David Blanco
Business Development Manager, AUTOSOL
Distribution: 4. (II) Cybersecurity: ensuring protection of the gas industry infrastructure
LEGAL LIABILITIES OF INDUSTRIAL CYBERSECURITY

Introduction

Every word we hear reminds us of its opposite.[1] "Safety" invokes thoughts of danger, and "assets" of liabilities. For industrial control systems (ICS) professionals, these opposing thoughts help discipline the processes industrial assets use to operate safely— by tailoring the procedures to avoid dangerous outcomes. These safety procedures rely on two assumptions: first, that decision-makers act on *accurate* data and second, that only one entity is exerting control over the assets.

Unfortunately, new cyber-threats to ICS undermine these assumptions. New technology gives hackers the ability to manipulate data and control industrial equipment from anywhere. Apart from new technical challenges, this also creates new legal challenges. When an accident occurs at a site, how does a company prove it was a hack attack and not a safety violation? If it is a hack attack, who is liable and what's the extent of the liability? The novelty of these issues makes it hard to answer these questions, but the risks of not addressing them make them impossible to ignore.

This discussion of liabilities and tort (civil) laws is not an "if-hack-then-this" prediction of how events will unfold. It's a starting point to a conversation where not even specialized attorneys can predict what the last word will be. What makes it such a difficult conversation to have is that ICS professionals have diverse business objectives and operational environments that make it impossible to just plug an incident into a formula to get an answer.[2]

Exposure to the possibilities allows for planning for the probabilities. Operators of industrial equipment know the physical and the financial results of field incidents, but when a cyber-incident is a contributing factor, the response mold is inadequate. Companies and individuals could find themselves under the jurisdiction of unfamiliar agencies, in violation of new regulations, or have insurances that do not provide coverage for cyber-events. Depending on the nature of the hack, trade secrets of the company itself and third parties could be exposed. Cyber-events have a tendency to compound other problems in a way that raises the profile of an incident often resulting in additional post-breach drops in stock value of between 17-30 percent.[3] All that being said, remember that this paper is not legal advice. It's an opportunity for exposure to new cyber-events and relevant context following those events.

To help ICS companies better understand these issues, this paper proceeds as follows: First, it presents the context of cyber-threats companies' face by broadly describing the threat. Then it breaks the topic down into cases. The first case discusses the compromise of a network via field equipment that resulted in physical destruction and provides a context relevant tort liability. The second case examines the compromise of field equipment as a result of a third-party contractor in the context of tort liability and insurance issues.

Cyber-Threats Against ICS

One of the biggest mistakes companies make when it comes to cybersecurity is to assume their network is not a target.[4] The rhetoric—calling it an argument would misrepresent its relationship to facts—that is usually invoked claims a company's network *can't* be hacked, *won't* be hacked, or *shouldn't* be the ICS professionals' responsibility. However, this ignores the capability, persistence, and ramifications of modern cyber-threats. For example, 2016 saw a 110% increase in the number of cyber-attacks against ICS networks from 2015.[5] Roughly 75% of all oil and natural gas companies experienced at least one cyber-attack last year.[6] This caps off a trend of attacks against ICS networks that increase each year. One of the reasons for this is the rich target environment.

North America has the most industrial devices connected to a network, which made those ICS networks susceptible to the 189 new cyber-vulnerabilities discovered on industrial equipment last year.[7] The problem is so real that the US and Canadian federal governments each established an Industrial Control System Cyber Emergency Response Team (ICS-CERT) to help industries respond to cyber-attacks. The US ICS-CERT responded to 290 incidents in 2016, which included "the first known cyber-attack to result in physical impact to a power grid."[8] The US government also created a new Office of Cybersecurity, Energy Security, and Emergency Response as a way to enhance industries' resilience to attacks.[9]

Although these statistics lend a sense of gravity to the threats, they don't help ICS professionals improve security. This is because facts without context are trivia, not truths. So, to give ICS professionals actionable truths to get ahead of these issues, specific examples of cyber security attacks are required that demonstrate the vulnerabilities of ICS systems and the destructive power of cyber-attacks.

