# If U.S. Essential Infrastructure is Brought Down, Is Your Law Firm Prepared?

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

© 2022 Sensei Enterprises, Inc.

**Can U.S. Critical Infrastructure Really Be Brought Down?**

That's the preliminary question. At one time, and not so long ago, we were not overly worried about our susceptibility to a major takedown of U.S. essential infrastructure. But those days are gone.

On October 28, the Washington Post reported that the United States is highly vulnerable to foreign cyberattacks designed to damage the economy, and needs to do far more to defend against them. This is the conclusion of a think tank report from the Foundation for Defense of Democracies.

The report concludes that our government has a blind spot when it comes to cyber economic warfare that could "cause a catastrophic strategic surprise" and destabilize U.S. critical infrastructure.

What can we do most effectively? Prepare. And yes, that applies to law firms too.

**Convincing Law Firms of the Problem**

Convincing law firms about the urgency of this problem would take forever because there is so much evidence, but let's focus on a few nuggets from the *Washington Post* article.

Moscow has proven its ability to use its surveillance dragnet to select U.S. targets. It's also proven itself very capable of penetrating U.S. critical infrastructure.

You may recall the SolarWinds 2019 hack by Russia, when attackers penetrated an IT company and broke into the networks of its customers, including nine federal agencies and more than 100 companies. How much better do you think Russian's assault capabilities are now? The betting money is that they are very, very good.

Don't forget about China, which has also proven itself gifted at penetrating U.S. networks. Other, but significantly lesser players, include North Korea and Iran.

Cyberwar may fall just short of armed conflict, but it could be catastrophic in its impact. While it is often said that the U.S. and its allies must prevent their enemies from becoming more and more able to take down critical infrastructure, there is a clear consensus that we and our allies are not at that point now.

**Law Firms Should Hope for the Best but Prepare for the Worst**

So, what constitutes critical infrastructure? The Federal Emergency Management Agency (FEMA) says critical infrastructure includes people, assets, systems, and networks, whether physical or virtual, so vital to the United States that their incapacity or destruction will have a

debilitating impact on security, the nation's economy, public health or safety, or a combination of those things.

The sheer number of disasters is almost unimaginable. But one must begin somewhere. So let's imagine that the power is out, not just locally but throughout the country. There was a time when we believed that scenario was not possible, but we are a lot less certain now.

What if all the major banks and Wall Street are taken down? Or the internet, our water systems, hospitals, defense agencies, the military, the federal government, state governments, transportation, major corporations, hospitals? The list goes on and on.

**Defending Against the Unthinkable for Law Firms**

We are not going to address the issues faced by the Am Law 100. They have millions of dollars to throw at Incident Response Plans (IRPs) and cybersecurity annually. Not so for the solo/small/mid-sized firms. Most of those firms have not yet even addressed hurricanes, tornados, floods, power outages and the like. 60% of law firms lack any IRP according to the American Bar Association's 2021 survey.

In the case of a successful attack on our critical infrastructure, your law firm and your clients may face innumerable difficulties. How will you pay your employees if the banks are taken out? If communications are at issue, how will you communicate with your clients and your employees? If your clients are part of the critical infrastructure of the country, what special problems must you be prepared for? If the internet is down, how will you function?

**Disaster Planning: It's Not Just for Hurricanes**

The header above is the title of a recent Legal Talk Network *Digital Edge* podcast author Nelson and co-host Jim Calloway recorded with Shawn Holahan, Practice Management Counsel and Loss Prevention Counsel for the Louisiana State Bar Association. She lived through losing access to her home and her office during Hurricane Katrina in 2005. So she knows a lot about traditional disasters and has continued to evolve her expertise as our world and its dangers have become more complex.

We suggest listening to the podcast because she includes so many things you will want to include in a law firm incident response plan – and her advice is spot on. But here are some of the chestnuts that particularly appealed to us (because they are so often ignored).

- Every law firm needs a "NO TECH" binder (she offers a list of what should be in the binder).
- Have a money plan – cash is king in emergencies if banks are closed, there is no internet, etc.
- Review your insurance coverage considering some of the possibilities we've listed above and prepare to substantiate your claims.
- Have alternative ways of reaching your employees and clients.

- Contact courts and opposing counsel as needed.
- Digitize and back up all client files – have alternate methods of accessing them.
- Take care of family, employees and clients – in that order.
- Triage issues "like a beast" and prioritize the ones with the biggest impact.
- Get your disaster message out.
- "Stay Zen" – especially when those around you are losing it.
- Remember that that disaster recovery is not a sprint but a marathon.

We would add to the list – do not delay in reviewing/revising your incident response plan. And if you don't have one, hop to it!!!

**Final Words from Benjamin Franklin:**

*"By failing to prepare, you are preparing to fail."*

***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.