AlixPartners

Digital

FEBRUARY 2019

EMERGING RISKS:

Cybersecurity and the Internet of Things in oil and gas

The oil and gas industry faces technical challenges unique to its business, with hundreds of thousands of onshore and offshore wells distributed over wide geographic areas and thousands of miles of pipelines requiring continuous monitoring, periodic maintenance, and constant connectivity to ensure safety and optimized performance.

As new, Internet-enabled technologies emerge to help address the operating challenges in these environments, companies must consider carefully the emerging risk of significant cybersecurity breaches in order to avoid or minimize the monetary, reputational, and operational damage from such intrusions. While additional computational and networking capabilities will drastically change how businesses operate in the future, the tradeoffs inherent in deploying such technology must also be kept in mind.

The connectivity of all of our myriad devices, known as the Internet of Things (IoT), has advanced dramatically for corporations and households alike. Micro-sized devices, heavily equipped with electronic and networking components, are increasingly becoming embedded into our working and personal lives. While the consumer implications are broad and increasingly visible, businesses are also improving their processes with increased automation and advanced analytics that take advantage of concepts such as predictive maintenance or near-real time monitoring of infrastructure.

As we move from early adoption into general acceptance, the number of IoT devices continues to grow at an exponential rate.

Only three years ago, there were

15.41 BILLION

IoT devices connected worldwide now however, according to Statista, the

23.14 BILLION

devices installed in 2018 will grow to more than

75 BILLION BY 2025

There is little debate over the benefits that can be realized by using these devices. However, corporations often overlook critical security considerations when deploying new, cutting-edge technologies, and IoT devices are no exception. The importance of considering security implications may not always be clear in the initial deployment of such technologies, particularly when executives are focused on the opportunity to reduce costs and increase their bottom line.

Lacking security-related analysis, a breach on a connected device could allow hackers to steal data, disrupt operations, and impact production.

Seasoned adversaries will often seek entry on an unsecured connected device in order to expand their access to sensitive databases and file structures in other locations. Popular IoT device developers claim that the security protocols that their hardware utilizes are fully secure and, in some instances, 'future proof'. In reality, without adequate security practices in place to support their use, these devices may actually be easy to compromise, as demonstrated by the SANS Institute.[1] As a result, it is likely that many organizations have not adequately quantified the risk resulting from their growing reliance on IoT devices. Data breaches are in the news far too often, and companies are suffering major impacts to their stock value, reputation, or operating earnings as a result. These impacts are particularly acute in industries that require an always-on, always-functioning infrastructure, where any disruption can cost hundreds of thousands, if not millions, of dollars per incident.

In the news, we have seen examples of attacks focused on shutting down connected devices. Taiwan Semiconductor Manufacturing Company (TSMC), the world's largest manufacturer of semiconductors, was forced to take multiple plants offline in order to recover from an attack.[2] Saudi Aramco, one of the world's largest oil companies, suffered one of the largest hacks in history in 2012. The hack originated on a single computer that was connected to their larger IT infrastructure, wreaking havoc throughout the network. As a result of the breach, which affected approximately 35,000 computers, Saudi Aramco was forced to take a number of their operations offline and had to resort to the manual handling of supplies, shipping and contracts with governments and business partners.[3]

This leads to an interesting challenge in the oil and gas industry, where companies will be keen to harness the significant benefits that IoT devices bring but must simultaneously work to protect their infrastructure from the expanded attack surface presented by the same devices.

Within the past few years, upstream and downstream oil and gas companies have seen an evolution in the technology available to monitor and automate operations. Companies are implementing this new technology to reduce non-productive time (NPT) by integrating information and operational technology to speed up processing time, to enable predictive maintenance, and to reduce frequency of disruptive incidents. Additionally, to prevent/minimize disruption, companies typically supplement manual inspections with programmable logic controllers (PLCs) to control valves and satellite connections to remotely monitor equipment – greatly improving overall operating efficiency. While the operational benefits from such initiatives are easy to measure and report, the risks of inadequately protecting this expanded attack surface are not often considered fully – raising the specter of operational disruption and loss of key assets.

