ReadiTech
A DRN COMPANY

TECH TIMES

READITECH BUSINESS TO BUSINESS PUBLICATION

Quarter 1 | 2024

A Day in the Life of a ReadiTech Expert

DAVID MALSAM

The statement "A Day in the Life" can be used to describe a routine or typical happenings of any person or profession. We are starting a new series of articles which focus on the daily happenings of our ReadiTech employees.

David Malsam, senior network analyst for Readitech Managed Services is going to walk through his "A Day in the Life."

"The best part about my job is that I am never bored and am always doing different things for different people. I also get the chance to collaborate with great people and customers." Said Malsam.

For David, who works out of ReadiTech's Aberdeen office, every day starts the same. He usually gets in the office around 8:00, and usually logs in right away to check the status of computer back-ups for clients, and to make sure that everything is backing up correctly. Also, at this time he usually will check the service board on our ticketing software for new RMM alerts. RMM alerts stands for remote monitoring and management and is software installed on computers and devices that watches and provides warnings of potential problems. If RMM provides alerts of problems or potential problems, David, and Michael Wegehaupt (another network analyst in the Aberdeen office) will call clients to communicate with them what the problem or potential problem may be, and what the next step would be in finding a solution to the problem.

"The best part about my job is that I am never bored and am always doing different things for different people. I also get the chance to work with a lot of great people and customers."
– David Malsam

From there, it is usually about mid-morning by now, so David and Michael move on to reviewing open tickets on the service board and are communicating with each other on what projects or customers they are dealing with for that day. At this time, they are also communicating with each other on what one another needs help with and if they will be out of the office on any project installations or service calls later in the afternoon.

Customer and client communication, working on projects as needed or simply updating clients on the status of current projects continues throughout the day. They are also working on service calls and dealing with projects from walk-in customers. Also in the afternoon, David and Michael will go on site to certain businesses for service calls if required for the specific project. If being on-site is not required, David and Michael call customers to communicate with them, resolve issues to problems or discuss solutions to these problems as well.

Sometimes Network Analysts are referred to as "heroes" by their clients because daily they are troubleshooting issues. David recalls helping a customer during a power outage. "There was a customer who had several systems that had shut down. I went on site and found a way to get all the machines and systems back on and working properly." This customer thought David was a "superhero" in the sense that it prevented them from having to shut down their business or part of their business for the rest of that day.

Protect Your Security System from Hackers

Simple knowledge to protect yourself online applies to not only computer and device safety; it also applies to your security system. From a simple doorbell camera to a fully integrated security system, more people are taking protective measures to keep their home and business secure from break-ins and protect against theft.

Here are some helpful steps you can take to prevent hackers from accessing your security system. These steps are not difficult, and are quite simple, but don't let that fool you into thinking they're not important in protecting your security system.

Tips to Protect Your Security System

1. Keep your system and camera's firmware updated. Manufacturers routinely release firmware updates to fix software bugs and patch security vulnerabilities. Some cameras will automatically download and install these updates, while other require you check for updates and update them on our own. Look to update your camera, under the settings menu of your camera's app.

2. Change your systems and camera's password. You might be surprised to learn how often security systems use the default password. Change your password from the default set up and don't use the same one for all your security or online accounts. That makes it easy for hackers to gain access to multiple accounts.

3. Set up a password manager. Whether you use a free password manager or use ReadiTech's password vault Keeper, password apps like these help you generate strong, random passwords for your online accounts. Password managers securely store your usernames and passwords for websites. We recommend you use an app with two-factor authentication to ensure your usernames and passwords remain secure and are only accessible by you.

4. Set up two-factor or multi-factor authentication if your system offers it. This extra layer of security involves you opting to have the camera company send you a one time-use passcode via a text message, phone call, e-mail or authenticator smart app. Two-factor authentication includes two layers of protection. If your username and password were hacked, your security camera is still secure since the second layer is a one-time code used to access it each time.

