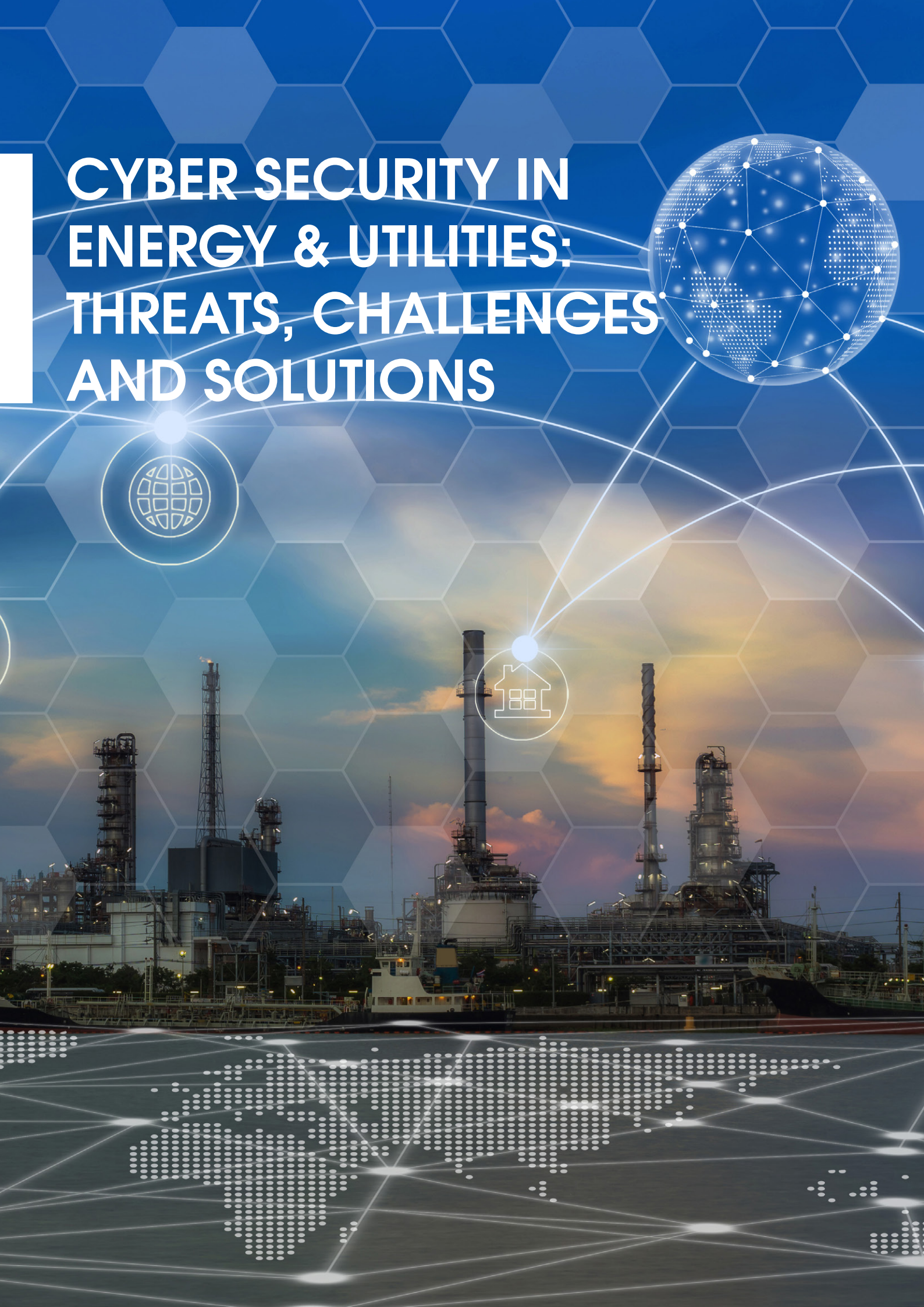
CYBER SECURITY IN ENERGY & UTILITIES: THREATS, CHALLENGES AND SOLUTIONS



"The current threat landscape involves all of the threat actors: Nation-states, hactivists, splinter groups, lone actors, and generic malware are all problems. Combine this with the insider threat and you see an industry that must rapidly evolve. Whether it be supply disruption, intellectual theft, financial gain, or reputational damage, energy and utilities companies must understand who they are fighting, what their motives are, the TTP (Techniques, Tactics and Procedures) that they employ, and the defences that must be in place to counter an attack." – Richard Byrd, director for Western US, Canada, Mexico and LATAM, Lockheed Martin

Cybercrime is steadily on the rise, both in terms of the frequency and severity of the threat it poses, to the point where it costs GCC businesses an estimated $1 billion annually.[1] The energy and utilities industry has acquired a growing target on its back for cybercriminals to aim at, as the technological sophistication of its infrastructure increases along with the economic and political value of its operations.[2]

In 2016, there were nearly 100 significant cyberattacks reported by oil and natural gas company leaders, with many more going unnoticed and/or unreported, costing an estimated $12.8 million in lost business and equipment damage. The industry is currently attracting around 25% of the GCC's annual cyberattacks, placing it roughly at the same at-risk level as the financial sector.

As the spectre of cybercrime rises and diversifies into new and troubling threat types, energy and utilities companies are retaliating by expanding their cybersecurity knowledge and capabilities. The Middle East cybersecurity market alone is estimated to attain growth at a CAGR of 22.5% from 2016-2022, and is expected to be valued at almost $10 billion by 2019.[3] To avoid incurring the significant costs of potential cyberattacks, companies must comprehend the current risk landscape and take the most appropriate measures to ensure adequate protection against it.