[1] In order to demonstrate the importance of proper security testing and design, SANS developed a series of straightforward exercises to demonstrate the relative ease of compromising a device leveraging the Thread protocol, a common IoT medium. SANS [https://www.sans.org/reading-room/whitepapers/internet/gorilla-deliver-assessing-security-googles-thread-internet-things-iot-protocol-38070]

[2] ZDNet [https://www.zdnet.com/article/tsmc-says-variant-of-wannacry-virus-brought-down-its-plants/]

[3] CNN [https://money.cnn.com/2015/08/05/technology/aramco-hack/index.html]

Operational disruption is not the only risk posed by insecure devices. As the energy industry is already heavily regulated, additional fines and repercussions are likely to be explored by regulators concerned about the systemic risk of a vulnerable infrastructure. The North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) protocol provides a set of requirements designed to better secure the assets that operate North America's bulk electric system. The protocol also stipulates the need for robust cyber capabilities to protect, detect, and recover all critical systems. Similarly, purchasing cyber insurance, while somewhat beneficial, is not a one-stop shop for mitigating fines and profit loss resulting from a cyber breach because residual mitigation and recovery efforts can continue to incur costs. And how do you quantify the potential, ongoing reputational and brand impact of such an incident?

Now the question becomes, what can organizations do to mitigate the risk stemming from this growing reliance on IoT devices? As technological capabilities evolve to more fully automated monitoring of operating conditions and to more advanced analytics and machine learning capabilities, security programs must also mature and enforce the concept of “security by design.” That is, IoT devices supporting communication and storage should have appropriate security layers in place. Sensitive data must be segmented from less secure networks, and any transmission of data over any network should be end-to-end encrypted. Security can’t be locked into the firmware, future-proofing requires upgradeable measures to address currently inconceivable new threats. Additionally, ongoing, real-time monitoring and automated incident alerting on IoT devices can enable timely response to any suspected compromise. Proper security testing, mimicking real-world scenarios, must include assurances that IoT devices and their supporting infrastructure are regularly scanned for vulnerabilities and upgraded when necessary. All these defensive measures need to be defined and documented, while driven by a security policy that aligns to both business and security objectives of the organization.

WHAT YOU NEED TO KNOW:

1. While the use of IoT devices within industry are growing exponentially, for all the cost cutting and strategic benefits they provide, these devices, and their connections to the internet, are not inherently secure.

2. A breach of a connected device has the potential for exponential damage as the impact traverses industrial and IT systems to which it connects.

3. The solution is to plan ahead, to consider security throughout the design, and to monitor in real time (security-by-design and defense-in-depth).

4. New cyber laws and regulations are being implemented on a nearly continual basis, reflecting an increased focus on the risks that unsecured connected devices can pose.

AlixPartners

CONTACT THE AUTHORS:

Gretchen Ruck
Director
+1 646 428 9185
gruck@alixpartners.com

Richie Stark
Vice President
+1 202 756 9078
rstark@alixpartners.com

FOR MORE INFORMATION CONTACT:

Bill Ebanks
Managing Director
+1 713 276 4919
bebanks@alixpartners.com

David Head
Managing Director
+1 248 262 8453
dhead@alixpartners.com

ABOUT US

For nearly forty years, AlixPartners has helped businesses around the world respond quickly and decisively to their most critical challenges – circumstances as diverse as urgent performance improvement, accelerated transformation, complex restructuring and risk mitigation.

These are the moments when everything is on the line – a sudden shift in the market, an unexpected performance decline, a time-sensitive deal, a fork-in-the-road decision. But it's not what we do that makes a difference, it's how we do it.

Tackling situations when time is of the essence is part of our DNA – so we adopt an action-oriented approach at all times. We work in small, highly qualified teams with specific industry and functional expertise, and we operate at pace, moving quickly from analysis to implementation. We stand shoulder to shoulder with our clients until the job is done, and only measure our success in terms of the results we deliver.

Our approach enables us to help our clients confront and overcome truly future-defining challenges. We partner with you to make the right decisions and take the right actions. And we are right by your side. When it really matters.

The opinions expressed are those of the author and do not necessarily reflect the views of AlixPartners, LLP, its affiliates, or any of its or their respective professionals or clients. This article regarding Emerging risks: cybersecurity and the Internet of Things in oil and gas ("Article") was prepared by AlixPartners, LLP ("AlixPartners") for general information and distribution on a strictly confidential and non-reliance basis. No one in possession of this Article may rely on any portion of this Article. This Article may be based, in whole or in part, on projections or forecasts of future events. A forecast, by its nature, is speculative and includes estimates and assumptions which may prove to be wrong. Actual results may, and frequently do, differ from those projected or forecast. The information in this Article reflects conditions and our views as of this date, all of which are subject to change. We undertake no obligation to update or provide any revisions to the Article. This article is the property of AlixPartners, and neither the article nor any of its contents may be copied, used, or distributed to any third party without the prior written consent of AlixPartners.