CIRCADENCE

Gamifying Cyber Security Learning

For the Oil & Gas Industry

The Importance Of Security In The Oil and Gas Industry

Research postulating the effects of a cyber attack on oil and gas companies paints a very dim picture of the outcomes. IQPC's report "What Comes After the Unthinkable?" sets the scene, forecasting the repercussions of the oil and gas industry if a cyber attack were to occur:

> *"Imagine pure chaos and you may be close to visualizing the possible effects of an attack on infrastructure. Our society desperately relies on the systems that have been put in place for both functionality and survival. Like a natural ecosystem, our society functions from a network of intertwined processes in a somewhat dynamic state of equilibrium. Remove any one of these functions and modern society will begin to fall. Like other cyber attacks, capital can be lost. More importantly, life can be lost."* [1]

The American people rely on oil and gas to help with a multitude of tasks include cooking, heating/cooling their homes, raising a family, communicating through use of electronic devices, and more to everyday life.

[1] IQPC Exchange, "What Comes After the Unthinkable? The Threat of Cyber Attacks on Critical Infrastructure," IQPC, Accessed 8 May 2018

To support those daily activities, there exists approximately 1,793 natural gas-powered electricity plants in the U.S. and they generated 34 percent of the nation's electricity last year[2].

Loss of access to these sources means loss of all the things we rely on daily to function in modern life. IQPC shares the socio-economic impacts a lack of oil and gas would have on society if impacted by a cyber attack:

"If there is no oil, transportation comes to an abrupt halt. If transportation stops, then industry – thus the economy, will stagnate. Most people will be unable to report to work. Productivity within the affected area would cease. Products, services and food cannot be delivered without oil. Food would be supplied locally at astronomical prices. Starvation is inevitable for individuals without access to farms or capabilities to be self-sustaining.

After long term unavailability, secondary products derived from petroleum will become unavailable. This absence would greatly affect the creation or recycling of plastics and its impact would include most clothing, technology (with physical plastic components such as phones, computers), hygiene items, and most medical equipment. Healthcare would be adversely affected as plastic-based items that are vital to sanitation would no longer be available after some time."

Economically, without oil and gas to produce energy, we wouldn't have a place in the global economy and the GDP would be greatly influenced by having to import resources from other countries. While thousands of facilities would need to be targeted to bring this "doomsday" reality to life, experts believe it's not impossible.

[2] Muyskens, J., Keating, D., Granados, S. "Mapping How the United States Generates its Electricity," Washington Post, 28 March 2017

Oil and Gas: Cyber Security Challenges and Threats

Security professionals of oil and gas companies seek to improve the security of operational technology (OT) to lower overall business risk

> *About 85 percent of critical infrastructure of privately owned [3], it is essential that these organizations understand the risks of inaction.*

However, this goal appears to be a far-fetched dream for many InfoSec leaders in the industry who are not blind to the oil and gas cyber security risks we face today. The Ponemon Institute surveyed oil and gas risk security managers for their 2017 report and found of those surveyed, **68 percent stated that their company had suffered at least one security compromise involving information loss or operational disruption in the past year**[4]. Respondents added that their enterprise doesn't have a strategy to manage OT digital risk and with the upward swing in digitalization in this industry, many believe the reliance on technology, while beneficial and needed, only opens them up further to attacks.

Further studies calculate a higher percentage of companies affected by cyber attacks. A 2018 Kroll report "Global Fraud and Risk Report: Forging New Paths in Times of Uncertainty" says of senior executives surveyed in the natural resources sector.

> *87 percent have been affected by cyber incidents in the past 12 months*[5]

[3] Souchek, Thomas Major, "Fusion Centers and Public-Private Collaboration," Office of the Director of National Intelligence, 28 June 2011

[4] Ponemon Institute, "The State of Cyber security in the Oil and Gas Industry: United States," Sponsored by Siemens, February 2017, Accessed 8 May 2018

[5] Kroll, "Global Fraud and Risk Report: Forging New Paths in Times of Uncertainty," Kroll, 2017, Accessed 8 May 2018

Email-based phishing attacks are the most common type (38 percent). Other common incidents include virus/worm infestations (37 percent) and change of data (31 percent)[6]. Ex-employees are reported as the most common perpetrators of cyber attacks, followed by freelance or temporary employees, then competitors.

The severity and vulnerability to oil and gas companies not only manifests in the aftereffects of an attack, it also manifests in the sheer volume of undetected threats.

