



INSIGHTS FROM BDO'S NATURAL RESOURCES PRACTICE

HOW TO PROTECT AGAINST CYBERATTACKS IN THE ENERGY INDUSTRY

By Gregory A. Garrett, CISSP, CPCM, PMP, Head U.S. & International Cybersecurity


Earlier this year, the U.S. Department of Homeland Security (DHS) and Federal Bureau of Investigation (FBI) took unprecedented action and publicly accused Russia of waging cyberattacks on U.S. critical infrastructure.

According to a joint [Technical Alert](#) (TA), Russian hackers conducted spear phishing attacks and infiltrated the control rooms of small U.S. electric utility companies where they staged malware. The threat actors sought information on industrial control systems (ICS) and supervisory control and data acquisition (SCADA) systems, potentially unlocking the gates to what could have been detrimental harm to critical U.S. infrastructure.

Those cyberattacks could be just the tip of the iceberg. At a cybersecurity summit, DHS Secretary Kirstjen Nielsen said that cyberthreats now pose a greater threat to the U.S. than physical attacks. Cyberwarfare is a worsening national security threat, and the US energy industry is a likely battleground for early attacks.

At a cybersecurity summit, DHS Secretary Kirstjen Nielsen said that cyberthreats now pose a greater threat to the U.S. than physical attacks. Cyberwarfare is a worsening national security threat, and the US energy industry is a likely battleground for early attacks.

In response to increased attacks, the DHS announced the creation of the National Risk Management Center to help guard the nation's banks, energy companies and industries from major cyberattacks that could severely harm critical infrastructure. The center will serve as a go-to resource for a company experiencing a cyberattack to seek the government's help early on and will eventually conduct simulations and cross-sector analyses to identify threats and weak points in U.S. infrastructure.



By 2020, BDO predicts **U.S. critical infrastructure** will be the target of the next generation of destructive cyberattacks: a Permanent Denial of Service (PDoS) attack.

ENERGY COMPANIES FACE DIVERSE AND QUICKLY CHANGING CYBERATTACKS

As the energy industry adopts new technology and implements more internet connected devices including automated value controls, pressure sensors, heat sensors, etc. utilizing the power of the Internet of Things (IoT), the number of potential cyber vulnerabilities are increasing dramatically. Further, threats such as spear phishing attacks, Trojan-horse software and wiper viruses are occurring every day, and even every hour, on energy company offices and senior executives. The frequency in which senior executives are targeted through social media and dark web reconnaissance is significantly increasing, including Business Email Compromise (BEC) attacks which are really elaborate spoofing attacks.

In the last year or so an increasing number of attacks have come through the supply chain. For the most part, these attacks involve numerous suppliers and accounting or payment processes. Control, valve and part-supply vendors are often targeted through financial system hacks, spear phishing or spoofing campaigns due to lack of sophistication in their efforts. Cyber vulnerabilities increase when networks link to extended networks, either on a multinational or global level.

The energy industry is also susceptible to Disrupted Denial of Service Attacks (DDoS), which are large scale attacks that temporarily disrupt services or operations. These attacks are often waged against electric grids but are not limited to the power sector. Hackers also target oil and gas pipelines and seek to disrupt oil exports and domestic supply by targeting a key junction so fuel can't flow through.

True to its name, PDoS attacks aim for permanent destruction and can manifest in three ways: Destroying physical equipment and structures, disabling services and/or wiping out data.

WHO IS HACKING THE ENERGY INDUSTRY?

The greatest cybersecurity threats to the energy industry are from international state actors in Russia, China, Iran and North Korea. Like the Russian attacks detailed in the DHS and FBI alert, these threats are intended to disrupt the operations and functions of the U.S. energy sector and primarily target a company's information technology and operational technology systems. As one of the largest and most sophisticated economies, an attack to the U.S. energy sector is the holy grail for cybercriminals. Countries with competitive oil supplies also stand to gain from disrupting the U.S.'s production and exports.

A criminal group called DragonFly is one group, presumed to be state sponsored, making headlines this year. DragonFly has orchestrated a number of attacks in Europe, Asia and elsewhere to gather intelligence on the operational and control systems within the energy industry. According to recent FBI and Europol reports, we have seen increased blurring between nation-state cyberattack groups and criminal cyberattack groups, as cyber-attackers are more often working as an integrated organization.

