The oil and gas cybersecurity enigma

Leon Hamilton[1] and Marianne Rauch[2]

https://doi.org/10.1190/tle41090641.1

Abstract

The digitization of the oil and gas industry creates potentially detrimental opportunities for terrorists, criminals, insiders, and activists to exploit. Due to the COVID-19 pandemic, working remotely has become the norm, and remote collaboration has been enabled by such Internet-based applications as Microsoft Teams, Zoom, and others. Remote employees may be more casual with cybersecurity, which further increases the risk of cyberattacks. Successful cyberattacks against oil and gas assets or operations have the capacity to cripple economies, disrupt power grids, and initiate political or public unrest and chaos. Cybersecurity defense should be as central to our organizational culture as turning on our workplace computer. We discuss the most likely weak points in our systems and possible solutions.

Introduction

Oil and gas, like many other industries, has been transitioning rapidly toward becoming a viable participant in the cyber ecosystem. The industry has large data sets that are suitable for machine learning applications and that require considerable computer resources for preparation and analysis. Cloud services such as Google Cloud are available and integrated to achieve scalability, business continuity, and reduced IT costs. The digitization of oil and gas creates opportunities for cyberterrorists, criminals, insiders, and activists (Progoulakis et al., 2021). Due to the COVID-19 pandemic, the last few years have been challenging as many offices were closed and workers sent home, but work still had to meet established performance metrics. Working remotely has become the norm, and collaboration has been enabled via such applications as Microsoft Teams, Zoom, and others. This growing dependence on the Internet results in cybersecurity challenges, economic risks, and possible data breaches or increased exposure to hacking operations (Eling et al., 2022). Cybercriminals know that remote employees are more casual with cybersecurity and susceptible to attack because these criminals collect, analyze, evaluate, bundle, and sell data reflecting individuals' online activities and use them to predict and modify end-user behaviors (Zuboff, 2019), which negatively impacts the safety of operations and exposes organizations to cyberattacks (Atstaja et al., 2021).

These attacks are not restricted to competitors who might want to exploit technological infrastructures or access proprietary information. Successful cyberattacks against oil and gas assets or operations have the capacity to cripple economies, disrupt power grids, and initiate political or public unrest and chaos (Atrews, 2020). For example, last year the Colonial Pipeline was compromised by cybercriminals, resulting in the president of the United States declaring a state of emergency as the disruption negatively affected the airline industry and populations experienced fuel loss in many southeastern U.S. states. Cybercriminals shut down 5500 miles of pipeline that resourced 45% of the East Coast populace resulting in fuel shortages (U.S. House of Representatives, 2021). To compensate for the inoperative pipeline, 13,000 midsized fuel tankers provided daily oil transport, resulting in increased fuel prices and significant declines in economic growth (Schachinger, 2021).

Recently, successful cyberattacks on European oil transport and storage companies have negatively impacted oil unloading and loading and supply chains within the European Union, which has led to disruption of energy sectors and economies in Germany, Belgium, and the Netherlands (Beer, 2022). The seriousness of the problem led to the World Economic Forum's Cyber Resilience in Oil and Gas initiative. Through this initiative, 18 global oil and gas organizations foster and share best practices and collectively align cyber resilience efforts within member organizations in a unified effort to mitigate cyberattacks (Jones, 2022; World Economic Forum, 2022). This combined effort to combat cybercrime — a problem expected to cost US$10.5 trillion globally by 2025 (Morgan, 2020) — illuminates the severity of the threat facing the industry.

Cybersecurity should be as central to organizational culture as turning on our workplace computers. Here, we discuss the most likely weak points in our systems and possible solutions.