Case 1: Safety Compromise

Safety Instrumented Systems (SIS) are highly specialized control systems designed to keep industrial processes operating in a safe state or to smoothly shutdown a process in case of hardware failure. Oftentimes, programmable logic controllers (PLCs) are utilized as SIS, but in cases where there is a predictable rate of hardware failure, specially designed SIS are deployed.[10] SIS act as the last-resort safety systems if an issue occurs that controllers do not see or cannot act on swiftly enough. Basically, they save lives, which is why a successful exploitation of SIS devices is so troubling. On August 4, 2017 the peace of mind SIS gave controllers was shattered when malware known as TRITON successfully remotely accessed and manipulated the Triconex emergency shut down safety solution.

The network that TRITON was discovered on was a distributed control system (DCS) that was isolated from the Internet as well as the victim company's enterprise network. Specifically, TRITON was found on the engineering workstation that engineers used to make programming changes to a SIS controller elsewhere on the DCS network.[11] How TRITON ended up on that workstation is not known. What is known, is that TRITON was a targeted, premeditated attack.

Since TRITON communicated to the Triconex controller using the Triconex's proprietary protocol, TriStation, the hackers clearly had foreknowledge of the victim's system and the engineering skills to reverse-engineer a protocol. Cybersecurity experts that analyze malware noted that the attackers deployed TRITON onto the right station shortly after gaining access to the network, indicating the tool was pre-built for this environment.[12]

Once on the system, TRITON integrated into the TriStation application suite and read the IP addresses and status of its target device.[13] The malware executed only when the Triconex controllers' key switch was set to "PROGRAM".[14] The other key-switch options were "OFF" and "RUN." TRITON then deployed a remote access trojan (RAT) onto the Triconex itself. From here, it exploited a zero-day vulnerability on the fourteen-year-old firmware version, version 10.3, that escalated TRITON's privileges to read/write. This allowed TRITON to inject files onto the controller.

From this position TRITON could have used the SIS to shut down the process, reprogram the SIS to permit an unsafe state, or reprogram the SIS to permit unsafe states while also using the DCS to create the dangerous states. TRITON actually attempted to prevent the controller from shutting down, by continually checking the status of the controller and resetting it to good states if it looked close to failure. This was likely done for two reasons. First, this helped hide the presence of TRITON by making sure it didn't interrupt operations until the time was right. Second, SIS are often triple redundant, so if TRITON tripped one of the three, then the other two safety controllers would initiate a shutdown. This is how TRITON was actually discovered.

Cybersecurity experts who examined TRITON noted that the malware was likely installed as a test for how to cause physical harm and the attacker's sophisticated attempts to expand on its abilities while on the system caused it to accidentally trip the system.[15] TRITON also had code that wasn't active, which would erase TRITON off the controller if the controller entered a failed state.

So how did TRITON get onto the engineering workstation on the isolated network in the first place? For the sake of this discussion, allow that TRITON was introduced onto the network by a third-party contractor whose infected laptop unleashed the malware onto the controller network. Since operations companies often have third-parties enter these facilities this scenario is not farfetched. But this story is more complicated than just a careless contractor. As Triconex's manufacturer noted after the attack, TRITON's exploit would not work if the Triconex key-switch was set to "RUN" mode.[16]

Although a few cyber-firms claim that in theory an exploit like TRITON could override the manual key-switch settings, the report read for this paper agrees with the manufacturer through its own testing. It's possible these controllers were left in "PROGRAM" mode to make the process of managing them easier. Since the DCS network was already isolated, allowing all the Triconexes to be accessed from the on-site controller station saved time. Again, for the sake of discussion, imagine that TRITON caused

damage and cost some employees their lives. This leaves the companies vulnerable to various liability issues.

Case 1: A Perspective On Legal Liabilities

For the purposes of creating a context in which this can be discussed with meaning, imagine that TRITON was successful in causing damage. At the Federal level, the implications of a hack-attack might appear straight forward since the Department of Transportation (DOT) already has primary authority to regulate pipelines through the Pipeline and Hazardous Materials Safety Administration (PHMSA).[17] However, the DOT's responsibilities cover the safety and inspections of the pipeline, not the security. Pipeline *security* responsibility is currently vested in the Transportation Security Authority (TSA), which is a part of the Department of Homeland Security (DHS).[18] However, the TSA has not issued specific regulations or mandates, due to a concern that mandatory standards might encourage pipeline operators to adopt a lower standard of protection than many operators have voluntarily adopted.[19]

