IEF-PILLSBURY ROUNDTABLE: CYBERSECURITY IN THE GLOBAL ENERGY SECTOR

AN INTERNATIONAL ENERGY FORUM PUBLICATION

9 OCTOBER 2014

CONTENTS

KEY INSIGHTS........2

1. EVENT BACKGROUND........3

2.UNDERSTANDING THE THREAT: TARGETS........3

3. UNDERSTANDING THE THREAT: SOURCES OF VULNERABILITY......4

4. ADDRESSING THE CHALLENGE........5

Education and training........5

Organisational governance and processes........6

Technologies........6

Laws and regulations........7

Risk-pricing and liability allocation........7

Information sharing........7

Coordination........8

5. CONCLUSIONS AND NEXT STEPS........8

KEY INSIGHTS

- Private information, intellectual property, industrial property and energy networks are all vulnerable to cyber-attacks.
- The nature of cyber-threats changes constantly, presenting an unprecedented challenge in terms of complexity and potential response strategies.
- To date, neither industry nor government has responded to the cybersecurity challenge to the point where hackers are kept in check.
- Contrary to the intuitive focus on information technologies, it is often the people working inside organisations that are at the core of vulnerabilities in the digital realm.
- Employees at all levels require greater awareness of the risks from cyber-threats and appropriate training to mitigate them.
- A “Maginot Line” defense, intended to stop threats before they enter an organisation, is of limited value. Breaches will occur. Resilience is key.
- There is a labour shortage in the fight against cyber-threats. Private enterprise can play a leadership role in addressing it.
- The traditional Chief Information Officer may not be the right person to address the growing list of cyber-threats. Specialised security teams, with a much broader range of complementary and specialist skills in various subjects, may be needed.
- CEOs and company boards of directors must take a close, active, and supportive interest in the activities of their cybersecurity teams, not least because investors are paying more attention to this component of corporate strategy when valuing firms.
- Organisations must ensure that standards and procedures for the up-keeping, upgrading and updating of the hardware and software in their information systems are in place, understood and adhered to by all personnel.
- The fluid nature of cybersecurity challenges may render useless any attempt to impose rigid regulation to control them.
- Companies that are able to demonstrate that they have certain cybersecurity practices in place should expect to pay lower cyber-insurance premiums.
- Information sharing at both the domestic and international levels is a central defence strategy already practiced by the hacking community.
- Existing governmental institutions and industry bodies can be tasked with the coordination of strategic courses of action, rather than creating new bodies for this purpose.

1. EVENT BACKGROUND

In the information age, oil and gas supply chains and electricity generation and transmission systems are as vulnerable to sabotage over the Internet as by direct physical attacks on facilities. The widely publicised 2010 Stuxnet attack on industrial installations in Iran, including a uranium enrichment facility, proved that cyber-threats can result in damage to critical physical infrastructure. The 2011 Night Dragon hacking of project finance and intellectual property data in the global oil and gas sector, and the 2012 Shamoon "malware" (malicious software) that reportedly infected and deleted the hard-drives of tens of thousands of computers at Saudi Aramco and other energy companies, both demonstrated the destructive potential of relatively crude yet targeted attacks. These examples highlight the progression of cyber-threats to the energy industry, from the realm of science fiction to stark reality.

To promote a better understanding of these new types of threats and attacks, the International Energy Forum and law firm Pillsbury Winthrop Shaw Pittman LLP organised a one-day event in Washington DC entitled "Cybersecurity in the Global Energy Sector", wherein roughly 100 participants sought to explore developing US and international trends and standards in cybersecurity. [1]

Cybersecurity refers to the practice of ensuring the integrity of electronic information, communications and control systems common to almost every sector of the modern digital economy. Today's energy systems and marketplaces are increasingly interconnected and interdependent, making cybersecurity a matter of paramount importance to national and international energy security.

This brief note is meant to help focus the lens on some of the core issues inherent in coping with the cybersecurity challenge. The usual but important disclaimer applies to this as to all International Energy Forum dialogue reporting: none of the insights presented herein should be interpreted as representing the position of the IEF on this subject, nor can they be attributed to any individual. They arose from the informal and open exchange of ideas among the roundtable participants and are presented here in condensed form.