Integration of reservoir computing, originally a recurrent neural network (RNN), is agile enough to accommodate temporal/sequential information processing (Tanaka et al., 2019). Benefits of an RNN and applicable machine learning programs that predict reservoir locations and properties include selecting seismic horizons, estimating missing yields, rapid learning, low training expenditures, and optimized computational performance. Machine learning can help solve complex problems using data with only minimal human interaction. Deep learning algorithms do not require supervision when coded correctly and when input data are valid. Consequently, these algorithms generate solutions at a fraction of the time it would take humans to perform similar tasks. With continuing increases in computational power and availability of cloud services, those processes are being applied more frequently. One example of applying machine learning is SaltSeg an automated salt interpretation tool developed by TGS (Satyakee et al., 2019). This application is a high-capacity deep convolutional neural network architecture that achieves human-level interpretation accuracy on seismic images. It is designed to work on low-resolution, noisy, incorrectly migrated seismic images. After each prestack depth migration, this tool can be used to quickly reinterpret the salt bodies that then are used for the next velocity model building and migration effort. Conversely, there is an adage that states "rabbit hunting is fun, until the rabbit gets

[1] Consultant, Houston, Texas, USA. E-mail: lhamilton79@hotmail.com.
[2] TGS, Houston, Texas, USA. E-mail: mrauchdavies@gmail.com.

the gun." SaltSeg and other machine learning protocols are fueling a dynamic, novel, digital ecosystem that expands efficiencies in the oil and gas sector. These applications when used on large data sets with millions of input data points can be very computer intense and often are moved to the cloud. Conversely, cybercriminals are utilizing similar systems and algorithms to facilitate hacking, phishing, cloud hacking, and myriad other cyberattacks to compromise and exploit industrial sectors (Ciancaglini et al., 2020).

The digital oil and gas world

The integration of machine learning presents an optimal strategy for compiling and assimilating large geophysical and geologic data sets to extract information while reducing or eliminating bias (Marzan et al., 2021). Recently, machine learning applications have expanded as computer power and processing speeds have improved exponentially. Processes that would have taken days or weeks are now executable within hours or overnight.

It is important to recognize potential risks of cyberthreats to upstream (exploration and production), midstream (transportation), and downstream (refining and marketing) oil and gas operations (Mohammed et al., 2022). Novel technologies place the oil and gas sector squarely in the crosshairs of cybercriminals as these technologies rely heavily on advanced transistors as the digitization center of gravity.

The Internet has become the substratum of a global cyberspace that enables a majority of social, communal, economic, and governmental activities between individuals and institutions that otherwise may not have been interacting. The proliferation of technology is embedded in the rapidly changing global landscape resulting in a digital ecosystem of indispensable, low-cost technological assets that benefit approximately 3 billion users worldwide (Tan et al., 2021). Furthermore, evolving Internet and cyberspace operations have generated billions of dollars for the global gross domestic product, of which oil and gas contributes approximately 3% (Kolaczkowski and White, 2022).

Just as it has become a medium for transmitting, processing, manipulating, and storing sensitive proprietary or personal information, the Internet has also become a haven for cybercriminals. Cybercrime costs the global economy US$6 trillion, which, if it were measured as a country, would represent the world's third-largest economy after the United States and China (Morgan, 2020). Thus, proactive cybersecurity mitigation efforts should be at the forefront of everyone's professional and personal radar.

What is cybersecurity?

Cybersecurity can be defined as practical measures, both proactive and reactive, implemented to protect an organization's infrastructure, proprietary or individual information, networks, and data against internal and external threats.

Proactive cybersecurity measures are implemented to prevent cyberattacks from ever occurring. Proactive cybersecurity accounts for all potential threats and identifies vulnerabilities that could be attack vectors and lead to significant issues. Some examples of proactive methodologies are outlined in Table 1.

Traditional cybersecurity measures are reactive in response to a successful cyberattack. Reactive cybersecurity implies that a breach has occurred, and we are reacting to it. This is problematic, expensive, and leads to loss of trust from customers and shareholders. Second- and third-order effects can include reputational damage, fines, operational disruption, and ultimately bankruptcy. Reactive measures to mitigate or resolve issues resulting from cybercrimes can take many years and should be the least preferred way to operate.

The difference between reactive and proactive practices is huge and has a significant impact on the successful management of cyberthreats. In a reactive scenario, we assume that the company has been breached because insufficient security measures have been implemented. Reactive measures like settlements and securing web access after an attack could be costly and time consuming and can result in insolvency. Being proactive means planning and instigating all needed practices within the organization before an attack occurs. Initially, proactivity is more time consuming and requires more resources, but it is the preferred way to mitigate security breaches.

