Hogan Lovells

Cyber security: A growing threat to the energy sector

An Australian perspective

MARCH 2016

Contents

Contact

This alert is written as a general guide only. It should not be relied upon as a substitute for specific legal advice.

If you would like further information please contact the lawyer mentioned below or the lawyer with whom you usually deal.

Tim Lester
Head of Corporate
Partner, Australia
tim.lester@hoganlovells.com
T +61 8 6208 6551
+61 2 9093 3501

Cyber security: A growing threat to the energy sector

An Australian perspective

Cyber security is a topic of increasing concern to businesses, governments and policy makers alike. A cyber attack has the potential to cause material damage and disruption to national economies, to the global economy, as well as to national and international security. Cyber security policy aims to protect the public from economic, social and physical disruption. While each industry has its own vulnerabilities, a cyber attack in the energy sector can be particularly severe and costly. It is important to be aware of the risks, comply with regulatory requirements, and to be prepared to respond proactively.

What is a "cyber attack"?

A cyber attack is either an incident that uses software, software code, computer technology or networks to commit a traditional crime (such as fraud or theft) or an incident that is directed at computers, connected devices or other information communication technologies to disrupt or damage supply, access or some other aspect of functionality.[1]

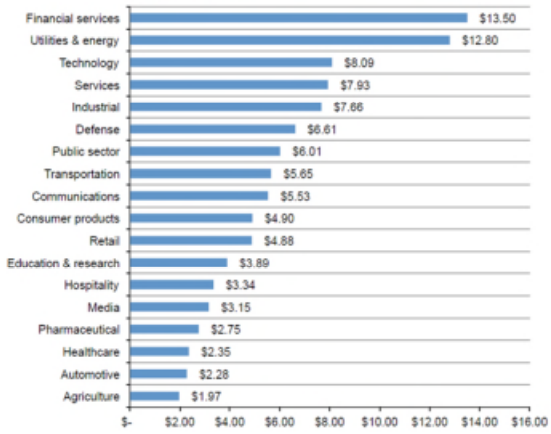
The growing threat to the energy sector

Incidents of cyber crime and the associated costs and issues vary across industries. However, Australian experience indicates that the energy industry appears to be the most highly targeted. CERT Australia, Australia's computer emergency response team, reported that 29% of incidents occur in this sector.[2] This is more than in the banking and financial services industry, which accounted for 20% of incidents, and the communications industry, which accounted for 12%.[3]

In the U.S., the Cyber Emergency Response Team issued two warnings during 2012 and 2013 specific to the gas industry based on an increased number of intrusions targeting gas pipeline companies.[4]

On a global scale, the cost of cyber crime in the energy sector is second only to the financial services sector, as evidenced in the table below. [5]

Figure 8. Average annualized cost by industry sector
Cost expressed in US dollars, $1,000,000 omitted
Consolidated view, n = 252 separate companies



The effects of a cyber attack in the energy sector

A cyber attack may disrupt general functionality or cause specific damage to intellectual property, critical infrastructure or physical property. Below are examples which highlight how broad and varied a cyber attack can be.

General functionality

Operational technology (OT) and supervisory control and data acquisition systems (or SCADA) are particularly at risk of cyber attacks. SCADA controls complex industrial processes, including production, centralised monitoring and control of dispersed meters and sensors. OT and SCADA are generally connected to the internet, which makes them more vulnerable. However, there have been examples of these systems being compromised even when they are not connected to the internet. A cyber attack on such systems can

[1] *Report 429: Cyber resilience: Health check,* AUStralian Securities and Investment Commission, March 2015.
[2] *2015 Threat Report,* AUStralian Cybersecurity Centre, 2015.
[3] Ibid.
[4] *ICS-CERT Monthly Monitor*, IndUStrial Control Systems Cyber Emergency Response Team, April 2012; April – June 2013.
[5] *2015 Cost of Cyber Crime Study: Global*, Ponemon Institute, September 2015.

cause business disruption, information loss, revenue loss and damage to assets and shareholder wealth.[6]

