# Ransomware Today: Top Tips for Law Firms

by Sharon D. Nelson, Esq., John W. Simek and Michael C. Maschke


**Ransomware Today**

Ransomware has been a curse for quite a while. Law firms are one-stop shopping for cybercriminals, alluring because they hold the data of many people and businesses.

More than 80% of attacks today exfiltrate or take your data. That means you have a data breach – and potentially a number of legally required notifications. Attackers will try for two ransoms, one for the decryption key to restore your data and – if you've been lucky enough to be able to restore your data with known good backups that are NOT connected to your network, the cybercriminals will still demand a hefty ransom to keep them from selling or leaking your data. They'll put pressure on you by calling the media or they will call your clients themselves to let them know that their data will be leaked or sold if a ransom is not paid.

The average ransom paid at the beginning of 2021 was $118,000 – by the end of the year, it rose to $322,000.

Ransomware now comprises more than 75% of cyberinsurance claims. Which is why you are paying more (30-40% more) for your premiums and getting less (as coverage exclusions proliferate). One increasingly common provision excludes attacks by nation-states. Often, it is unknown who the attacker is – and who is going to prove whether the attack was a nation-state attack? We are already envisioning the court battles.

Humans are a factor in these attacks more than 80% of the time - whether by clicking on a link, failing to abide by policies, using poor passwords, etc. We've even seen insiders selling out their employers for a portion of the ransom. Don't ever assume that insiders, especially disgruntled insiders, can't be a threat.

Remediation costs 10 times more than the ransom paid on average. This is one reason why some victims and their insurers may want to pay the ransom. They are counting on a good outcome, which is not always wise. If the cybercriminals retain your data, they may demand another ransom. And if you paid for a decryption key, it rarely works for 100% of your data.

By the end of 2021, the military - as well as both Microsoft and Google - announced that they had joined the fight. The military said they would impose costs on the ransomware gangs, though understandably declined to reveal the specifics.

Corporations are going to court to seize control of malicious websites. Our government is arresting gang members and offering millions of dollars for the identification of major ransomware players.

Russia itself shut down REvil, one of the most notorious Russian ransomware gangs in January 2022, based on information provided by the U.S. In retrospect, who knows why? Were they

placating us in advance before the war on Ukraine? Who knows? Their cooperation here remains a mystery to us.

**Our top tips for combatting ransomware:**

1. Use multi-factor authentication
2. Upgrade your router and firewall to include Intrusion Detection and Intrusion Prevention functionality
3. Keep software updated and patched
4. Use strong, complex passwords and a password management tool
5. Install Endpoint Detection and Response (EDR) software on all endpoints
6. Require annual mandatory cybersecurity awareness training for all personnel
7. Utilize a cloud backup provider to help protect your data from ransomware
8. Implement phishing testing for all employees
9. Utilize WPA2 or WPA3 to encrypt all wireless networks
10. Disable all unneeded network services
11. Change all factory default settings
12. Implement inactivity timers for all devices
13. Maximize log collection and retention
14. Begin implementing Zero Trust architecture

Could we go on and on with tips? Yup, but then your heads would hurt. Enough for now. Get these 14 things done and you're way ahead of most of your colleagues.

***Sharon D. Nelson*** *is a practicing attorney and the president of Sensei Enterprises, Inc. She is a past president of the Virginia State Bar, the Fairfax Bar Association, and the Fairfax Law Foundation. She is a co-author of 18 books published by the ABA.* *snelson@senseient.com*

***John W. Simek*** *is vice president of Sensei Enterprises, Inc. He is a Certified Information Systems Security Professional, Certified Ethical Hacker, and a nationally known expert in the area of digital forensics. He and Sharon provide legal technology, cybersecurity, and digital forensics services from their Fairfax, Virginia firm.* *jsimek@senseient.com*.

***Michael C. Maschke*** *is the CEO/Director of Cybersecurity of Sensei Enterprises, Inc. He is an EnCase Certified Examiner, a Certified Computer Examiner (CCE #744), a Certified Ethical Hacker, and an AccessData Certified Examiner. He is also a Certified Information Systems Security Professional.* *mmaschke@senseient.com*.