Preparing for (and Defending against) a Cyberattack on the Energy Sector

Victoria Sutton, MPA, PhD, JD
Distinguished Horn Professor
Texas Tech University School of Law

The utility and energy sectors of our society have increasingly become the target of cyberattacks. Industrial Controls Systems (ICS) saw a tripling of cyberthreats in 2020.[1] Ransomware and phishing attacks are major threats for 2021 with new variations using deep fakes and disinformation will be continuing threats.[2] Cyberhackers, nation-states, and the amateur to sophisticated hacker are seeking vulnerabilities and susceptibilities that exist due to our innocent past before internet connectivity and the IoT (Internet of things) web of opportunity.

Learning from other Cyberattacks

In 2009, the U.S. Department of Homeland Security disclosed that the electric grid in the U.S. had been infiltrated by Chinese hackers. Not only had they gained access to the electrical grid but they had embedded tools before they left so that the grid could be taken down on a moment's notice. That same year, the Department of Homeland Security began notifying law firms that they were known targets of cyberhackers.

Then in 2010, cyberattacks reached a new level of sophistication, when the Iranian nuclear facility, Natanz was brought to a halt with a malware attack called Stuxnet. The refusal of Iran to cease the development of nuclear weapons left few options to the rest of the global community, suggesting this was a strategic attack. Many believe it was the work of the United States and Israel.

Retaliation was expected.

In 2012, Saudi Aramco was cyberattacked, shutting down operations for several days. Iran was the suspect. No individuals or countries have been identified or charged with a crime for this cyberattack.

Then in 2013, a dam in a small town, just north of New York City, Rye Brook, New York, was infiltrated by a cyberhacker. The intruder attempted to take control of the gates of the dam which controlled flood waters. But for the dam gates being in disrepair, the cyberhacker would have succeeded in opening the gates and potentially causing flooding damage. In one of the first successful investigations, these hackers were

---

[1] Arielle Wardman, *Dragos: ICS security threats grew threefold in 2020*, TECHTARGET: SEARCHSECURITY (Feb. 24, 2021), https://searchsecurity.techtarget.com/news/252496808/Dragos-ICS-security-threats-grew-threefold.

[2] Robert Lemos, *Ransomware, Phishing Will Remain Primary Risks in 2021*, INFORMATECH: DARKREADING (Feb. 25, 2021), https://www.darkreading.com/threat-intelligence/ransomware-phishing-will-remain-primary-risks-in-2021/d/d-id/1340256.

Please cite as: Vickie Sutton, "Preparing for (and Defending against) a Cyberattack on the Energy Sector," *The Legal Framework for Digitization, Technological Innovation, and the Future of Resource and Energy Development* 6-1 (Rocky Mt. Min. L. Fdn. 2021).

identified. They were physically located in Iran, beyond the jurisdiction of the United States. Placing the individuals on the Interpol wanted list, should they decide to travel outside of Iran, was the only legal tool for reaching the perpetrators. Although it is likely this was government authorized and funded, without a clear connection to the government of Iran, the crime was simply one of unauthorized access to a computer under U.S. law. Even under international law and the interpretation of the laws of war, this attack arguably did not rise to the level that would make retaliation legal under international law for the United States.

In 2014, the next creative use of a cyberattack came against a United States company, almost certainly state-sponsored. Sony Entertainment, Inc. experienced literally hundreds of its computers being invaded by a cyberweapon that took control of the operating system and made access to any computer impossible. By the end of March, the company estimated its losses to be $41 million.[3] The motivation was clearly directed toward Sony's imminent release of a political satire movie, "The Interview" which depicted Kim Jon Il in a very negative, yet satirical way. First, there seemed to be an admission from North Korea that they were responsible for the attack, and then this was followed by indignant denial.