For example, in 2012, Saudi Aramco was hit by a computer virus, later named Shamoon, which disabled over 30,000 of the company's workstations and caused disruption for months.[7] A few weeks later Rasgas, a Qatari natural gas company, was also affected by the Shamoon virus. and forced to bring their entire network offline.[8]

Intellectual property

Cyber attacks can gain unauthorised access and subsequently use or release confidential information. This can result in a loss of future opportunity, reputation and financial gain that is difficult to quantify but can have a material impact on a business and its competitive standing. In December 2014, South Korea reported a cyber attack against the operator of its nuclear power plants.[9] The attackers released sensitive and confidential information online, including the plant equipment's designs and manuals.

Critical Infrastructure

Governments and their regulatory bodies around the world, are particularly concerned about cyber risks to systems of national interest and critical infrastructure. That is, those systems that, if rendered unavailable or otherwise compromised, could result in significant impacts on a country's economic prosperity, international competitiveness, public safety, social wellbeing or national defence and security. Critical infrastructure owned and operated by private companies, as is the case in Australia, are especially vulnerable to cyber attacks.

Damage to physical plant

Attacks can also use remote access to disrupt operations and cause physical damage to a plant and/or equipment. Motorola Solutions reported that wherever there is digitally enabled technology or an intelligent device, even a simple device that controls a valve on a pipeline, there is a risk of it being used as a portal and taken over without authorisation.[10] Such cyber attacks have the potential to cause equipment damage, a safety incident or loss of production.

In December 2014, the German Federal Office for Information Security reported that a steel mill's operations were affected by a cyber attack.[11] Attackers reportedly gained access to the steel plant's network through a malicious email, which resulted in a breach to the plant's control systems. This led to parts of the plant failing and meant that the blast furnace could not be shut down as normal, causing significant and costly physical damage.

How to respond to the risks: "cyber resilience"?

The response of governments, policy makers and businesses to the risk of a cyber attack is to promote, reinforce and implement "cyber resilience". Cyber resilience is the ability to prepare for, respond to and recover from a cyber attack. It's not just about preventing the attack from occurring, it's also about considering whether the business could continue to operate during an attack and how easily it would adapt and recover.[12]

General cyber resilience framework

Given that different regulations and requirements apply to different businesses, there is no uniform approach to building cyber resilience. The Australian Securities and Investments Commission (ASIC), Australia's corporate and financial services regulatory body, encourages businesses to use the NIST Cybersecurity Framework which was developed by the U.S. National Institute for Standards and Technology.[13] It is a standard risk management tool based on 5 key functions, as shown below. Essentially, the framework assists users to identify risks, critical assets and intellectual property, develop proportionate procedures and actions to protect against such risks, and respond and recover from a cyber attack if one occurs.

[6] *2014 Cost of Cyber Crime Study: Australia*, Ponemon Institute, October 2014.
Energy at risk, KPMG Global Energy Institute, 2013.
[8] Ibid.
[9] McCurry, *South Korean nuclear operator hacked amid cyber-attack fears*, The Guardian 2014).
[10] *White paper; Protecting Operations in the Energy Sector Against Cyber Attacks*, Motorola Solutions, 2014.
[11] *Hack attack causes 'massive damage at steel works'*, BBC News, 2014.
[12] *Report 429: Cyber resilience: Health check,* Australian Securities and Investment Commission, March 2015.
[13] *Report 429: Cyber resilience: Health check,* Australian Securities and Investment Commission, March 2015.

As it references global standards for cyber security, it is useful for international cooperation to strengthen the cyber security of organisations.