Also contributing to this situation is the fact that there are roughly 3,000 pipeline companies in the U.S., but as of 2016 the TSA's pipeline security division staff accounts for less than two-percent of the agency's surface transportation staff. [20] This leaves the industry relatively self-regulated when it comes to cybersecurity. Considering the rapidly changing nature of cyber-threats, voluntary standards give industry players the flexibility in meeting their obligations in regards to their employees, shareholders, the environment, and the public. Frankly, the pipeline industry generally supports this because "mandatory standards could establish a standard of care against which alleged negligence could be measured."[21]

Without a catalyst event, regulators are unlikely to change their current beliefs that voluntary standards may not actually reflect an industry consensus viewpoint about what is a reasonable or

effective defense due to the varying degrees of resources and expertise between companies.[22] The primary organization currently issuing cybersecurity guidelines for natural gas pipeline control systems is the Interstate Natural Gas Association of America (NGAA),23 while the primary organization issuing cybersecurity guidelines for oil pipeline control systems is the American Petroleum Institute (API).24 The API, for example, has adopted the Cybersecurity Framework, a set of voluntary standards, guidelines and best practices issued by the National Institute for Standards and Technology, an agency of the Department of Commerce. The Framework focuses on risk management in critical infrastructure sectors so that entities can better identify, protect, detect, respond and recover from cyber-attacks.

A lack of clear regulatory standards that a company might be held to after a cyber-attack does not automatically translate into a complete lack of liability. In some cases, third parties might suffer damages and seek compensation. In such cases where a cyber-event causes damages, the plaintiff (the party who

brings a case against another in the court of law) has the burden of proving liability as well as the obligation of quantifying any damages.[25] In such cases it is likely that the operator of a pipeline will be held liable for some damages.

Principles adopted by courts in other tort cases will most likely apply. One of these principles is that utilities and pipelines are "held to a higher standard of care than normal due to the danger they present to the public."[26] In some cases voluntary standards can be used to evaluate if a pipeline met its duty of care to the public. The standard of care for defendants in tort actions is defined as "what a reasonable person would have done under similar circumstances," which will "necessarily depend on the particular facts of each case."[27] Whether or not this duty arises turns on the question of if the damage from the cyber-attack was foreseeable.[28]

Although pipelines won't be held liable for every conceivable contact with the pipeline, the concept of foreseeability is flexible. Where the extent of harm is elevated, the courts will be more likely to determine the damage was foreseeable and that a prior event similar to the incident causing harm is not required to establish foreseeability.[29] Based on the trends presented earlier and the example of such an event actually occurring, a court could determine a pipeline cyber-event "would be expected to occur" and in light of such findings the pipeline would be found to have "a duty to protect third parties and the public from damages."[30]

Due to the increasing number of global cyber incidents, even if the attack was deemed terrorism, damage caused from the attack will most likely be deemed foreseeable.[31] This duty also carries with it a potential requirement for a company to warn the public in the event of a cyber-event, since the pipeline or utility, in the hands of a cyber-attacker, is a danger.

The third-party contractor in this hypothetical is not immune from liability either. At the very least, the pipeline company likely would have a breach of contract claim against the contractor. Increasingly, service contracts include cybersecurity provisions—terms that impose certain cyber obligations on the contractor. Though an in-depth review is outside the scope of this paper, typical provisions include the obligation for a contractor to adopt administrative, physical, and technical safeguards no less rigorous than a particular security standard, such as IEC 62443/ISA99. Other provisions include complying with applicable security laws and regulations, warranting that the contractor has no knowledge of any security vulnerabilities in its infrastructure, conducting routine penetration testing, following secure software development practices, and maintaining an incident response program. If a contractor will have access to a customer's network, as in our hypothetical, it is also customary for the provisions to require the contractor to follow the customer's information security policy.

Security provisions being in place, the contractor may well become ensnarled in litigation over this event, with the customer claiming breach of contract for failing to comply with one or more security

provisions. This by no means gets the pipeline company off the hook for its contribution to the damages. Nor does it shift the wrath of public opinion. Both companies may find themselves with black eyes—the contractor for failing to follow basic security principles, and also the pipeline company for, by way of audit, failing to ensure the contractor was meeting its obligations.

On the international level, the most significant source of cybersecurity law has come from the European Union (EU). In May 2018 the General Data Protection Regulation (GDPR) will be implemented. The GDPR is binding legislation on all EU states that imposes sweeping new requirements on controllers and processors of digital information. Controllers and processors are defined in their broadest sense as companies that determine the purpose or means of processing personal data and companies that perform any operations on personal data, respectively.

