# The New Frontiers of Cybersecurity During Natural Disasters (Including Pandemics!)

by Sharon D. Nelson, Esq. and John W. Simek



## The Times – They are A-Changing

Wise words from Bob Dylan. Natural disasters are steadily increasing. In 2020 we ran out of hurricane names and had to resort to the backup names from the Greek alphabet. We came close to using up all the names in 2021 too, but barely squeaked by with one remaining. December 2021 saw a wind disaster come through the central United States and devastate hundreds of miles of structures. According to meteorologists, at least 19 tornadoes in five states were unleased. We have experienced major flooding from hurricanes over the last couple of decades, severely impacting attorneys in their ability to practice law.

Whether there is a natural disaster involving tornadoes, ice storms, hurricanes, blizzards, etc., the primary concern is to protect the confidential information entrusted to attorneys by clients. Physical access to law offices and client data is hindered during a disaster.

How will you prevent someone from potentially gaining unauthorized access to client data during the disaster? Your security system may be disabled due to lack of electricity. You won't be able to control physical access if your office space is damaged. You may not be able to get to the client data (paper files, computers, servers, etc.) if your office is flooded - remember Katrina?

## The Cloud Becomes a Lifeline

As more and more law firms utilize cloud services (and law firms stampeded to the cloud in 2020) continuing operations during and after a disaster is becoming much easier. However, taking advantage of cloud services means that a connection to the internet is of prime importance. If your internet connection goes down, you'll need an alternative method to get to your client data.

Don't forget that you may be able to use your smartphone hot spot to access the internet and continue operations during a disaster. Another advantage of using the cloud is security. Generally, cloud providers are much more secure than

systems contained in a law firm's network. That is true for most solo and small firm attorneys.

### The Pandemic Revolutionizes Cybersecurity

We've mentioned some of the more common natural disasters, but the pandemic rocked us to the core. COVID-19 forced law firms and businesses to close up shop (most in a single day) and send employees home for an extended period.

The sudden closure of law firms allowed for only scant planning. We shut down our own office in less than an hour, although we were fortunately well situated for a work-from-home (WFH) environment.

A lot of law firms were not as fortunate. Those that didn't have laptops as a primary work device for their employees were forced to use home computers for work purposes as laptop demand skyrocketed and lead times for orders took months for delivery. The pandemic significantly slowed laptop production, which didn't help. Even though the pandemic forced WFH on many law firms, other natural disasters could also force law firm employees into a remote work environment.

### Work From Home is Less Secure

Home networks are 3.5 times more vulnerable to attack than law firm networks for a variety of reasons. Consumer grade equipment is used in home networks and not generally kept up to date. That includes computers as well as networking equipment such as wireless routers. Surveys show that less than 30% of users have changed the default administration password on their home routers. The cybercriminals read these the studies too! That is one reason the attacks on home networks increased significantly at the beginning of the pandemic. Cybercriminals knew that lawyers were now working from home utilizing insecure devices. A ripe target indeed!

Another consideration in a WFH world is the security of the device used to connect to the law firm network or cloud service. Devices located within a law firm network are typically centrally managed and kept up to date with the latest security patches and application updates. There are many more challenges when someone is remote, especially if working on a non-firm owned device.

To help improve the situation, some firms elected to make the home machines part of the law firm's centrally managed environment. This means that the firm would remotely patch the home computers and make sure all security configurations and updates were installed.

Obviously, there are some challenges when folding a home machine into the managed environment. Privacy considerations become top of mind. Not just the privacy (and security) of client information, but the personal privacy of the home user. There needs to be a crystal-clear understanding of what the law firm is allowed to do to the home user's computer and what information may be accessed. The obvious conclusion is that it would be a much better alternative to put a law firm owned device on the home network rather than taking control of a home machine.

### Training is critical!

Training is essential to adequately responding to a disaster. No matter what the disaster (e.g. tornado, hurricane, pandemic, etc.), employees are stressed out dealing with the situation. They may be concerned for the life and safety of family, friends, and colleagues. Their defenses are down - they may be moving way too fast and not thinking clearly.

Then they must deal with cybercriminals seeking to exploit a disaster. Training needs to be done for employees to properly recognize a phishing attack, especially since over 90% of successful cyberattacks start with a phishing email. Unfortunately, the cybercriminals have become very sophisticated and are constantly changing their methods and tactics to gain access to valuable information. That information may be the user's login credentials, firm financial information, or client information that ultimately results in financial gain.

Phishing attacks have drastically increased since the beginning of the pandemic. Besides trying to get users to click on an attachment or open a malicious link, cybercriminals want to let users feel safe when receiving a phishing email. There may not be any link or attachment with the attacker simply starting a conversation e.g., "Are you available to talk?" After a few "innocent" email exchanges, the attacker then "pulls the trigger" and gets to the real purpose of the email exchange. These attacks are primarily financially driven. The FBI categorizes these events as BEC (Business Email Compromise).

BEC accounts for the majority of internet fraud according to the Internet Crime Complaint Center's (IC3) *2020 Internet Crime Report*. The report identified total losses exceeding $4.2 billion dollars, with BEC being responsible for over $1.8 billion. In comparison, ransomware was only responsible for $29.1 million of losses. Some of the Q2 2021 stats show that the average request was for $106K, up from Q4 2020 for $75K.