The U.S. Department of Energy has issued guidance on

[14]

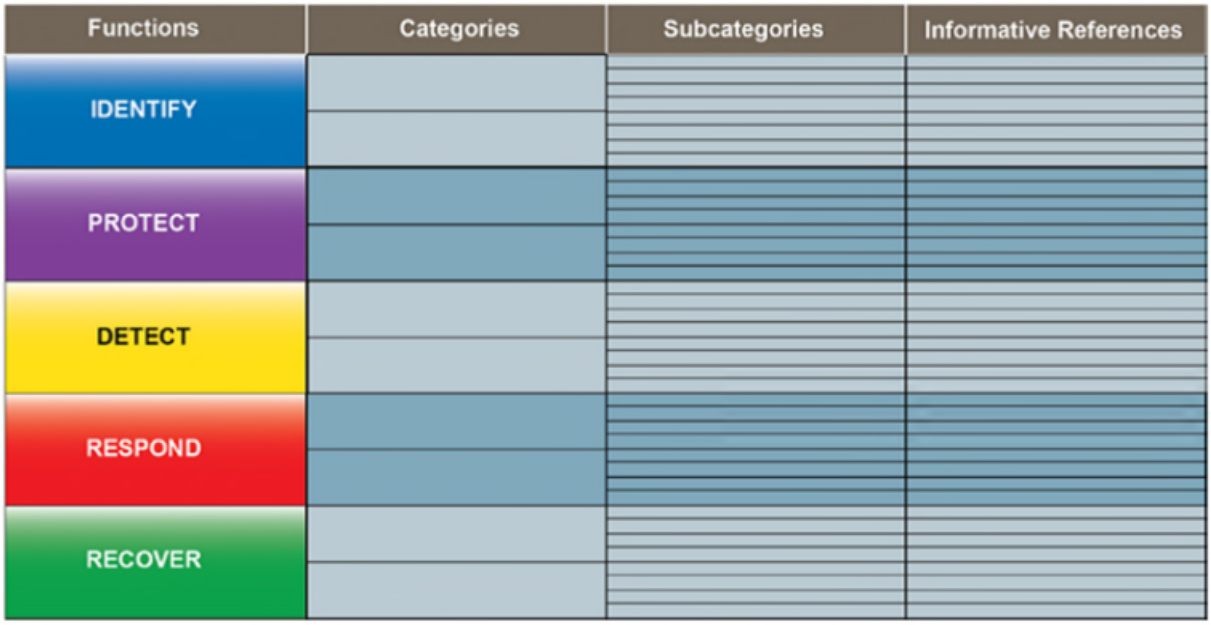


Figure 1: Framework Core Structure

implementing the NIST Cybersecurity Framework in the energy sector. Neither the framework nor the guidance are compulsory, particularly in Australia. However, adopting the framework will make it easier for companies to demonstrate sufficient care and diligence have been taken.

Strategies to mitigate cyber intrusions

While the NIST Cybersecurity Framework is a useful template for managing cyber risks on a general level, the Australian Signals Directorate (ASD) has developed more directive strategies to mitigate targeted cyber intrusions. The ASD claims that at least 85% of the targeted cyber intrusions that they respond to could be prevented by following the four strategies below:

1. Use application whitelisting to help prevent malicious. software and unapproved programs from running
2. patch applications such as Java, PDF viewers, Flash, web browsers and Microsoft Office
3. patch operating system vulnerabilities
4. restrict administrative privileges to operating systems and applications based on user duties.[15]

These strategies are only mandatory for Australian Government agencies. However, ASIC recommends that the regulated population adopt these strategies as well.

Cyber security as a regulatory compliance issue

It is also a regulatory compliance issue for many businesses to ensure that they are adequately protected from cyber risks. The applicable regulatory requirements will depend on the size and nature of business. Thus, it is important that companies know their obligations and what they need to do to comply.

For example, a company may need to disclose cyber risks as part of corporate disclosure requirements. This may include assessing how exposed the business is to an attack and if investors reasonably require information about cyber risks in order to make informed decisions. Addressing cyber risks in the company's prospectus and/or annual report may be necessary. If a business does suffer a cyber attack, it may need to be disclosed as market-sensitive information.

[14] Framework for Improving Critical Infrastructure Cybersecurity, National Institute of Standards, 2014.

[15] *Strategies to Mitigate Targeted Cyber Intrusions*, Australian Signals Directorate, 2016.

