What's White-Hot in Cybersecurity Today?

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

"What are you seeing in light of Russia's attack on Ukraine?"

That's the question we are most frequently asked these days by lawyers and by reporters. There was considerable worry when the attack began on February 24, 2022.

The Cybersecurity & Infrastructure Security Agency (CISA) immediately made it clear that all U.S. organizations should have their "Shields Up" considering possible threats. CISA is our favorite "go-to cybersecurity resource" for lawyers and its "Shields Up" website is chock full of useful information that is straightforward and written to be understood by the general public – which most government cybersecurity resources are not.

And unlike cybersecurity vendors, the information is public – you don't need to give them your name, email, and telephone number. Often the "white papers" and other offerings from the cybersecurity vendors are not terribly useful, except they now have your contact information so they can pester you by phone and email.

Though we agreed with CISA's readiness alert, we have not seen the expected impact on the U.S. from the Ukraine War – attacks have actually lessened. More than 80% of cyberattacks as of March 20 were directed at Russia or Ukraine. That could change in a heartbeat of course.

There is an army of hackers attacking Russia, more than 130,000 thus far and many Russian government websites have been taken down or badly crippled. Anonymous, one of the best-known hacker groups, has literally declared war on Russia.

Multi-factor authentication is increasingly critical.

At this point, we believe that the use of multifactor authentication is ethically required as a reasonable measure to protect client confidential data.

We need to stop complaining about MFA being inconvenient and simply recognize that the short extra steps of MFA keep us far more secure. The vast majority of time, MFA is free, so it is not a budgetary concern. MFA stops more than 99% of account takeover attacks and it doesn't get much better than that.

When you implement MFA, there are essentially four possible methods to provision the additional factor. The methods discussed are identified from the least to the most secure. The most common method is to receive a code via SMS text message. This is the most insecure of the MFA methods and is subject to a SIM swap attack. Even though text messages are the least secure, it is still a LOT more secure than not using MFA at all. Forget about receiving the MFA code to your email, which is totally worthless in protecting your email account.

The next method of getting the MFA code is to use an authentication app such as Google Authenticator, Authy, Duo, Microsoft Authenticator, etc. The authentication app will generate a code that changes every 30 seconds. Just enter the code when prompted. This method is more secure than a text message.

The next method is push notifications within an authentication app. Instead of typing in a code retrieved from a text message or generated in the app, a notification is "pushed" to your authenticator app requesting approval. All you do is accept or reject the access. No typing of a code is required.

The most secure method is to use a physical token such as a Yubikey, Titan Security Key, etc. Nothing to type, just connect the key to your device.

When configuring MFA, choose the most secure method available. As an example, if SMS and authenticator app are options, select the authenticator app.

Endpoint Detection and Response (EDR) is the next generation of security software.

EDR is different from your typical anti-virus/security software and is much more sophisticated. EDR uses artificial intelligence, heuristics, machine learning, etc. to establish a baseline for normal device operation. Should there be some activity that is suspicious and not normal, some sort of action will be invoked.

This action could include quarantining the files, blocking the task or service, or even automatically removing the device from the network. Some EDR solutions integrate with a SOC (Security Operations Center) to add a human element to the analysis and verification of the action taken. There is also the ability to roll back a device to a known good state.

EDR scales from the solo attorney all the way to large enterprises. There are very affordable solutions for solo and small firm attorneys. We now believe that EDR is ethically required as a reasonable measure for protecting client confidential data. EDR is an excellent alternative as a defense for ransomware. Should some abnormal activity be detected (e.g. file encryption process), the process can be terminated and the system restored to a state prior to the attack.

Zero Trust is a term law firms need to be familiar with. The term Zero Trust has been around for some time but is getting more attention and focus as law firms and businesses migrate to a more hybrid type of work environment and usage of cloud services is increasing. The perimeter security model does not work today and will be replaced with Zero Trust network architecture. Zero Trust is not a product you can buy off the shelf. Its complexity often baffles lawyers.

Basically, Zero Trust means just that. Do not trust any device, person, or access and verify everything. In other words, trust nothing and constantly verify, even if access was previously authorized. Zero Trust gives new meaning to Ronald Reagan's words, "Trust, but verify." Our government is requiring that Zero Trust be implemented by government agencies by the end of

2024. Businesses will certainly follow this lead. Many larger law firms are well on their way to establishing a Zero Trust environment.

All law firms should learn about Zero Trust, budget for it, and begin to take steps to implement it. Those pesky ethics rules demand that you take reasonable steps to be competent with legal technology and that you take reasonable steps to secure your clients' confidential data. There's no avoiding Zero Trust – so start your self-education now!

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 (CISSP), Certified Ethical Hacker (CEH) 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 and Digital Forensics 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*.