The legislation will apply to any companies that either control or process the information of persons residing within the EU, including companies with no physical establishments within the EU. Of particular relevancy to cybersecurity are the breach notification requirements contained in the GDPR.

In the case of a personal data breach, the data controller must notify authorities within 72 hours unless the breach is unlikely to result in a risk to the rights of and freedoms of individuals. The data controller must also notify the affected data subjects without undue delay if the breach is likely to result in a high risk to their rights and freedoms. Other requirements include

- The replacement of opt-out by opt-in consent for the processing of personal data
- The reorientation of companies around a new, central and heightened concept of data privacy
- The creation a data protection officer on par with other significant officers within the company
- Cross border data transfer safeguards
- Fines of up to either €10 million or 2% of annual worldwide gross revenue for the preceding financial year, whichever is greater, for not only breaches but also mere violations of the GDPR

The EU has further issued a Network and Information Systems Directive 2016/1148 (NIS Directive) to complement the GDPR. This directive establishes a mandatory minimum level of cybersecurity infrastructures for digital service providers and operators of essential services.[32] Operators of essential services are defined as entities that provide a service that is essential for the maintenance of critical societal and/or economic activities, the provision of which relies on network and information systems, and in respect of which a cyber incident would have a significant disruptive effect on the provision of the service. The energy sector is included among this group.

Individual member states are authorized to adopt even higher levels of cybersecurity standards with regard to these latter due to the greater potential danger they pose to the public. The directive will go into effect in 2018 and apply only to companies that have an establishment within the EU. Providers will be required to comply with certain risk management and breach reporting obligations. These include taking appropriate and proportionate technical and organizational measures to manage risks posed to their network and information systems, and to prevent and minimize the impact of incidents involving their network and information systems.[33] Essential service providers will be required to notify, without undue delay, the government of incidents that have a "significant" impact on the continuity of the services they provide. Debate will turn on the definition of what constitutes a "significant" impact.[34] If essential service providers do not meet the requirements of the directive, the EU states are authorized to initiate assessments of security measures and request evidence of the effective implementation of such measures, such as the results of security audits. If deficiencies are found, the authorities may set appropriate penalties and issue binding instructions.

Case 2: Field Equipment Compromise

In the oil and natural gas industries well sites, rigs, and pipelines are often hundreds of miles from control stations and IT security. In situations like these, hackers can compromise one site and pivot to attack other parts of the system if the right protections and controls are not in place. From this position, hackers can deny controllers access, destroy data, and even falsify data. An example of this comes from Turkey, where a segment of the 1099-mile-long Baku-Tbilisi-Ceyhan (BTC) oil pipeline exploded after an attacker succeeded in compromising multiple layers of the victim's supervisory control and data acquisition (SCADA) system. [35]

The hackers' entry point onto the SCADA system was, ironically, through the station's own surveillance system. The "central element" of the attack was two men's ability to access the operational controls at "valve station 30."[36] From there, they were able to manipulate equipment to perform beyond the safety set points resulting in an over pressurized pipeline. The explosion that followed went undetected by controllers for forty minutes because the attackers switched off the controllers' alarms and then cut off communication for the targeted site.[37] Roughly 30,000 barrels of oil were spilled over a water aquifer. The attackers also covered their tracks by deleting 60 hours of surveillance footage and the controller's real-time logs. This attack demonstrated the skills of the hackers in controlling equipment, jamming communications, deleting the right records, and suppressing alarms. They were so good at destroying evidence on the victim's network that the existence of the two attackers is only known because another security camera, which was on a different network, caught an image of the two men accessing the site before the attack. This attack occurred in 2008, but was only publicly known to have been a cyber-attack since 2014.

The total cost of the incident ran into the billions, with $460 million in transit tariffs and $1 billion of lost business, during the three weeks it took to clean up and repair the pipeline.[38] The recovery effort was that much more complicated and expensive because seven companies owned the pipeline.[39] One of the operators claimed it as an "act of terrorism" in order to get out of shipping contracts.[40] Not only does this prove that hackers have the technical skills to be successful, but also that their goals include destroying ICS equipment in the field. Cybersecurity is a misnomer in this context because the challenge isn't to just defend the networks, but rather to protect all the company's assets—physical field equipment and finances. Although this example occurred in Turkey, its broader implications for the industry are clear in regards to how the question of legal liability pertains to the victimized companies.

