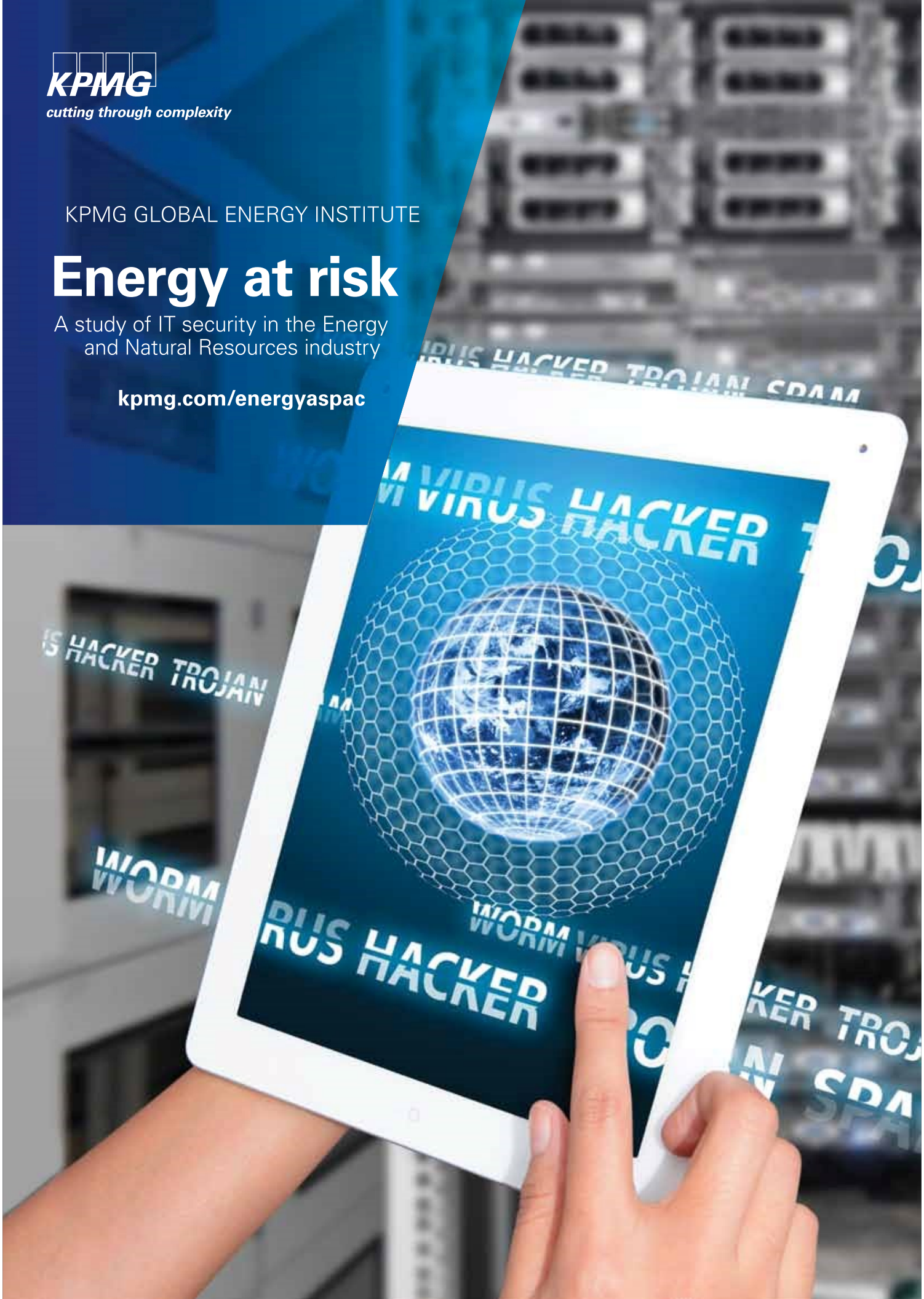
KPMG
cutting through complexity

KPMG GLOBAL ENERGY INSTITUTE

Energy at risk

A study of IT security in the Energy and Natural Resources industry

kpmg.com/energyaspac



EXECUTIVE SUMMARY

Companies now not only face cyber attacks from hacking groups, script kiddies and hactivists, they are also threatened by state-sponsored agencies with limitless resources. These agencies usually carry out cyber attacks to seek a competitive edge, gain access to intellectual property, or for sheer sabotage. In other words, cyber threats have never been more pervasive and attack damages never more real.