These are valuable tips in ensuring your security system keep you and your property safe. While there are many security systems available with easy-to-access surveillance to 24/7 monitoring, ReadiTech has the best security system options for you.

Contact ReadiTech 877-559-4692 to learn more about security options for your business or visit readitech.com.

PROTECT YOUR BUSINESS FROM CYBERATTACKS

As our world continues to become interconnected, cybersecurity continues to grow in significance and complexity. Do you know how to protect one of your most valuable assets? Your Data.

What if your customers' sensitive credit card data was stolen from your database? Or, what if your employees' cell phone and laptop were comprised giving hackers access to your network? These are real situations that can cripple your reputation and business. In fact, 60% of SMBs go out of business within six months of a cyberattack according to Connectwise, a cybersecurity IT management software provider.

ReadiTech recommends the most important step in preventing a cyberattack is to identify your greatest areas of risk for a security data breach. The most critical risks are not only within your IT environment, but in the processes, policies, and procedures that can leave you open to popular phishing and social engineering attacks.

CYBERSECURITY CHECKLIST:

You can't afford to find out after a breach where you are vulnerable. From performing security assessments to multi-factor authentication and encryption, ReadiTech recommends these critical ways to protect your business in 2024 from cyberattacks.

❑ **Security Assessment**
Establish a baseline and identify critical areas. ReadiTech can help you develop a plan to fit your budget. Close existing vulnerabilities and strengthen your security.

❑ **E-mail Anti-Virus/Spam Filter**
Secure your e-mail. Most attacks originate by e-mail. The ReadiTech team will help you choose a service designed to reduce spam and your exposure to attacks.

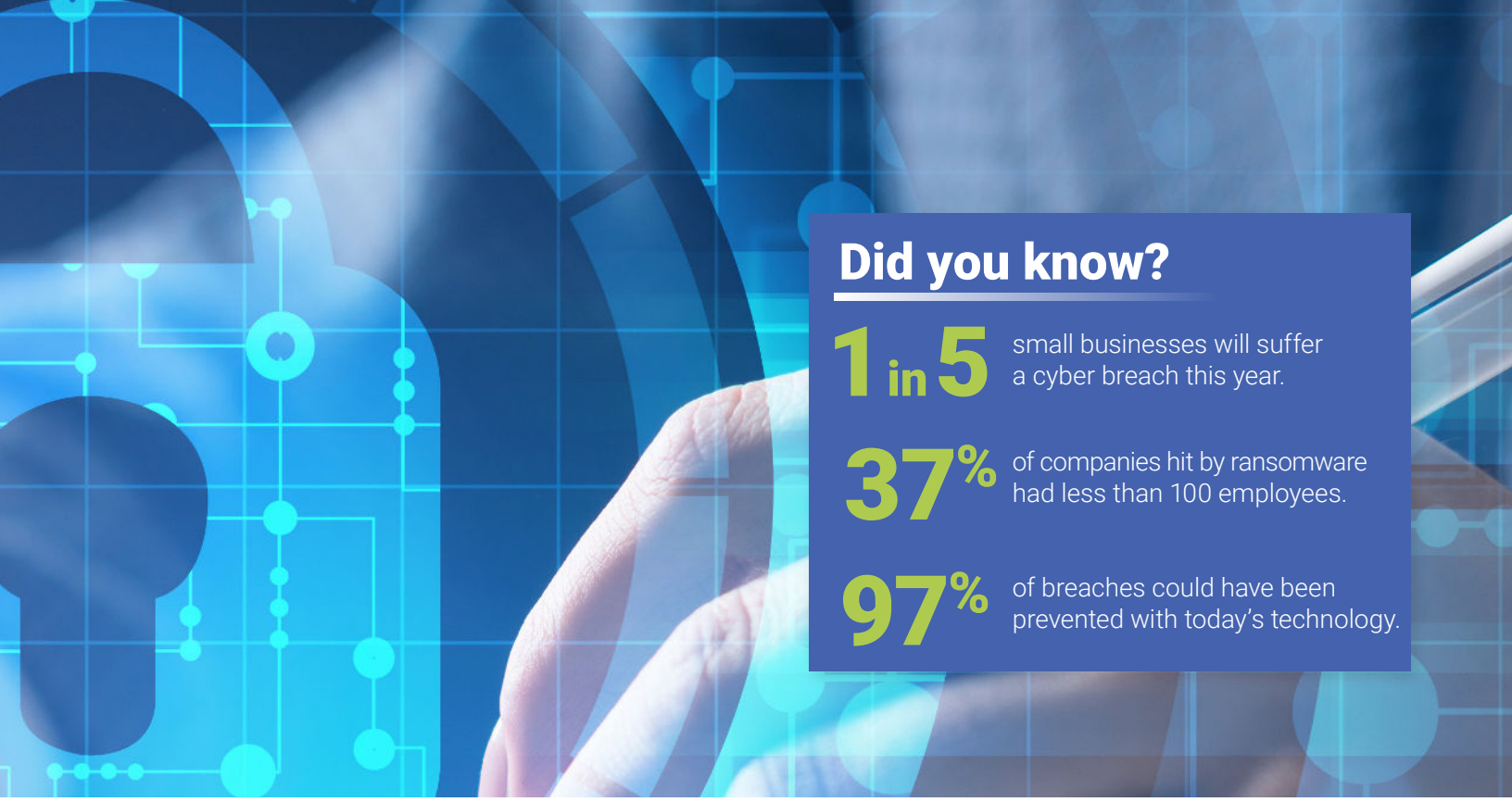
❑ **Security Awareness Training**
Train your employees often! Teach them about data security, e-mail attacks and your policies and procedures. ReadiTech offers web-based training solutions.

