2020 has been a groundbreaking year on many fronts. Unfortunately, the majority of them have not been good ones. On October 28, 2020, the FBI, HHS, and CISA jointly reported on an imminent threat to healthcare organizations (the Health and Public Health Sector) surrounding the Ryuk variant of ransomware and other malware most recently seen accompanying it. “We are experiencing the most significant cybersecurity threat we’ve ever seen in the United States,” said Charles Carmakal, Chief Technical Officer of the cybersecurity firm Mandiant, in a statement.

While this specific report was focused on the healthcare sector, the truth is that all businesses are increasingly vulnerable to cyber-attacks, and attackers seek those who are a good match for their malware and their skills. They care far less about what type of company you are.

Many cyber-attacks involve ransomware, a form of malicious software or malware, designed to deny access to a computer system or data until a ransom is paid and a decryption key (commonly called a decryptor) is given to the victim. The encryption is virtually unbreakable without the decryption key, and you should not spend valuable time seeking a way around the encryption if you are attacked with it. Ransomware can spread in multiple ways, but most typically, through phishing emails or by unknowingly visiting an infected website. Ransomware can be catastrophic to healthcare and other organizations, preventing critical information and systems for patient care from being accessed, for example.

ConvergeOne never advocates paying the ransom to cybercriminals. You are paying a criminal organization to extend their attack infrastructure further, rather than putting them out of business. Instead, you should build a cyber-aware culture within your organization and proactively follow a number of steps to keep your information and people protected from cyber-attacks.

As we plan for 2021, here are 21 cyber tips to get your organization started.
Cyber Tip 1: Do you know precisely what to do if you get hacked?

- Contract or create an incident response team, develop an incident response plan, and routinely test that plan to lock in improvements. Get help. Testing incident response is not easy.

- Disconnect or Turn off WiFi and Bluetooth. Unplug storage devices.

- Determine scope – shared drives / folders, network storage, USB, external storage, cloud-based storage, etc. Do you know what your “crown jewels” assets are and moreover, where they are?

- Check tools in use like Box, Dropbox, and Google Drive. You may be able to revert to unencrypted versions of your files that reside there. Know your RPO, Recovery Point Objective. What is the oldest saved information I can revert back to that still has current value to me.

- Know your backups, what is and isn’t backed up, and the order that restores much take place.

- Know your firm’s RTO, or Recovery Time Objective. How long do I have to get my files back before I start losing revenue every hour I have no access?

- We do not advise paying the ransom, but if you do, remember you need to reconnect encrypted drives to unencrypt them if you’ve disconnected them.

- Usually the attacker will give you access to a registry to file listing that has been created by the ransomware listing all files encrypted. Try to use Google to understand the version of ransomware you have been hit with. It’s important.

- Determine if your data or login credentials have been copied, and if so, how much and what. This can often be learned from the ransomware program’s announcement itself, as it brags as to what data has been copied or the information regarding your stolen data that the hacker posts on websites or blogs.

- Check your logs and any data loss prevention (DLP) tools to see if it noted any stolen data. Look for large unauthorized archive (e.g., zip, arc, etc.) files that contain your data that the hacker used for staging before they copied it. Look into any systems that might record large amounts of data being copied off the network. Look for malware, tools, and scripts that might have been used to look for and steal data. The main initial sign to look for to see if your data and credentials have been stolen is the ransomware gang telling you they have done it.

- Lastly, if the ransomware gang tells you they have your data or credentials, believe them. They don’t bluff that often. Do not panic.

Cyber Tip 2: Spear Phishing is a type of phishing attack that targets an individual or set of individuals. How can you combat spear phishing?

Don’t open a message or a link just because the correspondent seems to know a lot about you and never be afraid to ask before committing to any next step requested by the sender, especially if the sender signals a sense of urgency.

You should also send a “voice of leadership” messages to everyone containing guidance on what to look for, who to call, what to do, and that it is okay to not click or respond to any message that looks unusual or suspicious.
Ensure you are simulating phishing attacks against your users regularly to ensure they are sensitive to real approaches attackers will take. Have a continuous learning platform to deliver them. Educate staff to detect fast:

- “I can’t open normal files and get corruption error or my files have a strange extension.”
- “I get alarming messages indicating my computer has been infected and I cannot close them.”
- “I see a countdown timer on-screen.”

**Cyber Tip 3:** Your information is at risk everywhere: your home, your doctor’s office, getting coffee at the local coffee shop. Take heart and protect yourself.

Use Multi-Factor Authentication everywhere you log in, as you need a second mechanism to authenticate to system resources that is independent of that password. Use passwords that are made up of multiple random words strung together, with numbers and special characters. Leverage every privacy control available on social media, and develop a healthy skepticism of trusting any information or messages from those you do not know.