> *One report notes, an additional 46 percent [7] of cyber attacks on OT go completely undetected.*

When Senior Security Engineer of NIST, Jim McCarthy, interviewed security managers, they reported two cyber security issues that kept them up at night: identity and access management, and situational awareness[8]. Threats that go undetected are outcomes of the lack of situational awareness and quite possibly, a lack of proper identification and access management protocols in place.

With those statistics informing current cyber security approaches and thinking, it only makes sense why the oil and gas sector are scrambling to update their cyber security systems. ABI research estimated oil and gas companies will spend $1.87 billion on cyber security in 2018 alone[9]. With the increase in breaches, cyber security must be considered a safety priority, as operational systems are at risk of being hacked, causing not only a great loss in financial assets, but also risk in employee endangerment as well.

> *With the increase in breaches, cyber security must be considered a safety priority, as operational systems are at risk of being hacked, causing not only a great loss in financial assets, but also risk in employee endangerment as well.*

[6] Kroll, "Global Fraud and Risk Report: Forging New Paths in Times of Uncertainty," Kroll, 2017, Accessed 8 May 2018

[7] IQPC Exchange, "Best Practices for Cultivating a Culture of Security," IQPC, Accessed 8 May 2018

[8] IQPC, "The Most Common Cyber security Weaknesses," NIST, Accessed 8 May 2018

[9] ABIresearch, "Cyber-attacks Against Oil & Gas Infrastructure to Drive $1.87 Billion in Cyber security Spending by 2018," ABIresearch, 29 January 2013.

Relevant Standards and Regulations

While the oil and gas industry is in cyber jeopardy, there are several resources available for companies to utilize to strengthen their security posture. The following sources were provided by NIST and the National Cyber security Center of Excellence[10]:

ISA 99
Industrial Automation and Control Systems Security

IEC 62351
Communication Network and Systems Security

NERC Critical
Infrastructure Protection Plans v.3 and v.5

NRC 10 CFR 73.54
Protection of Digital Computer and Communication Systems and Networks

NRC Regulatory Guide 1.152, Rev. 3
Criteria for Use of Computers in Systems of Nuclear Power Plants

NIST IR 7628
Guidelines for Smart Grid Cyber Security

NIST SP 800-82
Guide to Industrial Control Systems Security

ES-C2M2
Electricity Subsector Cyber security Capability Maturity Model

[10] NIST and NCCoE, "Situational Awareness: Securing Networked Infrastructure for the Energy Sector," NIST, 15 November 2013

Lessons Learned: Oil and Gas Attacks

Organizations help companies make progress in identifying and preventing today's cyber attacks, yet it hasn't completely prevented them. The following list of oil and gas companies have already fallen victim, indicating a need for improved resilience—to be better prepared to respond to potential threats and determine that safe and reliable operations can be restored and maintained.[11]

- In 2010, Stuxnet, a malicious computer worm, was used to hijack industrial control systems around the globe, including computers used to manage oil refineries, gas pipelines, and power plants. It reportedly destroyed a fifth of Iran's nuclear centrifuges. The worm was delivered through a worker's thumb drive.[12]
- In August 2012, a person with privileged access to one of the world's leading National Oil Companies' (NOCs') computers unleashed a computer virus called Shamoon (disk-wiping malware) that erased three quarters (30,000) of the company's corporate personal computers (PCs) and resulted in an immediate shutdown of the company's internal network.[13]
- National Security Authority Norway said 50 companies in the oil sector were hacked and 250 more were warned to check their systems, in one of the biggest hacks in Norway's history.[14]
- Ugly Gorilla, a Chinese attacker who invaded the control systems of utilities in the United States, gained cyber keys necessary to access systems that regulate flow of natural gas.[15]
- In January 2015, a device used to monitor the gasoline levels at refueling stations across the United States—known as an automated tank gauge or ATG—could be remotely accessed by online attackers, manipulated to cause alerts, and even set to shut down the flow of fuel. Several Guardian AST gas-tank-monitoring systems have suffered electronic attacks possibly instigated by hacktivist groups.[16]

[11] EY, "Digitization and cyber disruption in oil and gas," EY Global Information Security Survey, 2016

[12] Kelley, Michael "The Stuxnet Attack on Iran's Nuclear Plant was 'Far More Dangerous' than Previously Thought," Business Insider, 20 November 2013

[13] EY, "Digitization and cyber disruption in oil and gas," EY Global Information Security Survey, 2016

[14] Paraskova Tsvetana, "Combatting Cyber-Attacks In The oil and gas Industry," FoxBusiness, 16 December 2016