The situation is especially grim for the Energy and Natural Resources (ENR) industry. The sector is plagued by two key problems. For one, top management has traditionally not placed sufficient emphasis on information security. Also, much more focus is placed on connectivity compared to security. As a result, the ENR sector has become an enticing and relatively easy target for cyber attacks.

As evidenced in recent cyber incidents "Shamoon[1]" and "Night Dragon[2]", the resultant loss and combined damage, be it substantial or intellectual, would be far greater than the cost of preventive security measures.

In this increasingly insecure environment, senior management should refresh their perspective to safeguard their key corporate assets.

For many organisations in the Asia Pacific, a cyber security-oriented structural transformation might be necessary.

"I am convinced that there are only two types of companies: those that have been hacked and those that will be. And even they are converging into one category: companies that have been hacked and will be hacked again."

Robert S. Mueller, FBI Director
RSA Cyber Security Conference
March 2012

[1] Shamoon, also known as Disttrack, is a modular computer virus discovered in 2012 that attacks computers running the Microsoft Windows "NT" line of operating systems. The virus is being used for cyber espionage in the energy sector. Its discovery was announced on 16 August 2012 by Symantec, Kaspersky Lab, and Seculert.

[2] Operation Night Dragon was a Cyber Attack against energy companies which was exposed by the security company McAfee. Night Dragon attacks are designed to steal sensitive data from targeted organisations. Unlike opportunistic attacks, the perpetrators appear to be sophisticated, highly organised, and motivated in their pursuits.

© 2013 KPMG International Cooperative ("KPMG International"), a Swiss entity. Member firms of the KPMG network of independent firms are affiliated with KPMG International. KPMG International provides no client services. No member firm has any authority to obligate or bind KPMG International or any other member firm vis-à-vis third parties, nor does KPMG International have any such authority to obligate or bind any member firm. All rights reserved.

CONTENTS

© 2013 KPMG International Cooperative ("KPMG International"), a Swiss entity. Member firms of the KPMG network of independent firms are affiliated with KPMG International. KPMG International provides no client services. No member firm has any authority to obligate or bind KPMG International or any other member firm vis-à-vis third parties, nor does KPMG International have any such authority to obligate or bind any member firm. All rights reserved.

What is going on

The Current Global Situation

Cyber threats and IT risks are omnipresent. Compared to the past when criminals used a scattergun approach, cyber attacks now are much more focused and intelligent. Let us first take a peek into an attacker's world.

An attacker's perspective

Understanding the perspective of an attacker is essential for everyone involved in fighting cybercrime. For that reason, staff in KPMG Netherlands interviewed one of their professionals – an 'ethical hacker'. He relayed us an intriguing fictitious story. It is up to you to judge how realistic this threat would be to your organisation.

"My employer insists on remaining anonymous, but rest assured, he is quite resourceful. He approached me a few weeks ago with a job offer. The goal he set was quite ambitious: steal as many secrets from the government as you can. Let me tell you about the steps I took.

First, I sat down to think about what I knew about the government's IT infrastructure. At a conference last fall, I had met an IT director of a ministry who had told me that all firewalls for the government were supplied by the same vendor, company Y. Hacking such a firewall was a formidable task - not something I was ready to take on directly. Instead, I took a more indirect approach.

I logged in to LinkedIn and searched for employees of software development companies who mentioned company Y as one of their clients on their LinkedIn profile. Many professionals mention prestigious client names in their profile, even when company policy prohibits name dropping. Shortly after, I found multiple software vendors which make niche software and listed company Y as a client. I visited the vendors' websites and scanned their externally reachable IP addresses until I found one which had an unpatched vulnerability in their web server: company X. After a day's work, I was inside their network.

Company X is a small organisation and they do not feel they need network segmentation, so I was able to reach all machines on their internal network through that web server. After some more work, I was able to elevate my privileges to domain administrator, which meant I had full access to all of their systems.

