The State of Cybersecurity in the Oil & Gas Industry: United States

EXECUTIVE SUMMARY

Sponsored by Siemens

Independently conducted by Ponemon Institute LLC

Publication Date: February 2017

The State of Cybersecurity in the Oil & Gas Industry: United States
Executive Summary
Presented by Ponemon Institute: February 2017

Ponemon Institute is pleased to present the results of *The State of Cybersecurity in the Oil & Gas Industry: United States* sponsored by Siemens. The purpose of this research is to understand how companies in the oil and gas industry are addressing cybersecurity risks in the operational technology (OT) environment.

According to the findings, the deployment of cybersecurity measures in the industry isn't keeping pace with the growth of digitalization in oil and gas operations. In fact, just 35 percent of respondents rate their organization's OT cyber readiness as high. With most respondents describing their organization as having low to medium cybersecurity readiness, 68 percent of respondents say their operations have had at least one security compromise in the past year, resulting in the loss of confidential information or OT disruption.

Following are eight key findings in this research.

1. Fifty-nine percent of respondents believe there is greater risk in the OT than the IT environment and 67 percent of respondents believe the risk level to industrial control systems over the past few years has substantially increased because of cyber threats.

2. Oil and gas companies are benefiting from digitalization, but it has significantly increased cyber risks, according to 66 percent of respondents.

3. Sixty-eight percent of respondents say their organization experienced at least one cyber compromise, yet many organizations lack awareness of the OT cyber risk criticality or have a strategy to address it.

4. Sixty-one percent of respondents say their organization's industrial control systems protection and security is not adequate.

5. Sixty-five percent of respondents say the top cybersecurity threat is the negligent or careless insider and 15 percent of respondents say it is the malicious or criminal insider— underscoring the need for advanced monitoring solutions to identify atypical behavior among personnel.

6. Only 41 percent of respondents say they continually monitor all infrastructure to prioritize threats and attacks. In fact, an average of 46 percent of all cyber attacks in the OT environment go undetected, suggesting the need for investments in technologies that detect cyber threats to oil and gas operations.

7. Sixty-eight percent of respondents say security analytics is essential or very important to achieving a strong security posture.

8. Security technologies deployed are not considered the most effective. Sixty-three percent of respondents say user behavior analytics and 62 percent of respondents say hardened endpoints are very effective in mitigating cybersecurity risks. In addition, 62 percent of respondents say encryption of data in motion is considered very effective. Yet, many companies do not have plans to deploy these technologies. Specifically, in the next 12 months less than half of organizations represented (48 percent of respondents) plan to use encryption of data in motion, only 39 percent plan to deploy hardened endpoints and only 20 percent will adopt user behavior analytics (UBA).

Part 2. Analysis of key findings

Profile of participants in this research

We surveyed 377 individuals in the United States who are responsible for securing or overseeing cyber risk in the OT environment[1]. Most of these individuals report to the head of industrial control systems (19 percent), head of quality engineering (15 percent), OT security leader (14 percent), head of process engineering (14 percent) and IT security leader (11 percent). Respondents work in the downstream (30 percent), upstream (24 percent), middle stream (17 percent) or all of these environments in the oil and gas industry (29 percent).

We have organized the findings according to the following topics:

- Challenges to cyber readiness
- Exploits & security breaches
- Digitization in the oil & gas industry
- Solutions to achieve cyber readiness

Challenges to cyber readiness

OT is at greater risk than the IT environment. Fifty-nine percent of respondents believe there is a greater risk in the OT than the IT environment. Sixty-seven percent of respondents believe the risk level to industrial control systems over the past few years has substantially increased because of cyber threats.

Cyber risks, especially across the supply chain, are difficult to address. Sixty-nine percent of respondents believe their organization is at risk because of uncertainty about the cybersecurity practices of third parties in the supply chain and 61 percent say their organization has difficulty in mitigating cyber risks across the oil and gas value chain**.**

Many companies are not prepared for cyber exploits and security breaches. Only 35 percent of respondents rate their organization's cyber readiness in the OT environment as high and 61 percent of respondents say their organization's industrial control systems protection and security is not adequate.

These perceptions are based on the following findings: 61 percent of respondents believe their organization has difficulty in mitigating cyber risks across the oil and gas value chain and less than half (48 percent) of respondents believe their organization is effective in achieving compliance with security standards and guidelines in the oil and gas industry.

Organizational challenges affect cybersecurity readiness. Only 33 percent of respondents believe there is full alignment between OT and IT with respect to cybersecurity operations. Sixty percent say they do not have enough staff and only 45 percent of respondents say they have the internal expertise to manage cyber threats in the OT environment.

Together negligent and malicious or criminal insiders pose the most serious threat to critical operations. Sixty-five percent of respondents say the top cybersecurity threat is the negligent or careless insider and 15 percent of respondents say it is the malicious or criminal insider.

---

[1] This US sample is part of a larger global study involving 1,092 qualified respondents in Europe, Middle East, Asia-Pacific and Americas.

Exploits & security breaches

Cyber attacks in the OT environment go undetected. Sixty-eight percent of organizations have suffered a security compromise that resulted in the loss of confidential information or disruption to operations in the OT environment over the past 12 months. However, on average, 46 percent of cyber attacks are believed by respondents to go undetected.