Table 1. Proactive measures and suggested solutions. Modified from TechAdvisory (2021).

Proactive measures	Required actions
Security training for all employees	Train everyone from receptionist to CEO on proper and secure Internet usage.
Update antivirus software and cloud services securities	Protect assets from the latest malware.
Software update	Always install the latest security patches.
Web-filtering services	Blacklist dangerous and inappropriate websites. Block suspicious e-mails.
Perimeter defenses	Scrutinize everything that tries to get past firewalls.
Policy of least privilege	Restrict users to essential access.
Data segmentation	Rank data and put higher protection around more sensitive data.
Strict access control	Enforce strong passwords, two-step authorization, screen locks, and logouts for idle screens.
Artificial intelligence-driven network monitoring	Use to identify suspicious activities and users.

What are the main cyberthreats?

Internal threats represent a profoundly complex and evolving risk that affects the technological infrastructure of oil and gas organizations. The Computer Emergency Response Team Coordination Center (CERT/CC) at Carnegie Mellon University offers a general insider threat definition. It defines an insider threat as "the potential for an individual who has or had authorized access to an organization's assets to use their access, either maliciously or unintentionally, to act in a way that could negatively affect the organization" (Costa, 2017). However, the National Cybersecurity and Communications Integration Center of the U.S.

Department of Homeland Security advises that "insider threats, to include sabotage, theft, espionage, fraud, and competitive advantage are often carried out through abusing access rights, theft of materials, and mishandling physical devices" (U.S. Department of Homeland Security, 2014). Sometimes the biggest danger comes from within. The CERT/CC identifies insider threats as outlined in Table 2. Responsible individuals could be anyone, past or present, employed by the company, which includes external partners or vendors. The consequences of internal threats could affect assets across the organization. Prolific interconnectedness within the oil and gas industry could exacerbate affected assets. Cyber events against the organization could be intentional or unintentional depending on the source, purpose, awareness, and other variables. The negative ramifications of insider threats against industrial control and process systems can result in negative reputational impact, exploited proprietary assets, lost revenue, operational disruption, and compromised safety instrumentation (Tsiostas et al., 2020; Zhu and Liyanage, 2021).

Table 2. Summary of sources, causes, and consequences of insider security breaches. From Costa (2017).

Responsible individuals	Affected assets	Intentional or unintentional acts against the organization	Negative ramifications
Current or former full-time employees	People	Fraud	Financial losses
	Information	Accidental loss or disposal of equipment or documents	Harm to organization and employees
Part-time employees	Technologies	Theft of intellectual property	Degradation of information
Temporary employees	Facilities	Cyber sabotage	Disruption of organization's ability to meet its mission
Contractors	Data	Accidental disclosure	Damage to organization's reputation
Trusted business partners	Proprietary assests	Espionage	Harm to organization's customers

External threats define outsider attacks in which individuals, nation-states, or groups attempt to compromise or gain unauthorized entry into the technological infrastructure of an oil and gas organization. Most external threats attack the organization to steal proprietary information or technological assets by applying phishing, viruses, or malware. These devastating attacks are usually executed by sophisticated cybercriminals. Cybercrime has become a business, and novel business models enhance the likelihood that cybercrime is being conducted by novices. Hacking as a service (HaaS) is centered on the professional hacker whereby they are the contractor who monetizes or commercializes their skillsets (Ollmann, 2008). This service is available to anyone with a credit card and access to a web browser. Consequently, hacking operations do not have geographic limits. Primary external security threats are human threats, network security threats, communication security threats, software threats, social and economic threats, legal threats, and physical security threats.

Do we have good practices?