For directors or officers of a corporation, cyber risks may affect their duties and annual director report disclosure requirements. Directors and officers have a duty to act with reasonable care and diligence. Therefore, for a director to have knowledge of their business' vulnerabilities, and to ignore the risk would be a breach of this duty. In some cases, it may result in disqualification from the role.[16]

For businesses regulated by the *Privacy Act 2009*, reasonable steps to protect confidential information are required. This may involve implementing effective ICT security, whitelisting and blacklisting entities or applications, encryption and/or requiring multi-factor authentication for access to information.[17]

Depending on the severity of a breach, a failure to identify and manage cyber risk can result in fines, penalties, enforceable undertakings, licensing conditions or a licence suspension or cancellation.

In particular, energy companies should:

- have strong compliance programs in place[18]
- be alert to and, indeed, have the systems in place to report or disclose:
  - potential issues
  - suspected market manipulation
  - reliability violations or
  - other potential offences or issues and
- have systems in place to mitigate the risk of an attack and systems and processes that can respond and recover should they be subject to one.

Global regulation of cyber security

It is early days and many countries have a patchwork of rules and regulations that address cyber security. Below outline a few highlights on regulation around the globe.

U.S.

In 2015, the U.S. passed two pieces of legislation; the *Protecting Cyber Networks Act* and the *National Cybersecurity Protection Advancement Act.* These pieces of legislation are aimed at improving the sharing of information between the private sector and government agencies. The second piece of legislation offers some liability protection for private entities that do so. The aforementioned NIST Framework also comes out of the U.S..

Europe

In December 2015, the EU informally agreed to the Network and Information Security (NIS) Directive which aims to establish a high level of cyber resilience across the EU. It is likely to be formally adopted in the next few months and, once this occurs, the member states will have two years to pass national laws implementing requirements of the directive, such as creating national cybersecurity bodies and cross-border cooperation strategies.

Significantly, the directive covers "operators of essential services". This term includes operators in the electricity, oil and gas sectors. Entities within the scope of the NIS Directive must implement “state-of-the-art” security measures that “guarantee a level of security appropriate to the risk.”

Singapore

Singapore established a dedicated Cybersecurity Agency (**CSA**) in April 2015, which oversees national cybersecurity functions. So far, the establishment of the CSA has led to Singapore signing memorandums of understanding with the UK, France and India, in each case committing to collaborate on cybersecurity.

China

On 6 July 2015, the Chinese government released for public comment a consultation draft of a new Cybersecurity Law. This law would increase obligations on network operators. The term "network operators" is broadly defined and includes owners, administrators and network service providers who use networks owned or administered by others in order to provide relevant services. This includes, but is not limited to, basic telecommunications operators, network information service providers, and important information system operators. These entities are obliged to have cyber security protocols in place and to take steps to protect against cyber attacks.

The Cybersecurity Law also imposes obligations on providers of information network products and services. Key IT hardware and equipment must meet mandatory security qualifications and acquire government certification before being sold.

Reporting cyber attacks

If a business experiences a cyber attack, it is advised that it be reported. In Australia, there are two agencies that the government has established to monitor and respond to cyber crime. The Australian Cybercrime

[16] *Report 429: Cyber resilience: Health check,* Australian Securities and Investment Commission, March 2015.
[17] *Guide to information security: Reasonable steps to protect personal information*, Office of the Australian Information Commissioner, April 2013.
[18] *Report 429: Cyber resilience: Health check,* Australian Securities and Investment Commission, March 2015.

Online Reporting Network (ACORN) was developed for small to medium businesses and generally deals with hacking, fraud, identity theft and attacks on computer systems. Making a report to ACORN involves submitting relevant information about the incident online. CERT Australia is for major Australian businesses and critical infrastructure. Reporting an incident with CERT Australia can be done on the phone or via email.

Conclusion

As society's dependence on technology increases, there is a corresponding need for cyber security to be taken more seriously. A cyber attack can target critical infrastructure or physical facilities, or disrupt an entire network's functionality. The repercussions of a cyber attack in the energy sector can be especially extensive and thus, it would be prudent for businesses to be cyber resilient. For some, this may involve adopting regulatory frameworks or ensuring that compliance obligations are being met. Irrespective of a company's size, nature of business or location, it is important to be aware of the risks and to be protected against potentially irreversible and costly damage.

