Potential Cyber-attacks against Global Oil Supply Chain

M Ali Nasir

Introduction

* Global supply chain's role in today's world
* decentralization and outsourcing increases numbers of exposure points
* information sharing with associates is indispensable but it also escalates the risk of it being compromised
* global supply chains (such as energy sector) are so complex that it is difficult to even assess the risk of compromised information at every stage

Cont.

* Cyber-attack on supply chain is the most destructive way to damage many linked entities at once due to its ripple effect. Significant examples are stuxnet, Shamoon and night dragon etc.

* Quantity and sophistication of cyber-attacks on global energy sector are increasing day by day.

* malicious entities are targeting energy sector so as to attain political outcomes, cause financial losses or at worst end up in mass human causalities

LITERATURE SURVEY

* high level of information sharing, automation and integration is required in a supply chain

* Information sharing is also the most sensitive part of SC and many organizations are unwilling to share even relevant information out of fear of information leakage, lack of trust, malicious individuals to misuse that information etc.

* SC security has become a major concern in a global market so it is the need of the hour to identify, assess and mitigate the loopholes that aid cyber-attacks

Cont.

* utilities (electricity, water, energy) SC have the most critical infrastructure because of their billions of users worldwide and as their infrastructure is constructed on a complex system known as the “Supervisory Control and Data Acquisition” (SCADA).

* global supply chains are vulnerable to cyber-attacks, which if not mitigated properly can result in to losses at high scale

CYBER-ATTACKS AGAINST OIL SUPPLY CHAINS

* Energy sector is data driven and malicious entities are targeting existing vulnerabilities to gain access to critical information as well as sensitive financial data

* Individuals targeting it range from casual hackers to organized trained terrorists, highly skilled intelligence agencies to employees with privileged access, and attacks vary from cyber espionage to casual hacks

* Cyber-attacks on oil SC can be broadly categorized into two groups;

I. Cyber Espionage
II. Disruption of critical business or physical operations by attacks on network

Cont.

* Global SCs are certainly getting dependent on automation technology for its timely and efficient depiction of end to end product delivery but this is also making them more vulnerable and attack prone

* Threats like these can lead to major environmental damage, leakage of confidential information, data corruption in geological surveys, power outages for long periods of time etc.

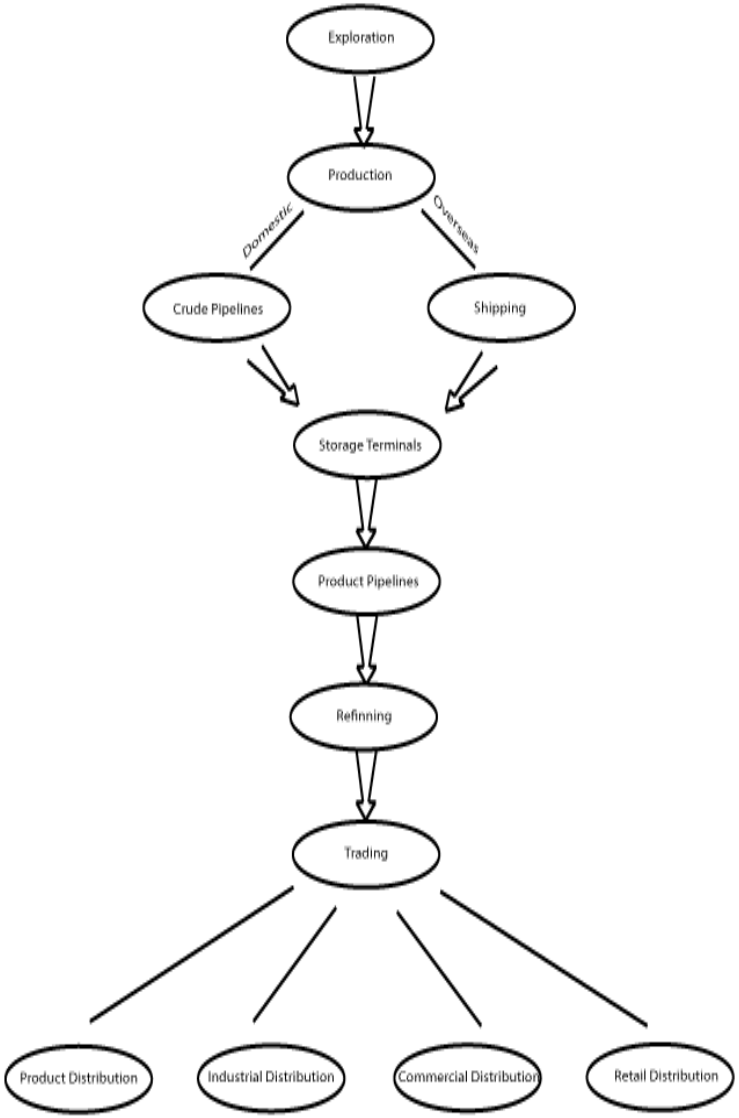
Cont.