The oil and gas industry consists of multiple business operations, and each business in the oil and gas industry must adopt specific corrective measures to strengthen the organization's cyber readiness and risk posture. Significant changes have occurred in oil and gas infrastructure that have increased vulnerabilities across the sector (Nygaard and Mukhopadyay, 2020). The large number of regulatory bodies publishing different standards makes it difficult to standardize on a comprehensive, straightforward oil and gas cybersecurity strategy that is applicable to the sector. Elevated awareness about technologies that could enhance cybersecurity initiatives could increase cybersecurity efficiencies and help mitigate novel cyberattacks on oil and gas infrastructures. It is worth noting that a 100% secure technological infrastructure is nonexistent, regardless of the industry. However, increasing end-user awareness and influencing information security compliance behaviors will pay dividends toward achieving the confidentiality, integrity, and availability (CIA) of digital information. The CIA triad is the standard that information security leaders utilize to manage information security operations and strengthen the security norms of end-users, who are the weakest link in information security. Traditionally, the most commonly transmitted proprietary data would include sensitive geophysical and geologic data; production reports; supply chain statistics; and health, safety, and environment information. However, command and control operations are more centralized and require network transmittal of operational information that is increasingly sensitive and proprietary. These operations create challenges for any industry but especially so for the complex and multilayered oil and gas industry. The challenge is not that executives do not understand cybersecurity, but that they are unaware of potential exposure of the organization to evolving risks when expanding to new market opportunities, external partnerships, usage of cloud services, and moving sensitive meetings from in-person to virtual communications. According to Ayoub and Firth (2021), "Just 29% of oil and gas cybersecurity leaders say the board or executive management committee understands the value of cybersecurity to the business," which is notably lower than in other industries (Figure 1). It is difficult, if not impossible, to lead or manage concepts that are not understood.

In many instances, cybersecurity teams are not integrated into organizational strategic planning processes. This a critical area of concern as one successful cyberattack can render an entire network nonoperational. Ayoub and Firth (2021) found that fewer than half (48%) of surveyed cybersecurity teams are included on the design and planning phases of a new initiative, and 65% of cybersecurity professionals suggest that oil and gas operations integrate new technologies to expand their competitive footprint before vulnerability assessments are conducted. Cybersecurity challenges are exacerbated by the fact that a significant percentage of business expansions, locally and globally, are executed by large, turnkey third-party partnerships or contracts.

Unlike oil and gas, many other industries have developed sophisticated cyber defenses and synchronized regulations. This lagging by the oil and gas industry is partly due to pushback by industry lobbyists against stricter standards and regulations. The Colonial Pipeline ransomware attack that forced a Bitcoin payment of US$4.4 million, resulted in a weeklong shutdown, local gas shortages, and fuel shortages across multiple states (Kilovaty, 2022). Unfortunately, more than half (54%) of oil and gas cybersecurity leaders complain about maintaining pace with industry regulations and struggling to keep systems compliant with legal statutes (Ayoub and Firth, 2021).

Virtual communication

The COVID-19 pandemic changed how we communicate and how we work. Many companies closed offices, either temporarily or permanently, and workers logged on remotely to perform tasks. Meetings were moved to virtual platforms such Zoom and Microsoft Teams. Video conferencing using Teams alone has increased by 535% in daily traffic in 2020 from 2019 (Figure 2) (Curry, 2022). The sudden expansion and integration of these technologies could increase exposure to multiple cyberthreat categories, including espionage, compromise of personally identifiable information, operational manipulation, and service disruption or discontinuance (Lewis, 2020), if we wrongly assume that established cybersecurity measures are sufficient under this "new norm."

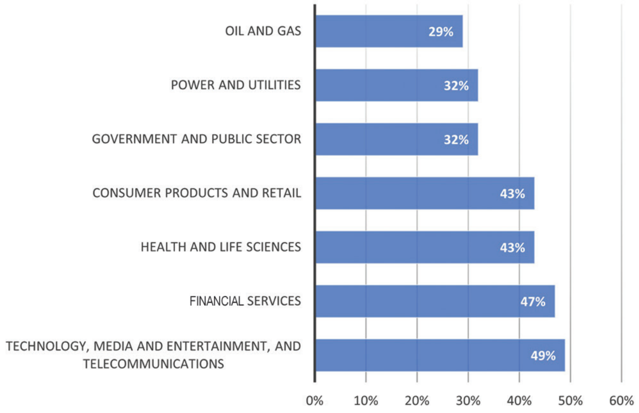

Figure 1. Percentage of boards of directors across different industries that fully understand the value of the cybersecurity team, according to cybersecurity leaders (modified from Ayoub and Firth, 2021).