This was where I hit a bump. I intended to change the source code of their product in such a way that it would allow me to connect remotely to the system of anyone who installed it, but I had never done that before. I then decided to log on to a hacker forum and posted a request for help. I offered 10,000 euros reward for a job well done. After a while, I was approached by someone who was willing to help me. I asked around to confirm his reputation in this field. I enlisted his help in modifying the source code of the main product of company X.

The security policies of company Y were very strict: only the system administrators can install software on the workstations, and both incoming and outgoing traffic goes through a proxy server. Luckily, the virus which my associate hacker had written communicates through DNS, which was not actively monitored or filtered. The software from company X was updated on a regular basis, and after three weeks I received a message which indicated that I had access to their workstations.

I called on my associate hacker once more, but this time for a more advanced task: reprogramming the firmware of the firewalls which company Y produces. He indicated that he needed the help of a contact who installed a backdoor in all firewalls for another 20,000 euros. Now, all I needed to do was wait for the next update of the firmware. I posted some fake security vulnerabilities for the current version of this firmware, to ensure that the firmware would be upgraded timely. And slowly but surely, I gained access to all internal networks of the government.

I could then route any traffic which flows through any government network through my own computer. I can also read all emails which are sent between government employees internally. I can find vulnerable servers by scanning the networks. In almost all the internal networks, I have found at least one server which I can exploit. I installed backdoors on hundreds of workstations which allows me the ability to monitor email servers, so emails with interesting attachments can be forwarded to me. Additionally, I have obtained login credentials for almost all major government databases.

Every day, almost two hundred gigabytes of government secrets are sent to me automatically. This amount is only limited by the amount of bandwidth I can get, and the number of hard disk drives I install. I'm being paid 100 euros per gigabyte of information. I will leave it to you to calculate my hourly wage."

© 2012

© 2013 KPMG International Cooperative ("KPMG International"), a Swiss entity. Member firms of the KPMG network of independent firms are affiliated with KPMG International. KPMG International provides no client services. No member firm has any authority to obligate or bind KPMG International or any other member firm vis-à-vis third parties, nor does KPMG International have any such authority to obligate or bind any member firm. All rights reserved.

The sad truth is that cybercrime is here to stay. A report by the Government Accountability Office indicated that 24 key government agencies in the United States have logged a 650 percent increase in cyber security incidents in 2011 compared to five years ago.

According to a survey by KPMG Netherlands, 49 percent of organisations have experienced some form of cybercrime activity during the past 12 months while the remaining may not even have proper detection measures in place.

Among the 49 percent, 10 percent indicated that they have been attacked more than 100 times within the past year. The remaining respondents said they were attacked successfully up to five times last year. Most of the incidents were not covered by the media and are therefore not publicly known.

Information leakage most common

Globally, information leakage is one of the most common challenges faced by organisations.

Opening an email containing a virus from a hacker can allow perpetrators to seize control of your computer, read your emails and record your passwords. Information leakage is in fact one of the most common types of incidents across the world and can easily take place in your daily life.

Take for example that you have made a donation to a local charity. In recognition of your contribution, the organisation lists your name on their website as a sponsor. Two days later, you receive an email from the Fundraising Chair asking you to confirm your donation. You open the email, fill out the form (you are also careful not to include any banking or sensitive information) and return it to the sender. But in reality, the email didn't come from the charity at all; the attachment was, in fact, a high quality fake containing a virus, allowing perpetrators to seize control of your computer, read your emails and record your passwords. Everything you know or see is now visible to the perpetuators. Clearly, information leakage is rapidly becoming a board-level risk.

A 2012 survey by KPMG suggest that more than three-quarters of the Forbes 2000 companies leak potentially dangerous data (See Figure 1 below).

Personal information and financial data are often lost due to hacking, system failure, human negligence and disgruntled employees. Some countries have already enacted legislation to curb such problems. The European Commission's General Data Protection Regulation released in 2012 states that companies have the obligation to protect their network and personal information.