2.UNDERSTANDING THE THREAT: TARGETS

Cyber-attacks pose two main types of threats to the energy sector, which can be distinguished according to their two principal targets: the organisation and the energy system. Threats at the organisation level involve employees who lack awareness or training on cyber-security, or hackers (internal or external) seeking to steal private information, intellectual property, or affect industrial property of strategic significance. The motivation may range from the purely recreational, especially if the hacker is a

[1] Featured speakers included the Honourable William C Ostendorff, Commissioner of the US Nuclear Regulatory Commission; Joseph H McClelland, Director of the Office of Energy Infrastructure Security at the US Federal Energy Regulatory Commission (FERC); Chad Fulgham, former Chief Information Officer of the US Federal Bureau of Investigation; and thought-leaders from the Atlantic Council, IBM, Mandiant Corporation, Marsh, Protiviti, Red Owl Government Analytics, Wipro, and numerous other companies and government agencies.

private individual, to the more sinister of accessing financial resources or interfering with company or government operations. In the latter case, hackers may be operating on their own or as part of an organisation, legal or illegal, public or private.

Threats at the level of the national energy system result from attacks that seek to interfere with the operation of integrated energy networks. Their aim is to cause direct harm to equipment or processes and disrupt the provision of energy products and services to populations at large. This is an area of increasing concern in the energy sector because of the growing use of electronic systems managed through Internet-connected controls, which provide an ever-expanding number of access points for malicious hackers to exploit.

Both sets of threats are related. An attack that stops the flow of oil, gas or electricity from one facility can be felt system-wide owing to the multiple interconnections through transmission lines, pipelines, satellite connections, and other electronic links. A disruption to a refinery in one country can affect operations of an oil supplier in another. Large corporations may have robust cyber-security defences, but smaller business partners or firms in their supply chain may not be as well protected. Hackers would target the weakest link (small players) that would provide them with access to the primary target (large players) or that would interrupt its operations. It would therefore be a mistake to think of cybersecurity in terms of purely isolated incidents whose impact is limited only to larger organisations.

To complicate matters further, the nature of cyber-threats changes constantly, presenting an unprecedented challenge in terms of complexity and potential response strategies. Hackers are nimble, technologically sophisticated and highly motivated by the prospects of financial, political, or other rewards. To date, neither industry nor government has addressed the cybersecurity challenge to the point where hackers are kept in check. While experts believe that cybersecurity is finally gaining the attention it deserves in some corporate boardrooms, a comprehensive understanding of cyber-threats among key stakeholders is generally lacking. Roughly 85% of security breaches today occur because victim companies did not have adequate policies or controls in place.

3. UNDERSTANDING THE THREAT: SOURCES OF VULNERABILITY

Contrary to the intuitive focus on information technologies when thinking about cyber-security, it is the people working inside organisations, not outside hackers or malicious actors, who are at the core of vulnerabilities in the digital realm. It is estimated that 60% of data that leaves organisations does so through employees, either passively, for example through the opening of infected email, or actively, by taking some of a company's intellectual property with them when they resign or change jobs. The incident involving Edward Snowden is perhaps the most devastating example of an inside cyber-attack to date that resulted in the unauthorised release of private or confidential information.

Likewise, the main conduit for the penetration of malware into an organisation is not necessarily a direct attack by hackers, but a lack of awareness or care on the part of employees--at all levels—in using their company's computers and networks. Clicking on internet links, downloading documents, bringing in external memory drives and other activities that are common to the daily routines of the members of any organisation can be the action that, inadvertently, opens the gates to a cyber-attack.

A "Maginot Line" defense, intended to stop threats before they enter an organisation, may therefore be of limited value, a reality amplified by the fact that 70% of malware in use today is used just once. Defences built for multiple incidents, or "one size fits all" strategies, do not address the true nature of the threat, which combines internal vulnerabilities with external and evolving inventiveness from hackers.

