help. Our penetration testing service is conducted by our own team of experts, never outsourced. This service provides a deeper level of protection which can be beneficial to small and enterprise-sized businesses as the threat environment becomes increasingly more daunting. To learn more about pen test, or penetration testing, and the other cybersecurity options we offer, contact your local Account Executive at 844-365-4968 or go to locknetmanagedit.com and request more information.

Locknet Information Security Director Receives Distinguished CISM Certification

Shannon Mayberry, Director of Information Security for Locknet Managed IT, recently received his Certified Information Security Manager (CISM) certification. Shannon has been with Locknet Managed IT for 14 years and, in that time, has become a trusted resource for our clients.

CISM is an advanced certification recognizing Shannon possesses the knowledge and experience required to develop and manage enterprise information security programs. Through the certification process, Shannon demonstrated his ability to review information security goals within the context of a business's other objectives and set up comprehensive security programs.

"Shannon's desire for continual learning exemplifies Locknet's commitment to keep our clients secure and productive. The threat landscape is changing at a rapid pace, and it takes an ongoing commitment to stay ahead of the risk," said Kris Kilgard, President of Locknet Managed IT. "When we bring on a new client, we commit we will do our best to keep their business secure. Shannon's expertise and leadership are vital to upholding that commitment."

Shannon also holds a Certified Information Systems Security Professional (CISSP) certification. CISM and CISSP are two of the most highly regarded certifications for cybersecurity leaders. Shannon is among an elite group in his profession to hold both a CISM and CISSP certification.

Protecting Email Address Privacy Using BCC

BCC, which stands for blind carbon copy, allows you to hide recipients in email messages. For security and privacy reasons, it is best to use the BCC feature when sending an email message to a large number of people. Whereas any email addresses that you place in the To field or the CC field are visible to everyone who receives the message, addresses placed in the BCC field are invisible to the recipients of the email.

Benefits of Using BCC
Using the BCC field to send an email message to a large group of people has a number of benefits, including:

- The privacy of email addresses is protected in the original message. Recipients will receive the message but won't be able to see the addresses listed in the BCC field.
- When an email is forwarded, the addresses of everyone in the To and CC fields are also forwarded along with the message. Addresses that have been placed in the BCC field are not forwarded.
- If you have placed a large list of recipients in the To or CC field, all of them will receive the reply. By placing recipients in the BCC field, you can help protect them against receiving unnecessary replies from anyone using the Reply All feature.
- Many viruses and spam programs are now able to sift through mail files and address books for email addresses. Using the BCC field acts as an anti-spam precaution. It reduces the likelihood that recipients will receive a spam message or a virus from another recipient's infected computer.

How to Use BCC in an Email
Most email clients have the option to BCC a few lines below the To: field. However, sometimes it is a separate option that is not listed by default. If you cannot locate it, check the help menu or the software's documentation.

If you want to BCC all recipients and your email client will not send a message without something in the To: field, consider using your own email address in that field. In addition to hiding the identity of other recipients, this option will enable you to confirm that the message was sent successfully.

LOCKNET
AN EOJOHNSON COMPANY

locknetmanagedit.com
eojohnson.com
844-365-4968

IOWA

129 Plaza Circle
Waterloo, IA 50701

MINNESOTA

2717 Hwy. 14 West, Suite M
Rochester, MN 55901

1800 East Cliff Road, Suite One
Burnsville, MN 55337

WISCONSIN

1505 Prairie Lane
Eau Claire, WI 54703

3310 S. Kinney Coulee Rd.
Onalaska, WI 54650

505 S. 24th Ave., Suite 204
Wausau, WI 54401

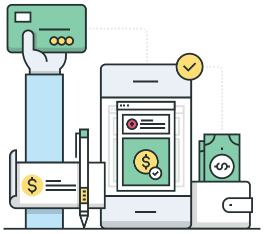
8400 Stewart Ave.
Wausau, WI 54401

Pay the easy way with ACH!

Did you know your Locknet invoices can be paid through ACH? Electronic payment processing through ACH has several benefits:

- Security of your payment
- Environmentally friendly
- Reduced time and associated costs
- Easier processing for your remote workforce

We hope you will join us in our commitment to an easier and greener form of payment processing. Reach out to your Account Executive to get started.



Locknet Managed IT Ranks Among Industry's Best-in-Class Businesses

For the seventh consecutive year, Locknet Managed IT has been selected as one of the technology industry's top-performing providers of managed services by the editors of Channel Futures. The Channel Futures MSP 501 survey examines organizational performance based on annual sales, recurring revenue, profit margins, revenue mix, growth opportunities, innovation, technology solutions supported, and company and customer demographics.

MSPs that qualify for the list must pass a rigorous review conducted by the research team and editors of Channel Futures. It ranks applicants using a unique methodology that weighs financial performance according to long-term health and viability, commitment to recurring revenue and operational efficiency.

"It's great to see us on Channel Futures' MSP 501 list again this year," said Kris Kilgard, Locknet Division President. "We are proud of the innovation and support we provide for our growing client base."

Channel Futures is part of Informa Tech, a market-leading B2B information provider with depth and specialization in the information and communication technologies sector.

Channel Futures.
Leading Channel Partners Forward
MSP 501
2022 WINNER

Torch AWARDS
BBB for Ethics
2022 WINNER℠

We are proud to announce that EO Johnson Business Technologies was named a 2022 Better Business Bureau Torch Awards for Ethics winner.

Since 2003, the Better Business Bureau (BBB) has honored businesses and non-profit organizations of all sizes that meet the highest standard of ethics and trust among their employees, customers and local communities, embodying BBB's mission to advance marketplace trust.

"My dad, Emery O. Johnson, always believed if we do what's right, the right things will happen," said Mary Jo Johnson, Owner and CEO of EO Johnson Business Technologies. "That remains the very blueprint of our organization today, and I know he would be proud that this organization continually lives up to that ambition."

Locknet Managed IT, an EO Johnson company, is committed to being a trusted resource for our clients. Our role as a managed service provider is a critical part of your business, and we truly value the partnerships we have developed.

EOJOHNSON
BUSINESS TECHNOLOGIES