**Cyber Tip 4:** Are you a cyber pro in need of a great metric to report to your leadership?

Report on how many times per day you get attacked, but you thwart the attack. How? Start at the outside interface of your perimeter firewall. Pull stats indicating your number of dropped packets at that interface. Do it for 30 straight days. It will give you a good idea of how many attacks you are defending against. Your leadership will gain perspective and you will gain credibility with them.

**Cyber Tip 5:** One of the easiest ways to protect your security is to keep your software up-to-date.

Patch operating systems, software, and firmware as soon as manufacturers release updates. Advise remote users not using company-owned assets to turn on auto-update and ensure they are current on software and patches, as well.

Also, make sure to take one additional step after an update and check your privacy settings. Sometimes the update reverts them back to a prior default setting.
Cyber Tip 6: Cyber pros and consumers beware! Dark Web monitoring is not something you check or sign up for only if you have been notified of a breach.

Your personally identifiable information may get swept up in the endless tide of breaches. The appearance of your firm’s data on the dark web requires prompt notification to your business. Contact ConvergeOne today to find out more about how we help hundreds of organizations keep from being a future dark web victim.

Cyber Tip 7: Today more than ever, insider threats and attacks that leverage identity vulnerabilities remain a blind spot for even the most advanced companies.

Your firm’s digital transformation needs modern, identity- and workload-centric Zero Trust security solutions to protect your work-from-home workforce. Remember: Companies that wait to act are tempting fate, so please ask us about Zero Trust today.

Cyber Tip 8: Attackers gain a foothold of your information by investigating your habits, actions, favorite things, and the names of your family and friends.

When it comes to social media, own your online presence. Share only to your comfort level, not beyond it. Why make cybercriminals’ jobs easier by giving your information out freely on social media? This allows criminals to guess your passwords that could contain items of significance to you (e.g., your favorite car, your wife’s name, your kids’ birthdates, etc.) and break into your personal and financial data. Remember to be a good online neighbor. Post only what you would have someone say about you—not more—and always operate under the premise of “don’t know you, don’t trust you.”
Cyber Tip 9: Are you protecting your home environment from cyberthreats? How many times have you ventured to a sketchy website?

Place a new DNS (URL) address on your router that points to a filtering system, protecting your family’s web surfing. Open DNS (Cisco Umbrella) for home use will provide you with a range of protective measure. You will be able to control what is seen (inappropriate content) and be secured from risky sites.

Cyber Tip 10: We are a “clicky” society. Train yourself to think before clicking on a link or opening an attachment in an email.

At times, we open email attachments without looking at who sent them or details in the email header. We’re distracted by current events like COVID-19 or the election, so we tend to open emails to retain information—and at times are opening up a pandora’s box. Always be aware of the source and information being sent.

Cyber Tip 11: Know what’s going on under your nose. “Dwell time” is a saying meant to describe how long an intruder is sitting within your network and collecting information before you notice it.

The average dwell time is 180 days before you even realize that a cybercriminal has infiltrated you network! By employing a Managed Detection and Response (MDR) plan into your environment, you can be made aware of traffic that is outside the normal range (anomalies) and increase your threat hunting capabilities. This will allow for visibility throughout and will help you take action when needed.

We also often see Remote Access Trojans (i.e., a RAT) included with ransomware that are hard to locate and eradicate. A RAT is malware that includes a back door for administrative control over the target systems. RATs are usually downloaded invisibly with other malware, like ransomware. Once the host system is compromised, the intruder may use it to distribute RATs to other vulnerable computers and establish a botnet or use it as a future entry point even after the ransomware portion of the payload has been thwarted.
Cyber Tip 12: Credit card and financial data extraction are on the rise. The handling of data is as important as credit card information.

PCI-DSS is a standard that merchants must follow. In fact, three states (Nevada, Washington, and Minnesota) have made it law. More will follow. The handling of data is as important as credit card information. Both physical and electronic handling should be taken into account, in terms of who has access to the information and what they are doing with it.

If there is no need to house customers’ data, then ensure that once the transaction has completed, no information is kept on the network. If there is a need to house credit card data, ensure proper masking techniques are employed. Only the last four digits should be visible, and these should only be used for authentication and authorization purposes. Clients should be aware that they should never share this information over the phone, and that four digits should be the normal request.

Cyber Tip 13: Are you practicing basic password hygiene?

At times, we forget that passwords should not be our favorite cars, children’s name, ages, pets, or birthdates. We should be vigilant in ensuring our passwords are not easily guessed in order to keep our data private. An important factor is to NOT reuse personal passwords with corporate assets or vice versa. If a cybercriminal were to break into a personal Gmail account with the same password that is being used for your database at work, they will have access to critical company assets. If you’re thinking to yourself, “I could never remember that many passwords,” then use a password manager that encrypts the information on your device to keep it away from prying eyes.
Cyber Tip 14: Do you use different profiles when you are on the internet? Remember to compartmentalize.

