The Craziest Cybersecurity Stories of 2020

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

Heaven help us – with that title, we hardly know where to start.

OK, we'll just quote a headline from Vice: "*New Yorker Suspends Jeffrey Toobin for Masturbating on Zoom Call*." You can't make it up, right? Somehow a highly respected New Yorker reporter, during a call between several New Yorker reporters and a radio station, didn't realize his video was on while he was touching himself.

He was not alone in Zoom stupidity. A Florida court was zoom-bombed in August by pornography when someone changed the secure Zoom defaults and allowed screen sharing, allowed participants to unmute themselves and completed the fiasco by posting the hearing link publicly at the Florida state attorney's office website complete with time and ID number. That's a trifecta of stupidity. So the court hearing for 17-year-old Graham Clark of Tampa, Florida (the alleged mastermind of the July 15 hack against Twitter which resulted in a bitcoin scam after the accounts of high-profile Twitter users were compromised) was terminated swiftly after someone injected a pornographic video clip into the proceeding.

No matter how well Zoom secures its platform, if you mess with the secure default settings, you are setting yourself up for disaster.

A law firm in Oklahoma learned the same lesson in May 2020. On August 14, Oklahoma's NBC 4 reported that an Oklahoma City law firm (not named) set up a Q&A session in May which was open to the public.

Someone named "Christine" joined the meeting and began showing a graphic video of a man sexually assaulting a child. Not something a law firm needs.

The meeting was brought to a quick close, followed by an investigation by both the Oklahoma City police and Zoom. User error again.

While we could recount Zoom stories forever, the BIG story of the year for the legal world was ransomware. Law firms, bar associations, and all manner of other organizations were hard hit as ransomware surged by 715% in the first half of

2020. 27% of victims are now paying the ransoms, especially when the cybercriminals have stolen law firm data before they encrypted it. This gives the option, if you can restore your data from your own good backups, for them to demand a ransom for destroying your data rather than publishing it.

The authors had all but begged our clients to allow us to put endpoint protection on their networks. But three law firm clients did not and were subsequently struck by ransomware. To the credit of all three, these clients were quick to blame themselves for not listening to our entreaties. Happily, they all had backup protection solutions and we they were up and running in less than a day without having to pay the ransom. They all signed up for endpoint protection subsequently. A hard-earned lesson.

But if you want the craziest story of the year, we were called in by a firm (not previously a client) that had been struck by ransomware and was completely out of business with NO USEABLE backup. All of the backups (local and remote) were deleted without the possibility of recovery. There were no multiple cloud backups impervious to ransomware, which is incredible these days.

The requested ransom was $250,000. We spent a pleasant Sunday afternoon with Homeland Security as we both realized we were dealing with a network that was completely and utterly screwed. Homeland Security understood the severity of the situation and did not object to paying the ransom. A ransomware negotiator (can you believe there are companies which specialize in this now?) was brought in and got the ransom down to $100,000, which the (now) client paid.

Even with the decryption key and multiple employees deployed to recover the data, it took a week to get them fully operational. Then we had to do a security assessment of the network because clearly their security posture was worse than anything we had ever seen, especially in a large organization. Here's some of what we found:

1. As mentioned above, the backups were not properly engineered.
2. More than 100 users were using two to four-character passwords to access the network.
3. 100-150 users were sharing the same password.

4. There was no enforcement of password requirements and changing passwords periodically. It was ok for users to have their username and password be the same.
5. There was no network diagram or documentation.
6. Lots of software was out-of-support and receiving no security patches.
7. Logging was not enabled which complicated the investigation of the data breach.
8. The onsite IT staff had a "no patch" policy. This is lunacy in the extreme. The staff member advised us that "patches break things" so he didn't believe in them. Oy. For those that may not know, there are managed services that test patches before they are deployed. The updates are blacklisted if problems are discovered. Updates that pass testing are automatically deployed to managed devices.

Switching gears, on November 4, it was reported that law firm Cole Schotz had obtained a restraining order against a former associate who allegedly used social media to disseminate confidential documents belonging to the firm and its clients.

Myles MacDonald, a former bankruptcy associate in the firm's Wilmington, Delaware office, appears to be a disgruntled ex-employee. He resigned from the firm in 2019, but at some point began releasing law firm files trying to damage "BigLaw" against which he had some sort of grudge.

Lesson? Get data loss prevention software – and don't forget to have an employee out-processing list. We've also seen intrusions from former employees whose access to the law firm network wasn't terminated when they left or were fired.

For those that may not know, ABA formal opinion 483 requires that lawyers monitor for breaches of confidential client data, stop the breach and notify the impacted clients. Now would be a good time to confirm that logging is enabled as a minimum and perhaps implement some sort of IDS/IPS (Intrusion Detection System/Intrusion Prevention System).

One last nutty scenario that could have been easily stopped: We have seen an increasing number of business email compromises. In our home state of Virginia,

we have seen a number of prominent lawyers whose email accounts have been compromised. We know this because author Nelson is a former VSB President, so she has been getting the phishing emails "from her friends" resulting from the compromises.

Remember, once they compromise your email, they have all your contacts, all your email, calendar entries etc. There is nothing you can do about that once it has happened. You can only prevent it in the future (and why weren't you doing this before?) by implementing multi-factor authentication, which stops 99.9% of account takeovers. If you have been a victim of this kind of compromise, make sure that the cybercriminal hasn't mucked with your email rules – for instance, by auto-forwarding all subsequent emails to their address.

All these nightmares were real. Since we are all living in Crazytown these days, make sure you shore up your defenses, especially in a work-from-home environment.

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 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