Case 2: A Perspective on Liabilities

In order to not repeat the points made in Case 1, imagine the hackers from the BTC attack also extracted and published trade secrets from third parties that resided on BTC's SCADA network. While it might seem that this issue is contained within the discussion of tort liability from Case 1, there are actually specific civil remedies and criminal penalties for companies that misappropriate trade secrets. These new risks derive from the Defend Trade Secrets Act (DTSA) of 2016 and include up to ten years of prison and fines up to $5 million. The reason this should be of heightened interest to the operators, managers, and executives of production sites, pipelines, and utilities is that the penalties of the DTSA could apply to them just as the practice of sharing secrets is becoming increasingly common. Roughly half of oil and gas CEO's expect to enter into a new joint venture or strategic alliance within the next year with 57 percent planning to work with competitors.[41] Secrets are shared when companies form joint ventures as a means to spread capital costs, overcome technological limitations, and mitigate overall risk.[42] Therefore, exposure to the DTSA will give individuals within companies the knowledge they need to make decisions that mitigate these risks for themselves and their companies.

The DTSA amended the Economic Espionage Act of 1996 by providing that "an owner of a trade secret that is misappropriated may bring a civil action under this subsection if the trade secret is related to a product or service used in, or intended for use in, interstate or foreign commerce."[43] Trade secrets are defined as a form of information the owner takes reasonable measures to keep secret and derives economic value from.[44] For the purposes of how cyber-issues might impact a company with this law, the ways in which reasonable measures might be interpreted should be examined.

In *Wellogix Inc. v. Accenture LLP*, for example, the U.S. Court of Appeals for the Fifth Circuit concluded that Wellogix's procurement software for oil and gas well drilling projects contained trade secrets, based in part on Wellogix's efforts to protect its software by placing it behind a firewall and stipulating that sharing of it was subject to confidentiality agreements.[45] Considering that the BTC pipeline was "built to be one of the most secure in the world," the chances of a firewall being part of the network

architecture are high.[46] Therefore, the theoretical loss of a third-party's trade secret through a hacking event on the BTC's SCADA system is not only useful for this exercise, but also applicable to other existing SCADA systems.

There are a number of ways through which the DTSA can apply to an entity, but the one most relevant to this discussion is for entities that "misappropriate" the information. Misappropriation under the DTSA involves the acquisition or disclosure of a trade secret without authorization by an entity that knows or has reason to know that the information was acquired wrongfully, including through "clear negligence." In the case of BTC, if trade secrets of third parties were exposed and negligence established, then individuals in the company, including its executives, could be the targets of the DTSA. After all, such events, even when accidental, call into question whether BTC took "reasonable measures" to maintain the secrecy of the information.

If a secrecy agreement included provisions for BTC operators to protect the trade secret by either preventing the trade secret from being on a vulnerable machine or establishing specific security procedures that were not followed, then BTC and BTC employees could be subject to the provisions of DTSA. The criminal penalties under the DTSA include a criminal sentence of up to 10 years in prison and allows for a fine of not more than $5 million. The DTSA also allows for litigation to be held in a federal court without having to establish federal jurisdiction. However, the DTSA does not pre-empt state law, meaning that a party can file suit under the DTSA in federal court and plead a state law claim arising out of the same facts.[47]

Conclusion

The effects of cyber-attacks on SCADA systems should be more of a discussion of *when* rather than one of *if.* As BTC demonstrated, not only do attackers have the motivations to do damage, they also have the opportunities and the know-how. As the TRITON malware showed, there is no peace-of-mind left in piece. Even systems designed to be the last defense against accidents that sit on isolated networks and have physical defenses are susceptible to cyber-attacks. Although SCADA operators have a solid grasp of the standards and laws of system safety, the security side of liability continues to evolve as fast as cyber-threats. Without the proper protections in place, companies leave themselves exposed to a multitude of tort actions and possible violations of the DTSA. Therefore, cybersecurity for ICS should be part of every discussion of industrial processes as well as one of the main areas for improvement when attempting to reduce legal liabilities.

---

1 Johann Wolfgang von Goethe, *The Goethe Treasury: Selected Prose and Poetry* (Courier Corporation, 2012), 291

2 National Institute of Standards and Technology Special Publication 800-30, Managing Information Security Risk: Organization, Mission, and Information System View, September 2012.

