CENTRE FOR INTERNATIONAL AND DEFENCE POLICY

BRIEFING NOTE **FOR INFORMATION**

SUBJECT: Cyber Security and the Extractive Sector

Cyber-crime is a rising concern for mining companies, with instances of hacking and information ransoming increased each year.[1] A 2013 cyber-security survey conducted by *EY* found that 41% of extractive industry respondents experienced an increase in external cyber threats over the past 12 months, with a further 28% experiencing an increase in internal vulnerabilities over the same period. The survey highlighted the following four vulnerable security areas in the extractive industry that can increase the risk of cyber-attacks.

1. **Centralization of operations**: Many companies are centralizing their operations to decrease costs along the supply chain, leading to more sophisticated IT systems and network infrastructures to connect workforces in different areas. Centralization of information assets and databases has increased the company's reliance on the internet, creating a potential pathway for external actors to access sensitive company information. This security issue is compounded given that centralization of information assets has integrated Operations and Information Technologies together, providing these external actors access to a broader range of company assets that they would have not enjoyed in the past.
2. **Government cyber-attacks**: There has been an increase in government sponsored cyber-attacks, either through direct action or unofficial affiliates, which poses a significant security risk to extractive companies. While under the guise of passive collection to assist in policy direction or national or state-owned company negotiations, government cyber-attacks can be aggressive and disrupt a company's operations. Furthermore, governments are able to invest heavily into cyber attacks with very little repercussions, especially in regions with underdeveloped legal institutions or intellectual property protections.
3. **Informal Activists**: Activists use cyber-attacks against mining companies when they feel that their interests have not been adequately satisfied by government or company policies. These attacks usually seek to disrupt a company's activities, expose confidential information to the public, and disrupt communications.
4. **Formal Security Protections**: Almost half of the respondents indicated that they did not have formal security systems in place to deal with cyber-attacks, with a majority of respondents indicating that they only had an informal system in place. These informal

---

[1] "Get ahead of cybercrime: EY's Global Information Security Survey 2014: Insights on governance, risk and compliance." *EY* (October 2014). http://www.ey.com/Publication/vwLUAssets/EY-global-information-security-survey-2014/$FILE/EY-global-information-security-survey-2014.pdf

systems only protect certain areas of the company's operations, and mainly operate reactively rather than proactively, to deal with cyber-security threats.

There are a variety of recommendations included in the survey to help deal with cyber-related security issues and address the four issue areas including; increasing the management importance of information security, integrating a security strategy and protocol that adheres to corporate objectives and considers the entirety of the current and future risk. To help achieve these recommendations the report outlines various operational directions, such as increasing budgets for cyber-security, create a specialized team to develop a security program, as well as constantly stay up to date with cyber-attack strategies through research and analytics to ensure consistent protection.

For more information please contact;

David Walsh-Pickering
Researcher | Centre for International and Defence Policy (CIDP)
Queen's University
138 Union Street, Kingston, Ontario, Canada K7L 3N6
Tel: (514) 980-0999
Email: d.walsh-pickering@queensu.ca
Website: www.queensu.ca/cidp