Many organizations seem to lack awareness about the cyber risks to their organization. While 68 percent of respondents say their organization experienced a cyber compromise, only 20 percent of respondents say it is very likely or likely their organization will experience a successful cyber exploit over the next 12 months. Only 20 percent of respondents say their organization experienced the DUOU, DUOU 2.0 or Flame virus/worm over the past 12 months.

Tasks intended to secure OT infrastructure are not completed. Only 41 percent of respondents say they continually monitor the OT infrastructure to prioritize threats and attacks. Fewer respondents say their organization is able to assess risks to determine resources necessary to address the risks or pinpoint sources of attacks and mobilize the right set of technologies and resources to remediate the attack, according to 38 percent and 37 percent of respondents, respectively.

Exploratory information is the area most vulnerable in the oil and gas value chain to a cyber attack. When asked to identify the top seven areas of greatest risk, 72 percent of respondents say it is exploratory information and 60 percent of respondents say it is production information. Also vulnerable are: potential partners and acquisition targets (56 percent of respondents), financial and organizational reports (53 percent of respondents), operational information (50 percent of respondents), details on drilling sites (47 percent of respondents) and field production information from sensors (46 percent of respondents). Only 18 percent of respondents say their organization conducts comprehensive audits every month (7 percent of respondents) and every six months (11 percent of respondents).

Digitization in the oil & gas industry

Migration to the digital oil field has benefits and risks. Oil and gas companies are benefiting from digitization. However, 66 percent of respondents are concerned that it has made them more vulnerable to security compromises. These increases have made organizations more aware of the need to have security analytics. Sixty-eight percent of respondents say this technology is essential or very important.

The biggest vulnerability to organizations is outdated and aging control systems in facilities. Sixty-three percent of respondents say outdated and aging control systems in facilities put organizations at risk. Also vulnerable are using standard IT products with known vulnerabilities in the production environment (61 percent of respondents).

Most organizations are in the early to middle stages of OT cybersecurity maturity. Forty-one percent of respondents say their organizations are in the early to middle stage of maturity with respect to their cyber readiness. This means many OT cybersecurity program activities have not as yet been planned or deployed or they have been planned and defined but only partially deployed.

Many organizations are outsourcing OT security operations. To support their efforts in addressing the heightened risk created by digitization, 52 percent of respondents say their organization currently outsources (16 percent of respondents) or would consider outsourcing its OT security operations (36 percent of respondents).

Solutions to achieve cyber readiness

Security technologies deployed are not considered the most effective. Sixty-three percent of respondents say user behavior analytics and 62 percent of respondents say hardened endpoints are very effective in mitigating cybersecurity risks. In addition, 62 percent of respondents say encryption of data in motion is considered very effective. Yet, many companies do not have plans to deploy these technologies. Specifically, in the next 12 months less than half of organizations represented (48 percent of respondents) plan to use encryption of data in motion, only 39 percent plan to deploy hardened endpoints and only 20 percent will adopt user behavior analytics (UBA).

Sharing of threat intelligence is considered valuable in reducing cyber threats. Critical to reducing cyber risks in the OT environment is the sharing of threat intelligence, according to 71 percent of respondents. However, only 43 percent of respondents say they participate in the Oil & Natural Gas Information Sharing and Analysis Center. The primary reasons for not sharing are concerns about the quality of threat information (56 percent of respondents) and insufficient resources (53 percent of respondents).

Operational solutions should focus on alignment between OT and IT and in-house expertise. As shown in this research, organizational challenges create difficulty in enhancing OT security. Only 33 percent of respondents say there is full alignment between OT and IT with respect to cybersecurity operations and only 45 percent of respondents say their organization has the internal expertise to manage cyber threats. Cybersecurity training and awareness of employees is critical because 60 percent of respondents say their organizations do not have such initiatives in place.

Caveats to this study

There are inherent limitations to survey research that need to be carefully considered before drawing inferences from findings. The following items are specific limitations that are germane to most Web-based surveys.

- Non-response bias: The current findings are based on a sample of survey returns. We sent surveys to a representative sample of individuals, resulting in a large number of usable returned responses. Despite non-response tests, it is always possible that individuals who did not participate are substantially different in terms of underlying beliefs from those who completed the instrument.

- Sampling-frame bias: The accuracy is based on contact information and the degree to which the list is representative of OT and IT security practitioners who are familiar with their organizations use of security analytics. We also acknowledge that the results may be biased by external events such as media coverage. Finally, because we used a Web-based collection method, it is possible that non-Web responses by mailed survey or telephone call would result in a different pattern of findings.

- Self-reported results: The quality of survey research is based on the integrity of confidential responses received from subjects. While certain checks and balances can be incorporated into the survey process, there is always the possibility that a subject did not provide accurate or truthful responses.

Ponemon Institute
Advancing Responsible Information Management

Ponemon Institute is dedicated to independent research and education that advances responsible information and privacy management practices within business and government. Our mission is to conduct high quality, empirical studies on critical issues affecting the management and security of sensitive information about people and organizations.

As a member of the **Council of American Survey Research Organizations (CASRO)**, we uphold strict data confidentiality, privacy and ethical research standards. We do not collect any personally identifiable information from individuals (or company identifiable information in our business research). Furthermore, we have strict quality standards to ensure that subjects are not asked extraneous, irrelevant or improper questions.