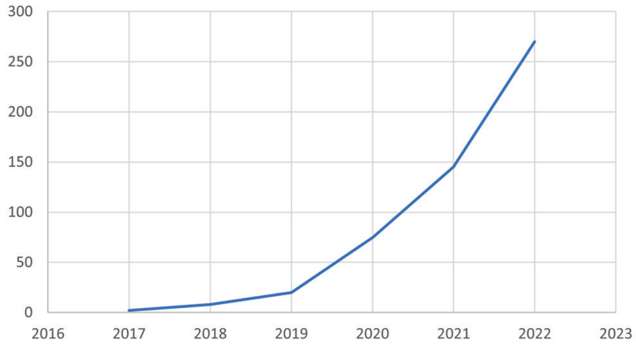

Figure 2. Number of Microsoft Teams users per year in millions (Curry, 2022).

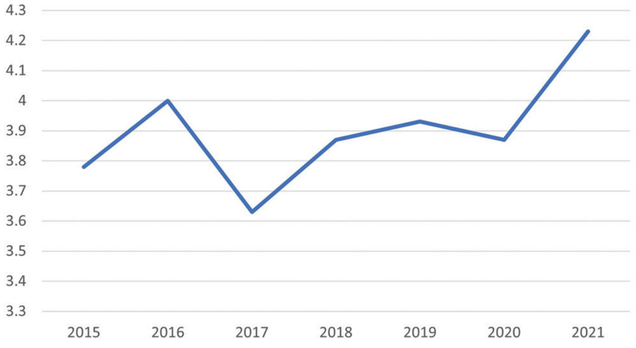

Figure 3. Average total cost of data breach in U.S. million dollars (Fichtenkamm et al., 2022).

During the initial months of the COVID-19 pandemic, cyberattacks against agencies in the United States increased to 30,000 attacks between 31 December 2019 and 14 April 2020, which was almost equivalent to the 2018 annual total of 31,107 (World Economic Forum, 2020; Statista, 2022). From May 2020 to May 2021, daily cybercrime complaints increased by 300%–400% (Aldridge, 2021). From January to April 2020, 907,000 spam messages, 737 malware incidents, and 48,000 malicious uniform resource locators (URLs) were registered. Average ransomware payment amounts increased by 60% during the second quarter of 2020. Also, from May 2020 to May 2021, Google blocked 18 million COVID-19-related scams daily. Phishing attacks increased by 220% compared to the annual average. According to IBM's Cost of Data Breach Report 2021 (IBM Security, 2021), the average cost of a data breach in 2021 increased to US$4.24 million. Figure 3 displays the increase in cost caused by data breaches during the COVID-19 pandemic. It also shows a significant trend upward starting in 2015 as was outlined by Fichtenkamm et al. (2022).

Dealing with cyberthreats

The response to evolving threats and modified policies potentially represents consistent interference to operational continuity that must occur for the safety of oil and gas technological infrastructure and data privacy. Leadership has a substantive role during the digitalization of oil and gas operations and could be the determining factor in whether or not an organization survives (Durmaz et al., 2022). The substratum to a successful CIA triad is employee conformance to established and modified information security policies emplaced to mitigate cyberattacks.

The insider threat is one of the most persistent concerns in cybersecurity and the National Counterintelligence Strategy of the United States of America 2020–2022 illuminates the bourgeoning and evolving nature of cyberthreats to critical industries such as oil and gas from foreign state and nonstate actors. To mitigate these threats, oil and gas organizations must have a resourced program that recognizes individual anomalous behavior and responds in a way that evokes trust and leverages the workforce as a partner. Some best practices to mitigate insider threats include (National Counterintelligence and Security Center, 2021; Erola et al., 2022):

- Monitoring information and communications technology utilizing rule-based methods;

- Creating a security intelligence program to analyze threats and vulnerabilities to personnel, physical, and information disciplines;
- Conducting trend analysis of frequent security violations and patterns of "close call" incidents;
- Developing a communications plan to educate the workforce of security concerns;
- Integrating multiple organizational disciplines (human resources, wellness, information technology, etc.) into security planning and operations;
- Ensuring resources are available for cross-organization learning; and
- Staying current on internal and external threats (and looking over the horizon).