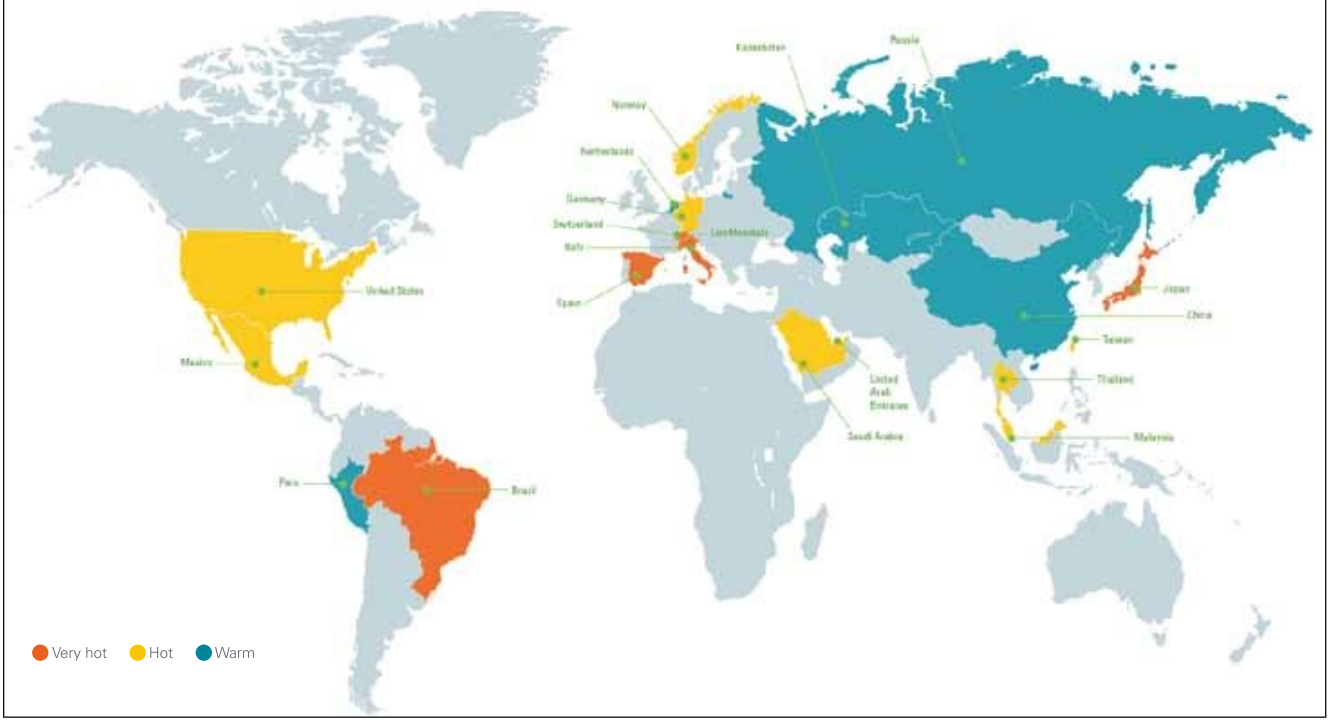
Companies must also notify relevant authorities within 24 hours after a serious breach, or face a penalty of up to one million Euros or two percent of turnover.

It is worth noting that hacktivist groups are often the agents responsible for information leakage. For instance, members of "Anonymous", a famous hacktivist group, are not only known for bringing down commercial systems and websites, they have also infiltrated into commercial organisations' computer systems, exposing correspondence and personal data to the public in the process.

In 2010, Anonymous penetrated Sony's network and cost the latter US$170 million dollars in reparation for the unauthorised disclosure of customers' names and credit card numbers. Another Anonymous' affiliate group AntiSec dumped over 860,000 user credentials including 75,000 sets of personal and financial information into the open Internet after breaking into the firm Stratfor's systems.

During the past few years, industries all around the globe have witnessed for the first time carefully engineered and profoundly complex attacks such as Stuxnet, Night Dragon and Shamoon (these will be described later in the document). Cyber security has become a grim issue that no one can avoid.

Figure 1: Heat map of information leaking countries



Source: KPMG Cyber Vulnerability Index 2012

© 2013 KPMG International Cooperative ("KPMG International"), a Swiss entity. Member firms of the KPMG network of independent firms are affiliated with KPMG International. KPMG International provides no client services. No member firm has any authority to obligate or bind KPMG International or any other member firm vis-à-vis third parties, nor does KPMG International have any such authority to obligate or bind any member firm. All rights reserved.