[15] Assante, Michael, "America's Critical Infrastructure is Vulnerable to Cyber Attacks," Forbes, 11 November 2014

[16] ERPScan "Oil and Gas Cyber Security Basics," ERP Scan, 16 March 2016

What we can learn from these examples is that the attack surface is wide for hackers and infiltration can occur at multiple levels. To lessen the attack surface, cyber teams need to be prepared to address all possible scenarios that can occur on said attack surface in order to effectively protect and defend IT and OT infrastructures. Oil and gas companies may not have the quantity of cyber professionals needed to monitor all areas of the attack surface at all times, which is why those employed, need to be up-to-date on the latest threat tactics and training in environments that reflect their everyday security environment.

Solution: On-Demand Gamified and Persistent Learning

Measures to preserve the operational integrity of oil and gas companies can be accomplished with the adoption of a new paradigm that focuses on **gamified learning** and **persistent learning** working together to bulk up defenses.

Gamified Learning:

Gamified teaching engages practitioners through modern learning strategies. It works by allowing trainees to apply what they know in simulated environments, creating a connected and interactive learning setting. Gamified learning appeals to the learning style of the next generation (people born after 1980), increasing retention up to 75 percent[17]. Other benefits of gamified learning include[18]:

- Increased engagement, sense of control and self-efficacy
- Adoption of new initiatives
- Increased satisfaction with internal communication
- Development of personal and organizational capabilities and resources
- Increased personal satisfaction and employee retention
- Enhanced productivity, monitoring, and decision making

Unlike compliance-driven teaching methods, gamified teaching engages practitioners individually and in teams, through modern learning strategies. It works by enabling learners to apply what they know to simulated environments or "worlds," creating a natural flow that keeps learners engaged and focused. Further, it can deploy connected, interactive, social settings that allow learners to excel in competitive, strategic situations.

[17] Digitec Interactive, "Solving the Training Dilemma with Game-Based Learning," Play to Teach, Accessed 9 May 2018

[18] NCBI "I Play at Work - 10 Principals for transforming work processes through gamification" 30 January 2014

To teach and hone skills, Circadence's cyber learning platform Project Ares offers mini-games to learn concepts, battle rooms to practice tactics, and missions to learn-by-doing on cyber ranges. The virtualized environments allow players to learn about both offensive and defensive tasks and protocols. Full-scale missions portray real-world cyberattack scenarios, like the WannaCry ransomware that disrupted medical devices, and offensive exercises covering adversary tactics are also available. Players use real-world commercial and open-source tools incorporated into mission design or they can add in new ones or write their own to see what works best with evolving threats.`

Persistent Learning:

Outside of gamification, persistent and hands-on learning will help take your cyber team to the next level. Benefits to this learning method:

- Increased engagement – by keeping learners engaged they are able to stay focused on the subject matter at hand
- Opportunities to close gaps immediately – instant feedback, instruction, and critique make it easy for learners to benefit from interaction with the instructor and peers and immediately implement this feedback to improve
- Risk mitigation and improved problem solving – hands-on training allows learners to master skills prior to working in real-world environments. People can work through tough scenarios in a safe training environment – developing problem-solving skills without risk.

To help oil and gas cyber teams stay abreast of the latest threats, Project Ares is designed for persistent learning, meaning it's constantly evolving with new missions rapidly added to address the latest threats and customer-specific training requirements. Further, targeted training can be accessed from the library of mission scenarios to train specific skill sets. Cyber security leaders can also add new custom exercises through Orion, our battle room builder, to address specific scenarios pertinent to the oil and gas industry.

As players engage in these activities, they earn experience points that lead to skill badges to bring forth the "gamified" aspect of learning—all of which is viewable on the platform's leaderboard. They are also able to play individually on the platform or in teams. In a naturally competitive way, players can have that hands-on experience they've been craving—even the experience of failure, which is critical to learning and growing. There are work role learning paths aligned to the NIST/NICE framework to standardize learning and the platform can help professionals take what they've learned in their certification work and apply it to realistic scenarios.

By placing the power of security in human hands, cyber security teams can proactively improve a company's ability to detect cyber-related security breaches or anomalous behavior, resulting in earlier detection and less impact of such incidence on energy delivery, thereby lowering overall business risk. Users are the last line of defense against threat actors so prioritizing gamified training for teams will foster the level of collaboration, transparency, and expertise needed to connect the dots for cyber security in oil and gas sectors.

Learn more about Project Ares Subscriptions