3 *See* Joseph R. Dancy & Victoria A. Dancy, Terrorism and Oil & Gas Pipeline Infrastructure: Vulnerability and Potential Liability for Cybersecurity Attacks, 2 Oil & Gas, Nat. Resources & Energy J. 579 (2017), http://digitalcommons.law.ou.edu/onej/vol2/iss6/2, *supra* note 17, at 584.

4 Shawn Henry, "Top 5 Cybersecurity Mistakes Companies Make and How to Avoid Them," CrowdStrike Blog, January 6, 2017, https://www.crowdstrike.com/blog/category/endpoint-protection/.

5 Dave McMillen, "Attacks Targeting Industrial Control Systems (ICS) Up 110 Percent," Security Intelligence, December 27, 2016, accessed January 6, 2017, https://securityintelligence.com/attacks-targeting-industrial-control-systems-ics-up-110-percent/.

6 Giacomo Tonini, "Hackers hit 75% of Drillers as Sketchy Monitoring is Blamed," *Bloomberg*, June 26, 2017, https://www.bloomberg.com/news/articles/2017-06-26/hackers-hit-75-of-drillers-as-sketchy-monitoring-is-blamed

7 "U.S. Has Most Internet Connected Industrial Control Systems," SecurityWeek, July 11, 2016, accessed January 5, 2017, http://www.securityweek.com/us-has-most-internet-connected-industrial-control-systems.

8 "ICS-CERT Year In Review," *Industrial Control Systems Cyber Emergency Response Team*, 2016, accessed June 27, 2017, https://ics-cert.us-cert.gov/sites/default/files/Annual_Reports/Year_in_Review_FY2016_Final_S508C.pdf, 8

9 Zeljka Zorz, "US Sets Up Dedicated Office For Energy Infrastructure Cybersecurity," *HelpNetSecurity*, February 19, 2018, https://www.helpnetsecurity.com/2018/02/19/energy-infrastructure-cybersecurity/

10 Clint E/ Bodungen, Bryan L. Singer, Aaron Shbeeb, Stepphen Hilt, Kyle Wilhoit, 2017, *Hacking Exposed: Industrial Control Systems*, New York: McGraw-Hill Education. P.24

11 Gregory Hale, "S4: Safety System Attack Details," *Industrial Safety and Security Source*, January 19, 2018, http://www.isssource.com/s4-safety-system-attack-details/

12 Blake Johnson, Can Caban, Marina Krotofil, Dan Scali, Nathan Brubaker, Christopher Glyer, "Attackers Deploy New ICS Attack Framework "TRITON" and Cause Operational Disruption to Critical Infrastructure," *FireEye*, December 14, 2017, https://www.fireeye.com/blog/threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html

13 Johnson, Caban, Krotofil, Scali, Brubaker, Glyer, "Attackers Deploy New ICS Attack Framework "TRITON" and Cause Operational Disruption to Critical Infrastructure," *FireEye*

14 Kelly Jackson Higgins, "ICS/SCADA Vendor Discloses In-depth Analysis of a Recent Targeted Attack Against One of its Customers," *DARKReading*, January 18,2018, https://www.darkreading.com/vulnerabilities---threats/schneider-electric-triton-trisis-attack-used-0-day-flaw-in-its-safety-controller-system-and-a-rat/d/d-id/1330845?print=yes

15 Higgins, "ICS/SCADA Vendor Discloses In-depth Analysis of a Recent Targeted Attack Against One of its Customers," *DARKReading*

16 Higgins, "ICS/SCADA Vendor Discloses In-depth Analysis of a Recent Targeted Attack Against One of its Customers," *DARKReading*

17 The DOT's website explains the relationship in more detail. https://www.phmsa.dot.gov/
18 6 U.S.C. §§ 203 (2002).

19 *See* Dancy & Dancy, Terrorism and Oil & Gas Pipeline Infrastructure: Vulnerability and Potential Liability for Cybersecurity Attacks, http://digitalcommons.law.ou.edu/onej/vol2/iss6/2, *supra* note 116 at 598

20 See Dancy & Dancy, *supra* note 120 at 599

21 *Id.*, at 600

22 *Id.*, at 615

23 Dancy, Terrorism, 599.

24 Dancy, Terrorism, 599.

25 Id. *Supra* note 131 at 601 (See Weiss v. Thomas & Thomas De. Co., 680 N.E.2d 1239, 1242 (Ohio 1997))

26 Id., at 602

27 See Sears, Roebuck & Co. v. Midcap, 893 A.2d. 542, 554 (Del. 2004); at 554

28 See Isaacs v. Huntington Mem'l Hosp., 695 P.2d 653, 664 (Ca. 1985), see also Darcy & Darcy, *supra* note 155 at 604

29 Dancy & Dancy, at 609

30 Id., at 610

31 Id., at 619

32 Jordan Robertson and Michael Riley, "Mysterious '08 Turkey Pipeline Blast Opened New Cyberwar," Bloomberg, December 10, 2014, Accessed March 15, 2016, https://www.bloomberg.com/news/articles/2014-12-10/mysterious-08-turkey-pipeline-blast-opened-newcyberwar.