Unlike the Rye Brook, New York dam cyberattack, this time there was millions of dollars of damage to a U.S. company on U.S. soil. The cyberhackers were likely in North Korea, out of jurisdictional reach of the U.S. and no admitted or apparent link to the government of North Korea. Without state action, this does not qualify as an act of war or a kinetic attack under the international laws of war. Three North Korean cyberattackers associated with companies that do business with North Korea (which typically means they are owned by the government) were indicted in 2018 and their indictments were unsealed February 17, 2021. The indictment contained dozens of cyberhacking incidents including banks, casinos and cryptocurrency sources. They were simply charged with unauthorized access (computer intrusion) for the Sony incident.[4]

In 2015, the first truly major cyberattack on the United States Office of Personnel Management saw the theft of the most detailed records of background investigations of all federal government employees (SF-86s). It was discovered that the intrusion began in 2013, and continued until 2015 when it was made public and federal employees, former and current, were notified of the breach. It is estimated that this cyberattack cost the United States in crediting monitoring services, alone, $133 million, and the total loss may reach $1 billion. No cyberattackers were identified, and no evidence has been seen of the use of any of the data that was stolen.

---

[3]Peter Elkind, *Sony Pictures: Inside the Hack of the Century*, FORTUNE (June 25, 2015), http://fortune.com/sony-hack-part-1/.

[4] *Three North Korean Military Hackers Indicted in Wide-Ranging Scheme to Commit Cyberattacks and Financial Crimes Across the Globe*, U.S. DEPT. OF JUSTICE (Feb. 17, 2021), https://www.justice.gov/opa/pr/three-north-korean-military-hackers-indicted-wide-ranging-scheme-commit-cyberattacks-and.

It was also revealed in 2015 that white hat cyberattackers from the University of Tulsa had been commissioned by the wind energy companies to do penetration testing on wind turbines to test their security. They were able to develop a proof of concept cyberattack that infected one wind turbine and could spread to others.[5] Five wind energy farms, owned by five different wind energy equipment manufacturers, were successfully penetrated, stopping the blades.[6]

Then in July 2020, very little publicity was given to a mystery fire that occurred at the assembly center for Iran's centrifuges for its nuclear weapons production facility, Natanz,[7] the same nuclear weapons facility that suffered a cyberattack from the Stuxnet malware in 2010. The fire damage was extensive causing a significant setback for the Iranian nuclear weapons program. The Iranian news release on the fire included a threat to any nation, particularly Israel and the United States, if they were involved with the sabotage.[8] It is unclear what triggered the fire.

In December 2020, in what could be determined to be the most damaging cyberattack to date, Solarwinds Corporation, a company providing systems software for governments and companies disclosed in an SEC filing they had not only been compromised, but their software was updated with the malware and distributed to 18,000 of their clients.[9] This new "supply chain" type cyberattack takes advantage of the accessible distribution networks of the target company.

In February 2021, a public drinking water system was attacked using the remote access and sharing software application, Teamviewer, to access the SCADA system and release excessive amounts of sodium hydroxide (common name, lye) into the drinking water distribution system.[10]

---

[5] Andrew Greenberg, *Researchers Found They Could Hack Entire Wind Farms*, Wired (June 28, 2017), https://www.wired.com/story/wind-turbine-hack/. (Three wind turbine hacking tools were developed in their proof-of-concept penetration exercise: "(1) Windshark, simply sent commands to other turbines on the network, disabling them or repeatedly slamming on their brakes to cause wear and damage; (2) Windworm, another piece of malicious software, went further: It used telnet and FTP to spread from one programmable automation controller to another, until it infected all of a wind farm's computers; and (3) Windpoison, used a trick called ARP cache poisoning, which exploits how control systems locate and identify components on a network. Windpoison spoofed those addresses to insert itself as a man-in-the-middle in the operators' communications with the turbines. That would allow hackers to falsify the signals being sent back from the turbines, hiding disruptive attacks from the operators' systems.")

[6] *Id.*

[7] Michael Lipin & Farhad Poulad, *Setback for Iran's Nuclear Program after Mystery Fire at Centrifuge Assembly Site*, HOMELAND SEC. NEWS WIRE (July 3, 2020), http://www.homelandsecuritynewswire.com/dr20200703-setback-for-iran-s-nuclear-program-after-mystery-fire-at-centrifuge-assembly-site.