4. ADDRESSING THE CHALLENGE

There are at least seven areas where people in organisations and governments can work to reduce the vulnerability of the energy sector to cyber-attacks:

- Education and training
- Organisational governance and processes
- Technology
- Laws and regulations
- Risk-pricing and liability allocation
- Information sharing
- Coordination

Education and training

Professionals working in organisations require greater awareness of the risks from cyber-threats and appropriate training to mitigate them. As mentioned above, threats inside a company or organisation are often more daunting than those lurking outside – and addressing them requires both technological and cultural change. Employees can be trained to identify malicious email, websites or other threats, raising the probability that they will avoid a click that could open the door to attack. Employee access to sensitive data should also be tracked and limited.

There is a labour shortage in the fight against cyber-threats, as well as an imbalance between the capacity of the public and private sectors--as industry often pays better than government. This creates an opportunity for private enterprise to play a leadership role on the cybersecurity front. For government, the idea of employing specialist contractors holds some interest because it offers flexibility in an area that is constantly changing. However, there is a potential risk that a small group of private firms may end up dominating the global market for cybersecurity services, which may raise yet another set of risks.

Organisational governance and processes

Recent data show that cybersecurity is rising in importance on the list of priorities of both public and private sector market actors. Cybersecurity appears to be a topic of considerable concern to some CEOs and Ministers, though many still view it as an IT matter that should remain under the sole purview of the Chief Information Officer (CIO). This presents challenges, as often the CIO is not in the top tier of management and has a natural propensity for focusing on technical solutions only. Cybersecurity preparedness and response measures are not purely technical in nature. The person(s) responsible for this function must command an ever-changing balance of technical, social, political, strategic and communications skills. In addition, a strong boardroom presence is essential.

CIOs are not always sufficiently empowered or do not always have the necessary training in change management to implement a new, holistic cybersecurity paradigm. On many organisational charts, CIOs report to Chief Financial Officers (CFOs), which can be an inherently problematic situation: CIOs may ask for more funding to enhance cybersecurity, while CFOs may decline in an effort to keep costs down. In contrast, where cybersecurity awareness is high, CIOs tend to report directly to the CEO or top official.

With the line between information technology and operational technology[2] blurring, specialised security teams, with a much broader range of complementary and specialist skills in various subjects, may be needed. These teams will have to be more nimble and flexible than the traditional groups in charge of IT or security functions.

It will be increasingly necessary that CEOs and company Boards take a close, active, and supportive interest in the activities of their cybersecurity teams, not least because investors are paying more attention to this component of corporate strategy when valuing firms.

Technologies

Those entrusted with the building and maintenance of cyber-defences for their organisation must ensure that standards and procedures for the up-keeping, upgrading and updating of the hardware and software in their information systems are in place, understood and adhered to by all. Compliance with password management and its on-going change, for example, can go a long way in reducing the people-related threats to cybersecurity.

[2] Operational technology (OT) covers the spectrum of systems that deal with the physical transformation of products and services, and typically falls under the catch-all category of engineering. OT may control pumps, motors, conveyors, valves, and forklifts, to name a few examples.

Laws and regulations

The fluid nature of cybersecurity challenges may render useless any attempt to impose rigid regulation to control them. In some realms regulation can be effective, but where cybersecurity is concerned it may be little more than a blunt tool. Security conventions may be required, but the method of implementation may be best left to industry and, at a more local level, to the individual players. In the United States, information in the financial and healthcare sectors is very closely protected under federal oversight, yet beyond those two sectors the laws are determined by the 50 states--which means a very diverse approach is employed within national borders. Standardisation of rules on a national and, conceivably international level, might allow companies to better focus on the challenge at hand.

Risk-pricing and liability allocation

The insurance industry has recently raised its profile in the burgeoning dialogue on cybersecurity, cyber-defence and cyber-resilience, which is logical as it is in the business of pricing risk and potentially disbursing funds in the event of a breach at a client firm. Insurance firms appoint, retain and deploy their nominated agents to audit clients, perform stress tests, advise on contract and legislative compliance, and to recommend and install software and hardware upgrades. In the event of a security breach at an insured client, they deploy their own teams to address the problem and mitigate their risk, in addition to providing a range of continuity of service solutions.