24% of the BEC attacks tried to divert employee payroll deposits while 47% requested funds in gift cards. Gift cards are popular since you only need the codes and not the physical card. Once the card is cashed in, the funds are converted to virtual currency such as Bitcoin. You will probably never see the money again once the gift card is redeemed. A request for gift cards is usually a "red flag." Instruct employees to be very wary of ANY request for gift cards.

### Clever Subject Lines in Phishing Emails

Cybercriminals never miss an opportunity and quickly create campaigns to take advantage of recent disasters. We saw upticks in phishing attacks during Katrina, when a Malaysian airliner went missing and again during the pandemic.

The subject lines for phishing emails try to entice you to engage with the attacker by using relevant topics, often indicating urgency. In its State of the Phish 2021 report, security firm Proofpoint identified the top ten themes used for phishing campaigns.

1. New Microsoft Teams request
2. Coronavirus advisory alert and health warning
3. Office 365 password expiration notice
4. Deactivation of old OneDrive account
5. OneDrive shared contract notification
6. Starbucks bonus
7. World Health Organization coronavirus safety information
8. New voicemail message alert
9. Alert about large number of files deleted from OneDrive
10. UPS shipping notice

Notice that these are all very current and relate to the current world situation with the possible exception of Starbucks.

## What Must Lawyers Do to Ethically Protect Confidential Data?

As attacks increase, lawyers need to be diligent in protecting access to client confidential data. This means having more stringent methods and policies to protect access credentials. Having weak passwords or reusing passwords is not an acceptable practice to protect client data. Using a password manager will help organize your logon credentials utilizing strong, unique passwords for each service.

Besides improving your password hygiene, you should be using two-factor authentication (2FA) wherever it is available. Should your password get compromised, 2FA will help prevent a successful takeover of your account. Note: 2FA is a subset of the more general multi-factor authentication (MFA). In studying the effectiveness of MFA, Microsoft has reported that utilizing MFA stops 99.9% of credential-based account takeover attacks.

One of the best features of MFA is the cost. Most MFA implementations are free. We have come to learn that FREE is a favorite word, especially among solo and small firm attorneys. Some vendors are now requiring that 2FA/MFA be enabled for all accounts. Google enforces 2FA for its accounts and your Ring doorbell account must have it configured too. Some commentators say that it is now ethically required to use MFA because it is a “reasonable” way to safeguard client data.

When configuring MFA, you may have some options for obtaining the second factor. It is very common to obtain the code via SMS text message. SMS text message are the least secure of all the methods. Having said that, getting the code via text message is **far better** than not having 2FA configured at all. If you have the choice, retrieving the code from an authentication app such as Google Authenticator, Authy, Duo, Microsoft Authenticator, etc. is better than getting a text message. Push notifications via an authenticator app are even more secure and using a hardware token such as the YubiKey is the most secure. Time to educate yourself on your MFA options!

## Encryption is Vital!

The ability to utilize encryption is another essential tool for attorneys. Attorneys need to protect the confidential client data while it is at rest and while in transit. Having the ability to communicate with encrypted email keeps the information

private. Many attorneys are now using cloud-based practice management systems that include client portals for securely communicating with their clients.

The pandemic has forced video conferencing upon us – and it will undoubtedly remain with us as so many law firms are hybrid. Attorneys need to know how to secure these video conferencing sessions. Zoom now has end-to-end encryption, but it is not turned on by default. Currently, Teams has limited end-to-end encryption ability. End-to-end encryption means that only the participants have control over the encryption keys and it is really only needed for the most secure of communications. Normal encryption methods are generally sufficient to secure client data while using third party services.

## The Curse of Ransomware

In case you are thinking that your practice is not important enough to be the victim of a ransomware attack, think again. Cybercriminals take advantage of disasters by adding to your misery. Think of it as a dual attack. While you are busy dealing with your disaster, cybercriminals attack as your defenses are down. Even during non-disaster periods, your environment should be prepared for a ransomware attack. In addition to your anti-virus security solution, you should investigate installing a relatively new form of security software called Endpoint Detection and Response (EDR). EDR is much more sophisticated and uses AI, machine learning, heuristics, etc. to help combat ransomware and other more sophisticated attacks. There are some EDR solutions that are very affordable even for the solo and small firm attorney.

Finally, make sure you have an Incident Response Plan (IRP) to address the various situations involving a disaster. As an example, what will you do if your office is flooded during a hurricane? How will you communicate with your employees? Can you still get to your files and access whatever you need to provide adequate representation for your client? How will you continue to practice law if there is a lockdown as we experienced at the beginning of the pandemic? Your IRP also needs to address what you will do in the event of a ransomware attack. Who are you going to call and in what order? Do you pay the ransom? Can you restore from backup? Have you tested your backups? Do you have multiple backups?

## "Too Cool for School"

Some of you will remember those words from childhood. Be wary that you never think like that when it comes to staying abreast of cybersecurity. The article you've just read could easily have been a book. And what law firms should be doing with respect to cybersecurity will change by the hour and day for the foreseeable future.

Seek out cybersecurity articles, training and CLEs to keep yourself technologically competent in a complex and potentially deadly world that moves faster than the speed of light.

*Sharon D. Nelson, Esq. 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 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.*