[8]

[9] Solarwinds Corporation, Current Report (Form 8-K) (Dec. 14, 2020), http://d18rn0p25nwr6d.cloudfront.net/CIK-0001739942/57108215-4458-4dd8-a5bf-55bd5e34d451.pdf.

[10] CYBERSECURITY AND INFRASTRUCTURE SEC. AGENCY, A21-042A, COMPROMISE OF U.S. WATER SUPPLY (2021), https://www.mass.gov/doc/joint-fbi-cisa-cybersecurity-advisory-on-compromise-of-water-treatment-facility/download.

> All computers used by water plant personnel were connected to the SCADA system and used the 32-bit version of the Windows 7 operating system . . . Further all computers shared the same password for remote access and appeared to be connected directly to the Internet without any type of firewall protection installed.[11]

Most troubling is an escalation that was announced in March 2021, with an announcement by the Biden Administration that they were planning to retaliate against Russia, the nation believed to be behind recent cyberattacks against the United States,[12] Solarwinds. Although China is responsible for far more cyberattacks and Russia is a distant second, and one of the two major, recent attacks was attributed to China, the Biden Administration has only announced retaliation against Russia through Jake Sullivan, spokesperson for the U.S. Department of State.

In 2009, the FBI notified law firms that hackers were targeting U.S. law firms to steal confidential information. Types of attacks against firms, have included phishing. Phishing attacks account for more than 80% of reported security incidents.[13] Zero-day exploits, Trojan horse viruses; DDOS attacks. In September 2010, a DDOS attack was used which resulted in crashing the law firm website and making visible the firm's unencrypted emails.

Firms are also vulnerable through unsecure devices. Unsecured laptops or stolen laptops are sources of vulnerability. The practice of buying your own device (BYOD) creates vulnerabilities beyond the control of the firm. Although this is attractive for bringing down firm costs, not using encryption further puts the firm at risk. Mobile device management systems can be used to shut down all mobile devices in the face of a cyberthreat. Further, all mobile devices should use encryption.

Legal Preparation for Cyberattacks[14]

Defending against cyberattacks is always much harder than doing the hacking. It is often said that in cyberdefense you have to succeed thousands of times, but a hacker only has to succeed once. The practice of law is now handling big data. Firms operate data centers and have global networks of computers. This interconnectivity also connects with financial resources of all parties.

Firms also do legal process outsource (LPO) for many aspects of work that were previously done in-house. For example, litigation support and legal research are often outsourced. Even due diligence and may be outsourced depending on the need. Firms

---

[11] *Id.*

[12] *U.S. Set to Retaliate against Russia, China for Massive Cyber Attacks*, HOMELAND SEC. NEWS WIRE (March 12, 2021), http://www.homelandsecuritynewswire.com/dr20210312-u-s-set-to-retaliate-against-russia-china-for-massive-cyber-attacks.

[13] Josh Fruhlinger, *Top cybersecurity facts, figures, and statistics*, IDG COMMS.: CSO (Mar. 9, 2020), https://www.csoonline.com/article/3153707/top-cybersecurity-facts-figures-and-statistics.html.

[14] JILL S. RHODES AND ROBERT S. LITT, THE ABA CYBERSECURITY HANDBOOK, 45 (2018).

may have given up their law libraries for digital resources, which means law libraries and research from them is often all outside the firm.

Legal ethics

Model Ethics adopted in 2012, updated by an ABA 20/20 Commission charged with looking at ethics in the context of new technologies, explicitly require lawyers to provide "competent representation" by keeping "abreast of changes in law and its practice, including the benefits and risks associated with relevant technology . . ." (Rule 1.1).

Further to protect the confidentiality of information, a lawyer shall make "reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client. (Rule 1.6). This is more than a one-time course, and requires the institutionalization of processes to continuously monitor and to encourage hypervigilance. This could lead to more serious issues of breaches in client confidentiality and breach of the fiduciary duty to clients.[15]

Responsibilities to Protect Sensitive and Confidential Data[16]

Just as law firms must safeguard their own information: business records, intellectual property, lawyer work product, financial and employment records; they must also safeguard client records. These might include: attorney-client privileged information, trade secrets, personally identifiable information (PII), such as health care, financial and law enforcement records. It is also important to consider non-clients and e-records that might be included in vast amounts of information from clients.