1 Albawaba, Cybercrimes cost GCC $1 billion a year, 23/02/2016
2 Albawaba, Cyber Attacks on the Rise in the Oil and Gas Industry: Experts, 04/10/2017
3 Markets Media, Cyber Security In Middle East 2017 Market Expected to Grow at CAGR 22.5% and Forecast to 2022, 20/11/2017

CRITICAL CYBERCRIME THREAT TYPES TO WATCH OUT FOR IN 2017-2018

Ransomware: By infecting devices and blocking access, cybercriminals can demand payment (increasingly in Bitcoin or other cryptocurrencies) from the owner to restore access. Energy and utilities companies are at risk due to the perception that they have the money and resources to pay the extortionists involved in ransomware.

Prominent examples: In February 2016, the WannaCry assault infected European hospitals and auto-plants, locking operators out of operating systems and stored data, demanding Bitcoin payments.[4] More recently, in mid-2017 the Petya ransomware type crippled the operations of Ukrainian banks, airports and government departments, while also spreading to the UK, Spain and Denmark. [5]

Data manipulation: A more subtle and insidious form of malware could be used to fake data about reserve levels of oil, gas, water, etc held by energy and utilities companies. For example, by manipulating data from field devices and tank management systems within the company's ERP systems, cybercriminals could make it appear that an oil company has far more oil than it actually currently carries, causing all manner of supply and logistical issues.[6]

Prominent examples: While no major instances of this type of cybercrime have been reported by the energy and utilities industry, the potential for this type of disaster remains pertinent to its ongoing cybersecurity efforts.

Plant and equipment damage: All energy and utilities assets contain a wide range of equipment and infrastructure types that are vulnerable to data manipulation and the reordering of processes by malicious actors. By hacking vulnerable systems, cybercriminals can change critical data values and commands to cause catastrophically destructive results.