❑ **Endpoint Detection & Response**
Protect your computers data from malware, viruses or file-less and script-based threats.

❑ **Multi-Factor Authentication**
Add an additional layer of protection to ensure if your passwords are stolen your data is still protected.

❑ **Computer Updates**
Keep Microsoft, Adobe and other applications up to date. ReadiTech provides a "critical update" service via automation to protect your computers from the latest known attacks.

Checklist continued on page 3



Did you know?

1 in 5 small businesses will suffer a cyber breach this year.

37% of companies hit by ransomware had less than 100 employees.

97% of breaches could have been prevented with today's technology.

Now, more than ever, IT security plays a critical role in the success of your business. Whether your business is looking to protect your devices and network from cyber-attacks or train your employees on the latest phishing attacks, we're here to help you achieve a secure, seamless and hassle-free network. Call ReadiTech today at 877-559-4692 to learn how your business can improve cybersecurity to protect valuable data.

According to a report by Cybersecurity Ventures, the global cost of cyber crime would hit $8 trillion in 2023 and increase to $9.5 trillion in 2024.

Cybersecurity Ventures is a leading researcher and trusted source for cybersecurity facts, figures and statistics.

❑ **Web Gateway Security**
Internet security is a race against time. Cloud-based security detects web and e-mail threats as they emerge on the Internet and blocks them on your network within seconds.

❑ **SIEM (Security Incident & Event Management)**
Uses big data engines to review all event and security logs from devices to protect against advanced threats and to meet compliance requirements.

❑ **Firewall**
Turn on intrusion detection and intrusion prevention features. Monitor incoming and outgoing network traffic and send the log files to a managed SIEM.

❑ **Backup**
Backup your important data so it can be recovered if deleted or becomes corrupted. Back up automatically and test to ensure files are available and working correctly.

For more ideas to take your business cybersecurity to the next level, visit readitech.com.

This institution is an equal opportunity provider and employer.

ReadiTech
A DRN COMPANY

ReadiTech HQ: P.O. Box 69, Ellendale, ND 58436-0069

NEED A CLEANUP?

Spring forward with an organized & secure network.
Call in the experts.

CLIENT FOCUSED—TECHNOLOGY DRIVEN

877.559.4692 • www.readitech.com