Oil and gas leaders must take responsibility for the institutional changes associated with the digital transition. They must establish risk levels and provide resources for human capital development aimed at enhancing institutional cybersecurity readiness (Prislan et al., 2020). Technological evolution and integration force operational and policy changes while simultaneously adding to existing employees' behavioral rules (Malimage et al., 2020). Cybersecurity automation technologies could enhance existing technological infrastructure defense systems and minimize cybersecurity risks with minimal human inputs. Unfortunately, this may energize fears that such automation technology will replace humans. The reality is that automation is meant to assist by automating repetitive and time-consuming tasks, not replace cybersecurity professionals. The recent enactment of the European Cybersecurity Act established a framework for integrating data-centric robots, but security vulnerabilities in robots are a serious concern for programmers and manufacturers, especially with sensitive oil and gas applications (Fosch-Villaronga and Mahler, 2021).

The response to evolving threats and modified policies potentially represents consistent interference to operational continuity, but it must occur for the safety of oil and gas technological infrastructure and data privacy. Leadership has a substantive part to play during the digitalization of oil and gas operations and could be the determining factor on whether or not an organization survives (Durmaz et al., 2022). The substratum to a successful CIA triad is employee conformance to established and modified information security policies emplaced to mitigate cyberattacks.

Conclusions

The oil and gas industry, like other large-scale industries that employ big data, is moving into cyberspace. This has many advantages such as unlimited storage space, on-demand computation resources, remote working capabilities, networking, etc. However, with these positive aspects comes an increased risk of cybersecurity breaches that could be catastrophic for individuals, companies, and entire countries. We discussed the main threats and how to mitigate them. It is important to emphasize that oil and gas institutions are critically important to national and global economies and thus cannot become stagnant regarding evolving cyberthreats and implementation of information security policies.

Data and materials availability

Data associated with this research are available and can be obtained by contacting the corresponding author.

Corresponding author: mrauchdavies@gmail.com

References

Aldridge, B., 2021, Does the pandemic explain recent spikes in cybercrime?: News & Observer, https://www.govtech.com/security/does-the-pandemic-explain-recent-spikes-in-cyber-crime, accessed 16 August 2022.

Atrews, R. A., 2020, Cyberwarfare: Threats, security, attacks, and impact: Journal of Information Warfare, **19**, no. 4, 17–28, https://www.jstor.org/stable/27033642, accessed 2 August 2022.

Atstāja, L., D. Rūtītis, S. Deruma, and E. Aksjoņenko, 2021, Cyber security risks and challenges in remote work under the Covid-19 pandemic: Proceedings of the 16th International Strategic Management Conference, https://doi.org/10.15405/epsbs.2021.12.04.2.

Ayoub, R., and C. Firth, 2021, How oil and gas security leaders can smooth the transformation path: Ernst and Young, https://www.ey.com/en_lu/oil-gas/how-oil-and-gas-security-leaders-can-smooth-the-transformation-path, accessed 2 August 2022.

Beer, E., 2022, EU terminals, oil storage hit by cyber attacks. Industry "caught napping": The Stack, https://thestack.technology/cyber-attacks-european-terminals-sea-invest-evos/, accessed 2 August 2022.

Ciancaglini, V., C. Gibson, D. Sancho, O. McCarthy, M. Eira, P. Amann, and A. Klayn, 2020, Malicious uses and abuses of artificial intelligence: Trend Micro Research, https://documents.trendmicro.com/assets/white_papers/wp-malicious-uses-and-abuses-of-artificial-intelligence.pdf, accessed 2 August 2022.

Costa, D., 2017, CERT definition of 'insider threat' — Updated: Carnegie Mellon University, Software Engineering Institute, https://insights.sei.cmu.edu/blog/cert-definition-of-insider-threat-updated/, accessed 2 August 2022.

Curry, D., 2022, Microsoft Teams revenue and usage statistics (2022), https://www.businessofapps.com/data/microsoft-teams-statistics/, accessed 16 August 2022.