33 Jordan Robertson and Michael Riley, "Mysterious '08 Turkey Pipeline Blast Opened New Cyberwar," Bloomberg, December 10, 2014, Accessed March 15, 2016, https://www.bloomberg.com/news/articles/2014-12-10/mysterious-08-turkey-pipeline-blast-opened-newcyberwar.

34 Jordan Robertson and Michael Riley, "Mysterious '08 Turkey Pipeline Blast Opened New Cyberwar," Bloomberg, December 10, 2014, Accessed March 15, 2016, https://www.bloomberg.com/news/articles/2014-12-10/mysterious-08-turkey-pipeline-blast-opened-newcyberwar.

35 https://ctovision.com/violent-cyber-attack-noted-date-2008-pipeline-explosion-caused-remote-hacking/

36 Jordan Robertson and Michael Riley, "Mysterious '08 Turkey Pipeline Blast Opened New Cyberwar," Bloomberg, December 10, 2014, Accessed March 15, 2016, https://www.bloomberg.com/news/articles/2014-12-10/mysterious-08-turkey-pipeline-blast-opened-newcyberwar.

37 Jordan Robertson and Michael Riley, "Before Stuxnet, Refahiye pipeline blast in Turkey opened new cyberwar era ," *The Sydney Morning* Herald, December 12, 2014, https://www.smh.com.au/world/before-stuxnet-refahiye-pipeline-blast-in-turkey-opened-new-cyberwar-era-20141212-125nvy.html

38 Robertson an Riley, "Before Stuxnet, Refahiye pipeline blast in Turkey opened new cyberwar era ," https://www.smh.com.au/world/before-stuxnet-refahiye-pipeline-blast-in-turkey-opened-new-cyberwar-era-20141212-125nvy.html

39 BP owns 30.1 percent of the BTC, while Socar holds 25 percent. Other shareholders include U.S. Chevron and ConocoPhillips, Norway's StatoilHydro, Italy's ENI and France's Total. Oran Coskun, Lada Yevgrashina, "Blast halts Azeri oil pipeline through Turkey," *Reuters*, August 6, 2008, Accessed February 25, 2018, https://www.reuters.com/article/us-turkey-pipeline-explosion/blast-halts-azeri-oil-pipeline-through-turkey-idUSSP31722720080806

40 Robertson an Riley, "Before Stuxnet, Refahiye pipeline blast in Turkey opened new cyberwar era ," *The Sydney Morning* Herald, December 12, 2014, https://www.smh.com.au/world/before-stuxnet-refahiye-pipeline-blast-in-turkey-opened-new-cyberwar-era-20141212-125nvy.html

41 Jennifer H. Roscetti & Charles T. Collings-Chase, "How to Protect IP In Energy Industry Joint Ventures," *Law360*, August 24, 2015, https://www.finnegan.com/en/insights/how-to-protect-ip-in-energy-industry-joint-ventures.html

42 Roscetti & Collings-Chase, "How to Protect IP In Energy Industry Joint Ventures," *Law360*, 2015

43 Peter J. Toren, "Five Things to Know About the Defend Trade Secrets Act," *IPWatchDog*, May 11, 2016, http://www.ipwatchdog.com/2016/05/11/five-things-know-defend-trade-secrets-act/id=68954/

44 Toren, "Five Things to Know About the Defend Trade Secrets Act," *IPWatchDog*, 2016

45 https://www.finnegan.com/en/insights/how-to-protect-ip-in-energy-industry-joint-ventures.html

46 Dancy & Dancy, at 588

47 Bradford K. Newman, Jessica Mendelson, MiRi Song, "The Defend Trade Secrets Act: One Year Later," *American Bar Association*, April 2017, https://www.americanbar.org/publications/blt/2017/04/02_newman.html