Critical information you need to help better protect your practice and your clients from one of the most serious threats to our nation.

WRITTEN BY **SHAWN E. TUMA**

Ransomware cyberattacks are the greatest existential threat that organizations in the United States face today. These organizations include your law practice as well as your clients—the two most important things to your own livelihood. This is serious. Ransomware literally shuts down operations within moments of the attack—often overnight.

This threat is so serious that in June 2021, the U.S. Department of Justice, or DOJ, announced that it will be treating ransomware with the same level of priority that it treats terrorism[1] and the White House issued a memo to all corporate executives and business leaders with the subject "What We Urge You To Do To Protect Against The Threat of Ransomware."[2] This is the first time such a memo has ever been issued. That is how serious the threat of ransomware attacks is to our nation.

In this article I summarize information from the DOJ;[3] U.S. Cybersecurity & Infrastructure Security Agency, or CISA;[4] Coveware;[5] SpearTip;[6] Tetra Defense;[7] and my own experience leading numerous organizations through the ransomware recovery and response process. Coveware, SpearTip, and Tetra Defense are three of the trusted cybersecurity vendors our firm's cyber incident response team uses for gathering intelligence about and negotiating with ransomware threat actors, recovering from ransomware attacks, and protecting against future attacks. Due to space limitations, I only hit the high points and do so without direct citation to the sources, but I strongly encourage you to analyze each of the sources referenced.

What is ransomware?

Ransomware is malicious software, or malware, that threat actors use to encrypt your data and deny you access to it until a ransom is paid. With ransomware, the threat actors do not care how intrinsically valuable your data may be—they know that it is valuable to you and if they can keep you from having the ability to use it, you will pay to get it back. The best way to circumvent a successful ransomware attack is to have viable backups of your data that can be restored quickly. Threat actors know this so, when they gain access to your environment, one of the first things they will do is search for your backups and either encrypt them or forensically delete them so they cannot be recovered.

While threat actors initially used encryption for leverage, they have evolved in their tactics. In many cases today, the threat actors will not only encrypt your data, but also steal your data and use a second level of extortion by threatening to publish the data if the ransom is not paid.

Who is at risk from an attack?

Every type of organization with a computer connected to the internet is at risk. This ranges from global enterprises down to small "mom and pop" shops, in every type of industry and of every level of sophistication. Coveware's latest study notes that *the most notable change observed in Q1 of 2021 was an increase in attacks on the professional services industry, specifically law firms.*

What is the impact on your organization if you get hit?

The consequences of a successful ransomware attack on important systems in your organization are that you immediately lose access to those systems and whatever operations they control are shut down. This often means a complete shutdown of your organization. In some cases, these interruptions are overcome quickly, such as when an organization has viable backups of its data that can be restored. When your organization does not have viable backups, you face being shut down for days, weeks, or maybe forever. The encryption used in ransomware attacks cannot be broken and, when your organization does not have viable backups of your data, you are faced with a Hobson's choice of only two options of negotiating with and paying the threat actor for the decryption keys or not recovering your data and not restoring your operations.

How much are organizations having to pay in ransom payments?

In Q1 of 2021, the average ransom payment alone was $220,298 and the median payment was $78,398. In addition to the payment, your organization will face other losses such as the lost profits from a business interruption, reputational harm, costs associated with negotiating, remediating, and investigating the attack. Then come the costs of complying with legal and regulatory obligations that may be triggered by such attacks, which include notifying individuals and reporting to regulators. If you find yourself in this situation you had better have cyber insurance that will cover these losses.

What are the most common methods the threat actors use to carry out these attacks?

The most common attack vectors that threat actors are consistently using are remote desktop protocol, or RDP, compromise, email phishing, and unpatched software vulnerabilities. Having vulnerable services and systems that face the public internet are among the most common ways threat actors can gain a foothold in your network. In most cases they are not looking for your organization in particular—they use scanning tools that can find any computer in a certain area that has a vulnerability that they know how to exploit. Once they find these computers, they begin exploiting the vulnerabilities and gaining access to the networks. Only then will they discover whose network they have compromised.

How can your organization better protect itself?

In order to better protect your organization, you should focus on addressing at least the following issues, which are by no means exhaustive, but are a good place to begin:

- Perform a risk analysis to better understand your organization's greatest risks—you cannot mitigate what you do not know exists.
- Backup your data, system images, and configurations, regularly test them, and keep at least one copy of the backups offline. Consider the "3-2-1 backup rule."
- Encrypt all sensitive data to ensure that if it is stolen, its confidentiality is not compromised.
- Update and patch your systems promptly, especially external-facing systems. Configure automatic updates on workstations and laptops where feasible.
- Require multi-factor authentication, or MFA, for every login for something important, especially external-facing systems and services. MFA is using two steps to log in instead of just one.
- Require cybersecurity and phishing training and exercises for all members of your organization, especially senior leadership.
- De-escalate privilege to the minimum necessary on user accounts, especially for high-value target users such as executives, accounting, and human resources and for vendor access.
- Use a reputable firewall that is configured to block access to known malicious IP addresses.
- Use a reputable endpoint detection and response, or EDR, solution.
- Identify external-facing systems by looking up IP addresses and DNS subdomains for your organization.
- Block public access to the services RDP, Secure Shell, Telnet, and file transfer protocol, or FTP.
- Perform vulnerability scans against external-facing systems.
- Have a security team and check their work.
- Have an incident response plan and business continuity plan and regularly exercise both.
- Segment your networks.
- Choose third-party service providers that are dependable and secure. **TBJ**

NOTES

[1] *See* Christopher Bing, *U.S. to give ransomware hacks similar priority as terrorism*, Reuters (June 3, 2021 6:50 PM), https://www.reuters.com/technology/exclusive-us-give-ransomware-hacks-similar-priority-terrorism-official-says-2021-06-03/.

[2] *See* Shawn E. Tuma, *Five Best Practices the White House Urges all Businesses to Take to Mitigate Risk of Ransomware Attacks*, Spencer Fane (June 3, 2021), https://www.spencerfane.com/publication/five-best-practices-the-white-house-urges-all-businesses-to-take-to-mitigate-risk-of-ransomware-attacks/.

[3] RANSOMWARE: What It Is and What To Do About It, U.S. Dept. of Justice, https://www.justice.gov/criminal-ccips/file/872766/download.

[4] Ransomware Guidance and Resources, Cybersecurity & Infrastructure Security Agency, https://www.cisa.gov/ransomware.

[5] Ransomware Attack Vectors Shift as New Software Vulnerability Exploits Abound, Coveware, https://www.coveware.com/blog/ransomware-attack-vectors-shift-as-new-software-vulnerability-exploits-abound.

[6] Caleb Boma, *Ransomware You Probably Didn't Know About*, SpearTip (June 12, 2020), https://www.speartip.com/resources/a-ransomware-you-probably-didnt-know-about/.

[7] *RST: Why We Made It and How You Can Use It*, Tetra Defense, https://www.tetradefense.com/cyber-risk-management/rst-why-we-made-it-and-how-you-can-use-it/.

SHAWN E. TUMA
is an attorney widely recognized in data privacy and cybersecurity law, areas in which he has practiced for over two decades. He is immediate past chair of the State Bar of Texas Computer & Technology Section and co-chair of the Data Privacy and Cybersecurity Practice Group at Spencer Fane, where he works primarily in the firm's Collin County office.