Prominent examples: In August 2015, hackers attacked a steel mill in Germany by manipulating and disrupting control systems to such a degree that a blast furnace could not be properly shut down, resulting in massive damage.[7]

Total operational shutdown: Hackers have already demonstrated their ability to go beyond damaging equipment and locking users out from their systems, and are capable of completely shutting down operations through massive manipulation of key systems. Whether motivated by political or economic objectives, hackers possess the ability to invade and totally control entire facilities if they find sufficient vulnerabilities to be exploited.

Prominent examples: In January 2016, hackers caused the first ever recorded power outage via cyberattack by infecting a Ukrainian facility with BlackEnergy malware. This use of physically destructive malware follows the 2012 Saudi Aramco attack, which wiped 35,000 computers and disrupted operations for days.[8]

4 Houston Chronicle, Ransomware could easily pinch oil companies, experts say, 15/05/2017
5 The Telegraph, Petya cyber attack: Ransomware spreads across Europe with firms in Ukraine, Britain and Spain shut down, 27/06/2017
6 Forbes, Cyber Security Risks To Be Aware Of In The Oil And Gas Industries, 03/04/2017
7 Wired, A Cyberattack has caused confirmed physical damage for the second time ever, 01/08/2015
8 Financial Times, Hackers shut down Ukraine power grid, 06/01/2016

CYBERSECURITY CHALLENGES IN THE ENERGY AND UTILITIES INDUSTRY

Increasing technological sophistication of operations: Digitisation of processes affords the energy and utilities industry untold levels of operational efficiency and a host of attached benefits. However, utilities are becoming increasingly exposed, because connecting formerly standalone operational systems and their IT networks to the internet exposes them to malicious actors familiar with their systems. As more data is being produced, captured and analysed by vast sensory networks and increasingly sophisticated digital technologies, the opportunity for hackers to discover and exploit vulnerabilities also grows.

Loss of experienced workforce: The energy and utilities industry has masses of experienced employees poised to leave within the next few years. This problem is particularly acute in the oil and gas sector, where 50% of the industry's workforce is within five years of retirement. The loss of workers who are so familiar with existing infrastructure and key processes may pose an inherent challenge to effectively plugging cybersecurity vulnerabilities.[9]

Remaining compliant with evolving regulations: Due to the critical nature of the services provided by energy and utilities companies, there are increased expectations for the reporting of compliance with security and privacy directives being issued by policy-makers both domestic and international. Scrutiny of these policy-making bodies is likely to intensify in the wake of emerging high-profile cyberattacks and companies must be proactive in their approach to regulatory compliance.[10]

9 Eniday, Tackling the Cyber Threat, 14/06/2017
10 IBM, Best practices for cyber security in the electric power sector, August 2016

KEY SOLUTIONS AND STRATEGIES TO RECOGNISE AND IMPLEMENT

Embrace cybersecurity from the top-down: Senior leaders must be able to objectively measure the level of cybercrime risk that their company is exposed to, while actively supporting the accurate assessment of current cybersecurity capabilities in order to determine what vulnerabilities exist and how best to address them.[11] Without management buy-in, any cybersecurity initiative is doomed to ineffectiveness, budget overrun and/or complete failure.

Educate your workforce: Systems are only as secure as their human operators, who are often the weak link in the defensive chain. Phishing emails are estimated to be used in 92% of cyberattacks to obtain credentials and allow attackers into networks.[12] Regularly educate your employees about the current and emerging cyber threat types and develop a culture of personal cybersecurity regarding suspicious emails and attachments, BYOD (Bring your own device) best practices and general awareness of potential hacker activities employees may encounter at home and at work.[13]

Cognitive and AI technologies: The rising speed, frequency and range of cyberattacks facing the industry requires a quicker security response capable of responding to such threats in a way that simply outstrips the capacity of unaided human agents. Cognitive cybersecurity technologies can track and identify emerging threat patterns occurring around the world, making companies aware of their presence and helping to formulate effective countermeasures, all at a speed previously unthinkable. [14]