Durmaz, O., S. S. Hawrami, and A. M. Hamasaeed, 2022, The suitable leadership for industry 4.0: Journal of Global Economics and Business, **3**, no. 8, 113–124, https://doi.org/10.31039/jgeb.v3i8.43.

Eling, M., M. Elvedi, and G. Falco, 2022, The economic impact of extreme cyber risk scenarios: North American Actuarial Journal, https://doi.org/10.1080/10920277.2022.2034507.

Erola, A., I. Agrafiotis, M. Goldsmith, and S. Creese, 2022, Insider-threat detection: Lessons from deploying the CITD tool in three multinational organisations: Journal of Information Security and Applications, **67**, 103167, https://doi.org/10.1016/j.jisa.2022.103167.

Fichtenkamm, M., G. F. Burch, and J. Burch, 2022, Cybersecurity in a COVID-19 world: Insights on how decisions are made: ISACA Journal, **2**, no. 1, 1–11.

Fosch-Villaronga, E., and T. Mahler, 2021, Cybersecurity, safety and robots: Strengthening the link between cybersecurity and safety in the context of care robots: Computer Law and Security Review, **41**, 105528, https://doi.org/10.1016/j.clsr.2021.105528.

IBM Security, 2021, Cost of a data breach report 2021, https://www.ibm.com/downloads/cas/OJDVQGRY, accessed 2 August 2022.

Jones, D., 2022, Oil and gas industry pledges cybersecurity cooperation at World Economic Forum: Utility Dive, https://www.utilitydive.com/news/oil-and-gas-industry-cyber-world-economic-forum/624518/, accessed 2 August 2022.

Kilovaty, I., 2022, Cybersecuring the pipeline. Houston Law Review, https://ssrn.com/abstract=4070074, accessed 2 August 2022.

Kolaczkowski, M., and A. White, 2022, Why do oil prices matter to the global economy? An expert explains: World Economic Forum, https://www.weforum.org/agenda/2022/02/why-oil-prices-matter-to-global-economy-expert-explains/, accessed 2 August 2022.

Lewis, J. A., 2020, Video conferencing technology and risk: Center for Strategic and International Studies, https://www.csis.org/analysis/video-conferencing-technology-and-risk, accessed 2 August 2022.

Malimage, K., N. Raddatz, B. S. Trinkle, R. E. Crossler, and R. Baaske, 2020, Impact of deterrence and inertia on information security policy changes: Journal of Information Systems, **34**, no. 1, 123–134, https://doi.org/10.2308/isys-52400.

Marzan, I., D. Martí, A. Lobo, J. Alcalde, M. Ruiz, J. Alvarez-Marron, and R. Carbonell, 2021, Joint interpretation of geophysical data: Applying machine learning to the modeling of an evaporitic sequence in Villar de Cañas (Spain): Engineering Geology, **288**, 106126, https://doi.org/10.1016/j.enggeo.2021.106126.

Mohammed, A. S., P. Reinecke, P. Burnap, O. Rana, and E. Anthi, 2022, Cybersecurity challenges in the offshore oil and gas industry: An industrial cyber-physical systems (ICPS) perspective: ACM Transactions on Cyber-Physical Systems, https://doi.org/10.1145/3548691.

Morgan, S., 2020, Cybercrime to cost the world $10.5 trillion annually by 2025: Cybersecurity Magazine, https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025/, accessed 2 August 2022.

National Counterintelligence and Security Center, 2021, Insider threat mitigation for U. S. critical infrastructure entities, https://www.dni.gov/files/NCSC/documents/nittf/20210319-Insider-Threat-Mitigation-for-US-Critical-Infrastru-March-2021updated-5Apr21b.pdf, accessed 16 August 2022.

Nygaard, M., and S. Mukhopadyay, 2020, Dragonstone Strategy — State of cyber security in the oil and natural gas sector: Lawrence Livermore National Laboratory, U.S. Department of Energy National Nuclear Security Administration, https://doi.org/10.2172/1602649.