It is recommended that law firms understand the scope of data that they are obligated to keep secure. In order for firms to accomplish this and protect confidential information law firms must have an inventory of what kinds of data they have, where it is stored. "Where" might include not only devices but backups and cloud storage accounts. Then, it is imperative to know the level of sensitivity for these data. Finally, law firms need to know how each of these categories of data is being secured.

Until a law office has conducted a risk assessment and adopted a comprehensive information security program, it will not be in a position to vouch for an appropriate level of security and its ability to protect sensitive and confidential data and information if requested by a client or the Court.

What is "Data Security"?[17]

Data security is a process: "A risk management process that security professionals undertake when protecting information and information systems." This

[15] *Id.* at 126.
[16] *Id.* at 65–92.
[17] *Id.* at 61.

process should include these three elements: confidentiality; integrity; and, availability.[18]

Confidentiality. Is the protection of information against unauthorized disclosure, whether intentional or accidental? Integrity is the protection of information against corruption, tampering or other alteration; this capability includes safeguarding the accuracy and completeness of information. Availability is ensuring that information and systems can be reliability and promptly accessed and used when they are needed.

This definition comes from NIST, the agency that has been charged with providing advice for cybersecurity to the government and to the private sector. The National Institute for Standards in Technology has developed cybersecurity standards for government and its contractors. They have encouraged the private sector to develop their own processes, using their guidelines. It is possible that NIST may develop cybersecurity standards for the private sector at some point.

Potential motives for offensive attacks

Motives against law firms can come from disgruntled employees, insider threats, or nation-states, both amateur and sophisticated cyberattackers. Simply compromising a firm or company's cybersecurity integrity can be damaging. They could be seeking specific revenge like embarrassment, and they could do that with misleading information. One case involved a phishing email with wedding photos from the parent's daughter's wedding. The photos had been taken from the web but looked like a personal email. Opening a phishing email will likely result in installing malware or other embedding features.

Foreign nationals from outside the U.S. can be engaging in economic and industrial espionage, for pecuniary, political or ideological goals. These can be unexpected, like the cyberattack on Sony Entertainment, thought to have originated from North Korea.

Malicious Insider Threat

A disgruntled employee, a legal secretary, was indicted by a Federal Grand Jury for hacking into her firm's computer after being fired and obtaining financial information of law firm employees. In another case, a computer technician at Bank of New York Mellon stole the identities of 2000 bank employees and opened bank accounts and credit cards.

How to guard against the insider?

The insider threat warrants specific defensive planning. The CERT National Insider Threat Center (NITC), Carnegie Mellon University, produces a handbook that

[18] Dept. of Com., Nat'l. Inst. of Standards & Tech., NISTIR 7298, Rev. 2, Glossary of Key Information Security Terms, 94 (2013) (definition of "information security").

focuses on how to prepare and defend against the insider threat.[19] Here are some checklist topics that can serve as a framework as you begin thinking about preparing for and defending against the insider threat.

Topic: Compromised passwords

____Frequently check for compromised passwords by setting

The Florida water system breach was traced to leaked credentials that had been available for some time.

Topic: Weak passwords

____Set random passwords to generate 10-character alphanumeric passwords. Advice from CISA following the Florida water system attack also included that the utility should "set random passwords to generate 10-character alphanumeric passwords," for example.[20]

Topic: Failure to patch known vulnerabilities

____ Software updates documented by IT cybersecurity staff

In our case in 2021 on the Florida water system, the attackers accessed the water treatment plant's SCADA controls via TeamViewer, which is remote access application. TeamViewer was installed on computers by the water treatment plant, to be used by personnel for conducting system status checks for remotely responding to alarms.