A key question is the extent to which these insurance companies may end up shaping the way companies and governments think about cybersecurity. Cyber-insurance appears to be improving cybersecurity preparedness, by requiring those seeking insurance to meet certain agreed-upon criteria to qualify for coverage. Companies that are able to demonstrate that they have good cybersecurity practices in place should expect to pay lower insurance premiums. This market process, whereby insurers price their policies based on the inherent risks of the companies they will insure, should encourage companies to acknowledge the benefits of good security and the costs of poor security. This process should in turn promote investment and improvements in cybersecurity readiness.

Cyber-insurers have a vested interest in ensuring greater security not only for their clients, but also as it relates to areas of associated risk, such as the networks with which their clients interact and the partners with which they do business. The growing list of security requirements imposed by cyber-insurers on prospective clients is a key feature of the important role they are playing. Should the widespread adoption of these requirements make them industry standards, that would likely help to boost preparedness to a degree that might not materialise through government regulation alone.

Information sharing

Information sharing through open communications is a central defence strategy at the national and international levels. Energy companies, regulators and security experts need to increasingly share security data. This will require a new level of trust in government-business relations, particularly in the post-Snowden environment.

The financial sector has long been a target of cyber-crime and provides insights that are valuable for the energy industry as it adapts and responds to cybersecurity threats. Financial actors and institutions have demonstrated an increasingly flexible, cooperative and open approach, leveraging pre-existing groupings such as those involving central bank governors and treasury departments, as well as super-national organisations such as the G20, to facilitate the sharing of insights and good practices among policymakers and market actors.

One salient example of this information exchange is the collaborative effort between the Depository Trust and Clearing Corporation (DTCC) and the Financial Services-Information Sharing and Analysis Center (FS-ISAC) in launching Soltra, a cyber-threat intelligence initiative. The objective is to create a network for the automated sharing of security intelligence to protect critical infrastructure. Another recent example is the cybersecurity working group created by the World Federation of Exchanges, which is striving to bring the world's stock exchanges together to share views on common threats. The group, called GLEX (for GLobal EXchange security), is an information-sharing and advocacy hub for large and small exchanges across the globe.

Coordination

Given that reaction times are of the utmost importance where cybersecurity is concerned, one path forward would be to task existing governmental institutions and industry bodies with the coordination of strategic courses of action, as opposed to creating new bodies for this purpose. As with information sharing, a high level of trust and smooth cooperation among actors in government, the IT sector and other industries will be essential if this suggested approach is to function.

5. CONCLUSIONS AND NEXT STEPS

Much remains to be understood about the challenge of cybersecurity in the energy sector. Industrial and governmental recognition of cyber-threats and the development of strategies to address them are still in nascent phases. This IEF-Pillsbury Thought Leaders' Roundtable attempted to identify and define key cybersecurity issues as a point of departure for future discussion, in the hope that it might also contribute to the timely development of necessary alliances and solutions.

Cybersecurity is a multi-disciplinary problem, with solutions that appear to be equally diverse. Threats may be the result of malicious hacking from half a world away from their target, made possible by the interconnectivity prevalent in this digital age. Employees and human nature present the possibility of breaches from within an organisation, either intentionally or inadvertently. The traditional overseer of digital security, the CIO, may not be equipped to prepare for and confront contemporary threats that now span technology, human elements and the operational infrastructure found in the energy sector and throughout global supply chains.

In the near future, a system of governance over network issues may need to be developed, and alliances between government and industry will be crucial to ensure that efforts to address security concerns are as focused and effective as possible. This implies the establishment of robust and sustained dialogue where there has been little to date. Trust must be developed among players in a cyber-industry that has been, by its very nature, secretive rather than inclusive.

Despite these challenges, the costs of inaction are high. The scale of recent cyber-breaches in the retail and financial sectors reveal the extent to which shareholder value can be jeopardised. High profile breaches in the energy sector demonstrate how national interests can be profoundly impacted by an attack on IT infrastructure and the operational infrastructure it controls. Effective solutions will encompass elements of IT and organisational engineering, policy and cooperation that cross-political and corporate boundaries. First, however, cybersecurity must be accorded the highest level of priority in corporate boardrooms and in Ministers' conference rooms, on par with financial, market and operational concerns.

The mission of the IEF is to promote energy security through dialogue. The IEF's hope is that future discussions on cybersecurity will explore the issues presented herein, and that those discussions will help to create an atmosphere of cooperation that in turn engenders a more secure energy sector for all.