Don’t let a compromise of one account lead to a compromise of many. Use different names and random word passphrases for:

- Work-related activity
- Social networking sites
- Shopping and e-commerce
- Banking, finance, and stock trading

Cyber Tip 15: Avoid public Wi-Fi! When at the airport, hotel, coffee shop, or other public space, using free Wi-Fi opens you up to many possible threats.

If possible, try not to connect at all, but if you need to, ask and understand the exact SSID (the wireless network name) of the official public Wi-Fi network at your location and keep your connection time short. Also, do not allow auto-connections to public Wi-Fi. Hackers can load malware, steal your passwords and PINs, or even take remote control of your contacts and camera.

Cyber Tip 16: When it comes to data breaches, believe half of what you see and none of what you hear.

When a data breach gets announced to the public, very often details are still being investigated by the organization announcing the breach and their forensic teams. Even if you are told you are not affected by a breach of a site you use or visit, change your passphrase immediately and be suspicious of any unusual activity on your accounts. Cyber criminals can use data stolen to achieve goals like various forms of extortion and other economic crimes.
Cyber Tip 17: Update those browsers! Browsers should all have secure design, secure features, and be updated regularly.

Unfortunately, some browsers are more secure than others. At minimum, make sure you are using the most up-to-date version of your browser and any associated plug-ins. If you can’t update your browser due to compatibility issues, have two browsers. Consider the one you can update your “privacy” browser for any activity that involves sensitive data and choose that browser carefully based on its security attributes.

Cyber Tip 18: Smartphones beware: When was the last time you checked the URL of the site you were visiting on your smartphone?

Hackers are getting smarter by embedding malware into sites that look authentic. Ensure your banking and financial sites are real before divulging your username and password. Better yet, try banking on a laptop, which houses anti-virus and malware features for your protection.

Cyber Tip 19: Prying eyes are everywhere. Keep your desk, work area, or office free of “useful information” clutter.

Your notes, files, and documentation could provide a passerby information on medical, financial, and client information—which leads to privacy issues and, ultimately, fines and penalties.

Cyber Tip 20: Sometimes it’s good NOT to share. Never give more information out than you should.

Ensure the person on the other end of the line is who they say they are, perhaps by having them confirm a specific item or action. Provide as minimal information as possible for authentication, as giving them more data could lead to a possible compromise.
Cyber Tip 21: Ever hear of a link verifier? Two link verifiers you can try are https://urlvoid.com and https://sitecheck.sucuri.net

Link verifiers are free, web-based tools that analyze domain names and URLs to tell you if a site is blacklisted or not. Now remember: Never automatically click on a solicitation or request to log into anything. Become a proactive compromise preventer!

Please take the information about cyber-attacks included at the beginning of this white paper very seriously, follow the cyber tips, and get help wherever necessary. The purveyors of these attacks are criminals, pure and simple, and they have no remorse for their actions. If you need help, ConvergeOne is here for you. With our help, you can avoid becoming tomorrow’s headline. We can assist with the following:

- Health Checks
- Training
- Incident Response Planning, Testing and Services (7x24, 365 days)
- Licensing

Please contact us via your ConvergeOne National Account Manager or email jvigorito@convergeone.com and cripkey@convergeone.com (send to both simultaneously).

About the Authors

Joe Vigorito is the Senior Director, Cybersecurity Lifecycle Consulting in ConvergeOne’s National Cybersecurity Practice. For eleven years, he was the Chief Information Security Officer for the largest industrial and atmospheric gas company in the world, including “chemicals of concern” facilities. For the last several years, Joe has provided guidance and advisory counsel to various major corporations and public sector entities on elevation of their cybersecurity posture, including areas of risk, compliance, management, policy, training, and audit.

Vito Nozza is the Principal Consultant, Cybersecurity Lifecycle Consulting in ConvergeOne’s National Cybersecurity Practice. His career spans 20+ years in Enterprise Architecture, with 15 years specific to Cybersecurity. He has held roles as a CTO, Director, Principal Architect, and Global Security Advisor, which have all led to establishing guidance and consultative measures to SME and Enterprise-grade entities. Vito has been paramount in establishing cloud security, guided frameworks, and disaster/incident response plans, with overall GRC and ERM goals.

About ConvergeOne

Founded in 1993, ConvergeOne is a leading global IT service provider of collaboration and digital infrastructure solutions. Thousands of enterprise and mid-market customers trust ConvergeOne with customer experience, cybersecurity, data center, enterprise networking, and unified communications solutions to achieve business outcomes. Our investments in cloud infrastructure and managed services provide transformational opportunities for customers to achieve financial and operational benefits with leading technologies. More information is available at convergeone.com.
Is Your Business Prepared to Withstand a Ransomware Attack?

The ConvergeOne Ransomware Readiness Workshop focuses on your organization’s readiness to withstand a ransomware attack. During this workshop, ConvergeOne experts will analyze your environment in areas like user awareness training, network security and segmentation, testing and monitoring, incident response plans, and disaster recovery.

Schedule your complimentary Ransomware Readiness Workshop today.