References

Australian Cybersecurity Centre, (2015). *2015 Threat Report*, [online] p.11. Available at https://www.acsc.gov.au/publications/ACSC_Threat_Report_2015.pdf [Accessed 23 February 2016].

Australian Securities and Investment Commission, (2015). *Report 429: Cyber resilience: Health check*. [online] p.4 – 6; 16; 31; 38. Available at http://asic.gov.au/regulatory-resources/find-a-document/reports/rep-429-cyber-resilience-health-check/ [Accessed 23 February 2016].

Australian Signals Directorate, (2016). *Strategies to Mitigate Targeted Cyber Intrusions*. [online] Available at: http://www.asd.gov.au/infosec/mitigationstrategies.htm [Accessed 23 March 2016].

BBC News, (2014). *Hack attack causes 'massive damage at steel works'*. [online] Available at http://www.bbc.com/news/technology-30575104 [Accessed 23 February 2016].

Industrial Control Systems Cyber Emergency Response Team, (April 2012). *ICS-CERT Monthly Monitor*. [online] Available at https://ics-cert.us-cert.gov/monitors/ICS-MM201204 [Accessed 23 February 2016]

Industrial Control Systems Cyber Emergency Response Team, (April – June 2013). *ICS-CERT Monthly Monitor*. [online] Available at https://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Apr-Jun2013.pdf [Accessed 23 February 2016].

KPMG Global Energy Institute, (2013) *Energy at risk*. [online] p.3. Available at www.kpmg.com/Global/en/IssuesAndInsights/ArticlesPublications/Documents/energy-at-risk.pdf [Accessed 23 February 2016].

McCurry, J. (2014). *South Korean nuclear operator hacked amid cyber-attack fears*. [online] Available at http://www.theguardian.com/world/2014/dec/22/south-korea-nuclear-power-cyber-attack-hack [Accessed 23 February 2016].

Motorola Solutions, (2014) *White paper; Protecting Operations in the Energy Sector Against Cyber Attacks*. [online] Available at http://communities.motorolasolutions.com/community/ea/think-oil-and-gas/blog/2014/10/20/protection-against-cyber-attacks-in-the-digital-oilfield [Accessed 23 February 2016].

National Institute of Standards, (2014). *Framework for Improving Critical Infrastructure Cybersecurity*. [online] p.7. Available at http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf [Accessed 23 February 2016].

Office of the Australian Information Commissioner, (2013) *Guide to information security: Reasonable steps to protect personal information*. [online] p. 15 – 22. Available at https://www.oaic.gov.au/images/documents/privacy/privacy-guides/information-security-guide-2013_WEB.pdf. [Accessed 24 March 2016].

Ponemon Institute, (2014) *2014 Cost of Cyber Crime Study: Australia*. [online] p.3. Available at http://www.ipsi.com.au/wp-content/uploads/2015/02/Australia_Cost-of-Cyber-Crime-Report_Ponemon-Institute.pdf [Accessed 23 February 2016].

Ponemon Institute, (2015) *2015 Cost of Cyber Crime Study: Global*. [online] p.10. Available at http://www.cnmeonline.com/myresources/hpe/docs/Report_2015_Ponemon_GLOBAL.pdf [Accessed 23 February 2016].

www.hoganlovells.com

Hogan Lovells has offices in:

Alicante
Amsterdam
Baltimore
Beijing
Brussels
Budapest*
Caracas
Colorado Springs
Denver
Dubai
Dusseldorf
Frankfurt
Hamburg
Hanoi
Ho Chi Minh City
Hong Kong
Houston
Jeddah*
Johannesburg
London
Los Angeles
Luxembourg
Madrid
Mexico City
Miami
Milan
Minneapolis
Monterrey
Moscow
Munich
New York
Northern Virginia
Paris
Perth
Philadelphia
Rio de Janeiro
Riyadh*
Rome
San Francisco
São Paulo
Shanghai
Silicon Valley
Singapore
Sydney
Tokyo
Ulaanbaatar
Warsaw
Washington, D.C.
Zagreb*

*Associated offices