It appears that Teamviewer may have been used instead of updating the operating system and SCADA system. "All computers used by water plant personnel were connected to the SCADA system and used the 32-bit version of the Windows 7 operating system," according to the CISA alert. "Further, all computers shared the same password for remote access and appeared to be connected directly to the Internet without any type of firewall protection installed."[21]

It was reported in 2020, that 60% of data breaches were the result of outdated software.[22]

Topic: Unattended access applications

____Do not allow unattended access applications, like Teamviewer, to automatically start up with windows. The alert from federal agencies lists recommendations

---

[19] Michael Theis and the CERT National Insider Threat Center, *A New Scientifically Supported Best Practice That Can Enhance Every Insider Threat Program!*, CARNEGIE MELLON UNIV.: SOFTWARE ENG'G INST. (Apr. 9, 2019), https://insights.sei.cmu.edu/insider-threat/2019/04/a-new-scientifically-supported-best-practice-that-can-enhance-every-insider-threat-program.html.

[20] CYBERSECURITY AND INFRASTRUCTURE SEC. AGENCY, *supra* note 10.

[21] CYBERSECURITY AND INFRASTRUCTURE SEC. AGENCY, *supra* note 10.

[22] Fruhlinger, *supra* note 13.

specific to TeamViewer—"Do not use unattended access features, such as 'Start TeamViewer with Windows' and 'Grant easy access.'"[23]

Topic: File hosting programs, e.g., Dropbox

____ No propriety file hosting programs may be used.

At least one firm prohibits the use of Dropbox or any other file-hosting program. In 2012, a Dropbox breach occurred and users' emails were subjected to a flood of spam.

Topic: Mobile Device Vulnerability

____Use Mobile Device Management

For example, Hackers can fake a "hotspot" in airports and can intercept or redirect your information through Wi-Fi. A MDM can be used to close down all mobile devices that may be compromised.

Checklist of Threats based on accident, inadvertent or natural events that should trigger the use of the cybersecurity checklist.

___Human error

___Accidents

___Disruption of infrastructural services

___Natural disasters (weather, snow, lightning strikes, tornados)

___Threats from Cloud Computing and Wi-Fi

The mission creep of personnel who may not trust their IT department was cited as a concern that had to be considered, so that IT can properly be prepared for defending against a Cyberattack.[24]

For international firms, there are at least three ISO standards for continuity management processes that meet expectations for international compliance.[25]

---

[23] CYBERSECURITY AND INFRASTRUCTURE SEC. AGENCY, *supra* note 10.

[24] Deloitte spokesperson presentation at the 2nd Annual Cybersecurity and Energy and Utilities Conference (Oct. 7-8, 2013).

[25] The ISO 2700 series of standards provide auditable standards that complement the NIST cybersecurity framework for reducing cybersecurity threats.

Law firm recommendations

- Develop a comprehensive information security plan
- Conduct a risk assessment
- Use encryption software
- Only known users should have access to devices or network
- Develop a data retention and destruction plan
- Engage in pre-event liaison planning with law enforcement, etc.
- Build teams of first-responders, in house

What cybersecurity steps did Sony Entertainment take after their high profile cyberhack presumptively by North Korea?

> *As Sony struggles to repair its reputation, it has also undertaken the challenge of reconstructing its blitzed computer network, this time with an array of precautions to resist—really resist—the next assault. Sony's "secure rebuild" strategy is expected to take a year, slowly returning the studio to normalcy while plugging the myriad weaknesses that its attackers so readily exploited. The plan's premise is zero trust. It imposes precautions that Sony wouldn't previously countenance because they were too inconvenient and expensive. It's aimed at keeping bad guys out, preventing them from reaching anything valuable if they get in, and blocking them from stealing it if they do.*
>
> *To resume operations safely, Sony began by building an entirely new "white network," completely segregated from the potential contagion of its old "black network." At the start Internet access was tightly restricted. Sony will keep as little information as possible on its active network; the rest will be stashed securely, encrypted and cut off from the Internet. Emails will be archived after just a few weeks. System administrators will have access only to areas required for their jobs. Employees will be barred from installing applications that aren't pre-approved. Sony will require everyone to use two-step login procedures. Firewalls will be put on the most restrictive settings. The studio will embrace an array of "next generation" cyberdefense technologies.*
>
> *If implemented, it will represent a major step-up in cybersecurity for Sony. Will that be enough to prevent another cataclysm? Cyberexpert Lewis says that's the wrong question. "Think of it as a continuum of risk," he says. "You can do nothing, and you're at 100% risk. Or you can do a lot and you can get the risk down to 10% to 15%." The company was much*

closer to 100% risk last year and is heading much lower. That is undeniable progress. . . .[26]