Ollmann, G., 2008, Hacking as a service: Computer Fraud and Security, **2008**, no. 12, 12–15, https://doi.org/10.1016/S1361-3723(08)70177-5.

Prislan, K., A. Mihelič, and I. Bernik, 2020, A real-world information security performance assessment using a multidimensional socio-technical approach: PLoS ONE, **15**, no. 9, e0238739, https://doi.org/10.1371/journal.pone.0238739.

Progoulakis, I., N. Nikitakos, P. Rohmeyer, B. Bunin, D. Dalaklis, and S. Karamperidis, 2021, Perspectives on cyber security for offshore oil and gas assets: Journal of Marine Science and Engineering, **9**, no. 2, 112, https://doi.org/10.3390/jmse9020112.

Satyakee, S., S. Kainkaryam, C. Ong, and A. Sharma, SaltSeg: A β-variational autoencoder constrained encoder-decoder architecture for accurate geologic interpretation: 89th Annual International Meeting, SEG, Expanded Abstracts, 2493–2497, https://doi.org/10.1190/segam2019-3216875.1.

Schachinger, S., 2021, Colonial Pipeline cyberattack reveals economic impact of ransomware: Barracuda Corporate Blog, https://blog.barracuda.com/2021/05/12/colonial-pipeline-cyberattack-reveals-economic-impact-of-ransomware/, accessed 2 August 2022.

Statista, 2022, Number of cyber security incident reports by federal agencies in the United States from FY 2006 to 2018, https://www.statista.com/statistics/677015/number-cyber-incident-reported-usa-gov/, accessed 2 August 2022.

Tan, S., P. Xie, J. M. Guerrero, J. C. Vasquez, Y. Li, and X. Guo, 2021, Attack detection design for dc microgrid using eigenvalue assignment approach: Energy Reports, **7**, supplement 1, 469–476, https://doi.org/10.1016/j.egyr.2021.01.045.

Tanaka, G., T. Yamane, J. B. Héroux, R. Nakane, N. Kanazawa, S. Takeda, H. Numata, D. Nakana, and A. Hirose, 2019, Recent advances in physical reservoir computing: A review: Neural Networks, **115**, 100–123, https://doi.org/10.1016/j.neunet.2019.03.005.

TechAdvisory, 2021, A guide to implementing proactive cybersecurity measures, https://www.techadvisory.org/2021/10/a-guide-to-implementing-proactive-cybersecurity-measures/, accessed 2 August 2022.

Tsiostas, D., G. Kittes, N. Chouliaras, I. Kantzavelou, L. Maglaras, C. Douligeris, and V. Vlachos, 2020, The insider threat: Reasons, effects and mitigation techniques: PCI 2020: 24th Pan Hellenic Conference on Informatics, Association for Computing Machinery, 340–345, https://doi.org/10.1145/3437120.3437336.

U.S. Department of Homeland Security, 2014, Combating the insider threat, https://www.hsdl.org/?view&did=753189, accessed 2 August 2022.

U.S. House of Representatives, 2021, Cyber threats in the pipeline: Using lessons from the colonial ransomware attack to defend critical infrastructure: U.S. Government Publishing Office, https://www.govinfo.gov/content/pkg/CHRG-117hhrg45085/html/CHRG-117hhrg45085.htm, accessed 16 August 2022.

World Economic Forum, 2022, Global CEOs commit to collective action on cyber resilience, https://www.weforum.org/press/2022/05/global-ceos-commit-to-collective-action-on-cyber-resilience-ffa0ba5f56/, accessed 2 August 2022.

World Economic Forum, 2020, COVID-19 risks outlook: A preliminary mapping and its implications, https://www3.weforum.org/docs/WEF_COVID_19_Risks_Outlook_Special_Edition_Pages.pdf, accessed 2 August 2022.

Zhu, P., and J. P. Liyanage, 2021, Cybersecurity of offshore oil and gas production assets under trending asset digitalization contexts: A specific review of issues and challenges in safety instrumented systems: European Journal for Security Research, **6**, 125–149, https://doi.org/10.1007/s41125-021-00076-2.

Zuboff, S., 2019, The age of surveillance capitalism: The fight for a human future at the new frontier of power: PublicAffairs.