Leveraging big data: The corporate security perimeter has all but disappeared in recent years thanks to the growing adoption of cloud and mobile services, so cybersecurity has shifted from traditional perimeter protection to proactively monitoring and detecting emerging threats and malicious practices. Advanced analytics is the key element in this developing form of cyber resilience, since the detection of such threats requires the correlation of various data sources ranging, from server and application logs to network events and user activities.[15]

Third-Party and supply chain security: IoT and the cloud allows for greater seamless collaboration with third parties but also invites greater risk, as previously standalone processes are exposed to the internet. Utility companies should establish appropriate levels of security within the utility ecosystem by implementing comprehensive third-party and supply chain risk management programs that include standardised security requirements for all collaborators.

11 Ibid
12 BCG, Ensuring cybersecurity in the electric utility industry, 16/08/2017
13 PwC, Power and Utilities Cybersecurity and Privacy, 04/08/2017
14 Security Intelligence, Drilling for Answers: Cyberattacks on the Rise in the Oil and Gas Industry, 08/06/2017
15 Bi-Survey, Big Data Security Analytics: A Weapon Against Rising Cyber Security Attacks? December 2016

Sources:

https://www.forbes.com/forbes/welcome/?toURL=https://www.forbes.com/sites/forbestechcouncil/2017/04/03/cyber-security-risks-to-be-aware-of-in-the-oil-and-gas-industries/&refURL=&referrer=#64f501983f0a

https://www.albawaba.com/business/cyber-attacks-oil-and-gas-1029692

https://www.albawaba.com/business/14-cybersecurity-threats-watch-out-2017-909952

https://www.eniday.com/en/sparks_en/cyber-threat-oil-and-gas-industry/

https://securityintelligence.com/drilling-for-answers-cyberattacks-on-the-rise-in-the-oil-and-gas-industry/

https://www.offshoreenergytoday.com/top-10-cyber-security-threats-for-oil-and-gas-industry/

http://www.isssource.com/stuxnet-hit-4-oil-companies/

https://www.albawaba.com/business/cyber-crimes-cost-gcc-1b-year-808798

https://www.alliedmarketresearch.com/press-release/cyber-security-market.html

https://marketersmedia.com/cyber-security-in-middle-east-2017-market-expected-to-grow-at-cagr-22-5-and-forecast-to-2022/266918

http://www.houstonchronicle.com/business/article/Security-pros-warn-WannaCry-ransomware-could-11148101.php

https://www.rigzone.com/news/oil_gas/a/145887/ransomware_poses_potential_threat_to_oil_gas_cybersecurity/

https://www.rigzone.com/news/oil_gas/a/145887/ransomware_poses_potential_threat_to_oil_gas_cybersecurity/

https://www.wired.com/2015/01/german-steel-mill-hack-destruction/

https://www.ft.com/content/0cfffe1e-b3cd-11e5-8358-9a82b43f6b2f

https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/

http://www.telegraph.co.uk/news/2017/06/27/ukraine-hit-massive-cyber-attack1/

https://www.pwc.com/us/en/power-and-utilities/cyber-security.html

https://www.bcg.com/publications/2017/power-utilities-technology-digital-ensuring-cybersecurity-electric-utility-industry.aspx

https://www-935.ibm.com/services/multimedia/WR928534SF-Best_practices_for_cyber_security_in_the_electric_power_sector.pdf

http://www.govtech.com/library/papers/Leveraging-Big-Data-to-Drive-Cybersecurity-140617.html

https://bi-survey.com/big-data-security-analytics

CYBER SECURITY FOR ENERGY & UTILITIES

Join **DEWA, ADNOC, Saudi Aramco, Mubadala** and more at the **7th Cyber Security for Energy and Utilities** conference, taking place from **27-29 March 2018 at the Dusit Thani Hotel in Abu Dhabi**, to learn how you can protect your data, systems and ecosystem from the advancing nature of cyber threats and attacks.

Visit **cybersecurityme.iqpc.ae** for more information.