Advising energy sector clients

It is important to note that both MRPC Rules 1.1 and 1.6(c) impose duties to the client on the lawyer. MRPC Rule 1.1 describes counsel's obligation to "provide competent representation to a client". MRPC Rule 1.6(c) requires that counsel's obligation must include making "reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to representation of a client." So both of these rules require that lawyers and their firms gain a level of expertise in cybersecurity necessary to advise clients. In the case of energy sector clients, that should include knowledge of previous cyberattacks on the sector, and resources for staying current with warnings and advisories from federal agencies, relevant to their clients.

To carry out this duty, the obligation begins ideally at the start of the representation. This meeting should be confidential and clear that attorney-client privilege is applicable. A discussion might begin with a description by the client of their operation and how dependent the operation is on digital assets. How communications are conducted, and whether any export controls might be violated with digital communications. By talking through these details, the client may become aware of risks of which they may not have been aware.

This will enable you to jointly explore the client's steps to creating a cybersecurity plan that includes a good understanding of the business operations, the dependency on digital assets. Other aspects that may be critical are to ensure privilege is maintained through cybersecure processes and avoid any inadvertent disclosures. This will almost certainly involve encrypted email, as a start. Then the aspects of the insider threat should also be considered.

When advising clients, your discussion should include: the client's operation; dependence of its operation on digital assets; and, how communications can be compromised. Clients may be unaware of all of these risks.

You might work through aspects of the operation, and data storage and retrieval. An important asset to consider is the preservation of the client's IP address, including contingency and disaster recovery plans. Another point of consultation with the client would be when they begin a new field of activity or new venture. This consultation can provide an opportunity for the client to understand the regulatory frameworks around the new venture area, any data security standards that might be specific to this area, and any state or federal requirements for reporting data security incidents.

---

[26] Elkind, *supra* note 3.

Advice to the client should also include a plan for if or when the client receives a notice from the federal government, Federal Cyber Intelligence, the U.S. Department of Homeland Security. This notice will be one of two types: (1) imminent target notices; or (2) catastrophic target notices. The “imminent target” notice will include “unclassified reports of cyber threats to the U.S. homeland that identify a specific targeted entity. The target may be your client or a target may be from your client’s industry sector. The second type of notice, a catastrophic target notice, will not specifically report a threat but will inform the recipient that its company is among the “most critical of the critical infrastructures” and that a cyberattack against it “could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security.”

Alerts can be voluntarily requested from the Cybersecurity and Information Security Agency in the category of “Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)”. Your client should be advised to contact the firm should they receive such a notice, immediately. This is a conversation firms should have with their clients before they receive a notice.

Remember, that a defense that a cyberattack is “unforeseeable” is likely to be an unsuccessful defense. The following checklist in anticipation of receiving these notices can be used in attorney-client discussions for steps to be taken in preparation:

- Discussion with client about the arrival of a DHS notice before it arrives
- Prepare a plan for immediate response to the DHS notices;
- Decide on what improvements to the plans should be made before arrival of any notices
- Decide on what additional improvements might be made if the client receives each kind of notice from DHS

In conclusion

Law firms have an affirmative duty to provide cybersecurity to their own information as well as client information.

Ethics complaints to ceasing the law firm can result from hacking and data breaches

Legal ethics explicitly require lawyers to develop a cybersecurity plan

These obligations will continue to become more important as breaches continue to rise in frequency.

- The Model Rules of Professional Responsibility apply to law firm cybersecurity practices as well as to advising clients about cybersecurity planning and compliance.

- Not only must a data security plan be a continuous process, counsel must be continually aware of changes in the law, and reporting obligations for clients and the firm
- Specific industries and fields have specific reporting requirements and expect these to be changing continually
- Notices from DHS impose obligations on clients to respond and prepare
- Having these discussions with clients at the earliest possible time, is advisable and should enhance the client's reputation and reduce its exposure to lawsuits and liability