Beyond cyberwarfare, cybercriminals inciting attacks on the energy industry are also motivated by financial gain and environmental activism. Hackers often perpetrate attacks to gather wealth through ransom attacks, and criminal cartels—or organized cyberattack groups—habitually conduct spear phishing. Hacktivists, or environmentalists that politically oppose fracking, the development of pipelines, or other actions taken by the oil and gas industry, also pose a threat to the industry. To make matters worse, the energy industry lacks the sophistication that financial services and other sectors possess when it comes to combatting cyberattacks.

Ten best practices

to effectively detect and respond to cyber risks:



- 1** Hire an independent firm to conduct an email and network threat assessment



- 2** Bolster access controls



- 3** Implement stronger audit controls



- 4** Ensure 24 x 7x 365 monitoring of your network with advanced intrusion detection systems (IDS)



- 5** Make top-down personnel education a priority for everyone (from the Board of Directors, to the C-Suite, managers and employees)



- 6** Create an internal and external crisis communications plan



- 7** Implement cyber insurance claims preparedness and adequate coverage



- 8** Create an incident response plan



- 9** Conduct periodic incident response exercises and simulations to test your response capabilities



- 10** Develop and test a Business Continuity Plan (BCP) and Disaster Recovery (DR) plan

PROTECTION STARTS WITH ASSESSING AND IMPROVING YOUR CYBERSECURITY

Chances are, many energy companies have already conducted an [International SOS](#) risk framework assessment, which allows them to see if they are up to date on industry best practices. The framework includes assessments to detect any malwares or malicious software, penetration testing on the network, employee education and awareness, monitoring, end-point protection, assessments of backup systems and real-time cyberattack response and recovery drills. If your company has not conducted the assessment yet, that's a good place to start.

HOW DOES CYBERSECURITY FIT INTO ENERGY COMPANIES' BUDGETS?

Energy companies are actively cutting costs and embracing digital and technological transformation to enhance operational efficiencies. With an industry-wide emphasis on minimizing expenditures, are companies allocating enough resources to mitigate the risk of costly cyberattacks?

The global oil industry as a whole is taking measures to prioritize cybersecurity. According to ABI Research, the international oil sector is expected to increase investments on cyber defenses by **\$1.9 billion this year**. On a company-by-company basis, however, many energy players are underfunding cyber. Midsized companies in particular are often behind the power curve in implementing and maintaining cybersecurity controls.

Energy companies of all sizes must balance their business need to streamline costs and increase efficiency while prioritizing cybersecurity protections.

Gregory A. Garrett is the Head U.S. & International Cybersecurity at BDO USA. He can be reached at ggarrett@bdo.com.



According to ABI Research, the international oil sector is expected to increase investments on cyber defenses by **\$1.9 billion this year**.



People who know Natural Resources, know BDO.

CONTACT:

GREGORY GARRETT

Head of U.S. and International Cybersecurity
ggarrett@bdo.com

CLARK SACKSCHEWSKY

Tax Office Managing Principal and National Practice Leader
csackschewsky@bdo.com

BDO'S NATURAL RESOURCES INDUSTRY PRACTICE

BDO's Natural Resources industry practice provides assurance, tax and advisory services to emerging and established businesses in the United States and all over the world who are involved in both the traditional and alternative energy industries. Our clients often operate across borders either raising capital or making acquisitions abroad. Our extensive industry knowledge is supported by our international network of more than 1,500 offices in 162 countries, allowing us to provide a consistently high level of service wherever our clients do business.

ABOUT BDO

BDO is the brand name for BDO USA, LLP, a U.S. professional services firm providing assurance, tax, and advisory services to a wide range of publicly traded and privately held companies. For more than 100 years, BDO has provided quality service through the active involvement of experienced and committed professionals. The firm serves clients through more than 60 offices and over 650 independent alliance firm locations nationwide. As an independent Member Firm of BDO International Limited, BDO serves multi-national clients through a global network of more than 73,800 people working out of 1,500 offices across 162 countries.

BDO USA, LLP, a Delaware limited liability partnership, is the U.S. member of BDO International Limited, a UK company limited by guarantee, and forms part of the international BDO network of independent member firms. BDO is the brand name for the BDO network and for each of the BDO Member Firms. For more information please visit: www.bdo.com.

Material discussed is meant to provide general information and should not be acted on without professional advice tailored to your needs.

© 2018 BDO USA, LLP. All rights reserved.