* energy sector has faced more targeted attacks than any other business

* different companies have collectively lost approximately 600 billion dollars in intellectual property theft

* Globally more than 50% of cyber-attacks on critical infrastructure resources in 2012 were targeted at energy sector. The forthcoming cost of such attacks will touch $1.87 billion by 2018.

GLOBAL OIL SUPPLY CHAIN



SOLUTIONS AND RECOMMENDATIONS

Department	Potential cyber threats	Countermeasures
Exploration Facility	1. Information leakage 2. Social engineering 3. Inference attacks (sensitive information extracted from non-sensitive data) 4. Malicious insiders	1. Suitable Access Control policy , 2. Periodic Facility monitoring, 3. Security training of employees on information sharing

Cont.

Department	Potential cyber threats	Countermeasures
Production Facility	1. Infiltration through infected device, 2. Confidentiality breach of critical information such as power usage, threshold temperature and voltage values etc.	1. Internal network should be separated form internet, 2. no remote flash or hard drives in or out of facility, 3. Periodic monitoring of values, 4. Efficient & reliable alert reporting mechanism for safety hazards

Cont.

Department	Potential cyber threats	Countermeasures
Information and Communication Management	1. Data management 2. Protection of IP 3. Spear-phishing 4. Default passwords 5. Loss or falsification of different kind of Logs	1. Conduct cyber threat analysis 2. Regular information audits 3. Data Loss Prevention technology 4. Secure Data exchange architecture 5. Business partners evaluation systems w.r.t. to secure information sharing

Cont.

Department	Potential cyber threats	Countermeasures
Crisis Management & Disaster Recovery	1. Inappropriate Business continuity plan 2. Irresponsive Incident management 3. Absence of data loss prevention, detection and recovery techniques	1. Penetration testing 2. Periodic risk assessments 3. Incident response team 4. Regular information audits 5. Storage & review of e-mail or computer files 6. Onsite first responders trained to handle digital evidence

FUTURE RESEARCH DIRECTIONS

* This paper presents the groundwork to build a framework for identification and to minimize cyber risks in global supply chain; next step is mitigation of identified threats with customizable security policies and appropriate measures for prevention of cyber-attacks from damaging as less as possible.

Conclusion

* Energy sector is considered to be most nourishing for hackers for different purposes, securing energy sector is a top priority as a lot is at stake from environment to human lives, money to political influences; needs to be handled very carefully.

* identified potential exposure points or attacks that can be made on an oil supply chain and how they can be mitigated.

* It is very necessary to assess and analyze cyber vulnerabilities at every step of SC because of its ripple effect; if they are properly identified they can be suitably dealt with.

References

* Albert Y. Ha, Shilu Tong; (2008), contracting and Information Sharing Under Supply Chain Competition, International journal of Management Science, vol. 74, pg. 701-715
* Bronk, C. (2014). Hacks on gas: Energy, cyber security, and U.S. defense; *Baker Institute for Public Policy.* Retrieved from: https://bakerinstitute.org/research/hacks-gas-energy-cybersecurity-and-us-defense/
* Byers, E. (2013); Next generation cyber-attacks target oil and gas SCADA. *Pipeline & Gas Journal;* Retrieved from: http://www.pipelineandgasjournal.com/next-generation-cyber-attacks-target-oil-and-gas-scada
* Christopher R. Moberg, Bob D. Cutler, Andrew Gross, Thomas W. Speh, (2002) "Identifying antecedents of information exchange within supply chains", International Journal of Physical Distribution & Logistics Management, Vol. 32 Iss: 9, pp.755 – 770
* Clayton, B. & Segal, A. (2013), addressing cyber threats to oil and gas suppliers; *Council on Foreign Relations.* Retrieved from: www.cfr.org
* KPMG; (2014), Energy at risk study of IT security in the Energy and Natural Resources. Retrieved from: http://www.kpmg.com/Global/en/IssuesAndInsights/ArticlesPublications/Documents/energy-at-risk.pdf