ENR Related Security Incidents

General

Of all the potential marks at crosshair, the ENR industry is one of the most attractive targets for cyber criminals.

According to the United States (US) Department of Homeland Security News Wire published in April 2012, American water and energy companies deal with a constant barrage of cyber attacks on a daily basis. These incidents usually take the form of cyber espionage or denial-of-service (DoS)[3] attacks against the utilities' industrial-control systems.

According to a survey report released by The Centre for Strategic and International Studies in 2010, "critical infrastructure firms such as power grids, industrial control networks and oil refineries are facing staggering level of cyber attacks, and are not adequately prepared to defend themselves".

In April 2012, the US Cyber Security response team warned of attacks upon the gas industry. The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) reported a number of cyber intrusions targeting gas pipeline companies. Analysis of the attacks confirmed they are part of an ongoing campaign dating back to December 2011 and indicated Spear Phishing was used to target a number of specific individuals across the gas pipeline industry.

Spear phishing is an e-mail spoofing fraud attempt that targets a specific organisation, seeking unauthorised access to confidential data.

Shamoon

On 15 August 2012, Saudi Aramco, a large national oil and gas company with global operations, announced that they had to disconnect their IT systems from the Internet while dealing with a serious disruption of their network. The disruption, which continued for two weeks, was the result of a cyber attack that used a computer virus to disable over 30,000 of the company's workstations.

The virus, later named as "Shamoon", was the first significant cyber attack on a commercial target to cause real damage. It is also the most destructive attack the private sector has experienced to date.

Later in the same month Rasgas, a main player in the Qatari Liquid and Natural Gas scene, was also hit by the Shamoon (as per security experts) virus and consequently forced to bring their entire network offline.

Night Dragon

Another series of cyber incidents in the ENR sector were dubbed collectively by security company McAfee as "Night Dragon". McAfee believes that these attacks on global oil, energy and petrochemical companies may have started as early as in 2007.

Evidence from McAfee has shown that this series of well-coordinated and specifically focused attacks involve a myriad of different techniques and methods. The primary target seems to be any financial information related to bids and oil-and-gas operations.

McAfee also pointed out that all the attacks took place regularly during weekdays from 9am to 5pm in GMT +8 time zone, which matched with the source location as determined by the IP address, thus pointing at the high possibility of "company men" being hired to perform the job systematically.

Others

There are many more cyber security incidents which have taken place in the ENR industry.

In 2011, a Canadian-based company which supplies remote administration and monitoring tools to Fortune 100 energy companies reported that it had suffered a security breach. Upon breaching the corporate network, the attackers installed malicious software on computers and stole information related to a remote administration tool which the company supplies.

Another incident of more recent times occurred in early 2013. In February 2013, the US Department of Energy confirmed that computers and servers at its Washington headquarters were compromised in the previous month. In this attack, personally identifiable information of several hundred employees and contractors may have been compromised. Seemingly non-critical at first glance, this information may however be used to further future attacks into having serious consequences.

In another case, unidentified hackers helped a manufacturer in China obtain the breakthrough design of a wind turbine by an energy company in the United Kingdom. The Chinese manufacturer subsequently made and sold the product at a much lower price, driving the original company in the UK into closure.

DoS attacks represent yet another form of cyber security attacks which cause huge financial losses and massive damage to companies in the ENR sector. A report published by McAfee in 2011 stated that four out of every five oil, gas and power companies have suffered at least one DoS attack in 2011.

Cyber attacks are also increasingly escalating into cyber warfare. In an October 2012 Wall Street Journal article, U.S. officials noted that "Iranian hackers with government ties have mounted cyber attacks in 2012 against American targets, escalating a low-grade cyber war ... The Iranian effort culminated in a series of attacks against U.S. banks as well as electronic assaults on energy companies in the Persian Gulf."

These incidents clearly show the increasing severity of cyber attacks and give an idea on how important cyber security will be in the future.

[3] A denial-of-service (DoS) attack or distributed denial-of-service (DDoS) attack is an attempt to make a machine or network resource unavailable to its intended users.

© 2013 KPMG International Cooperative ("KPMG International"), a Swiss entity. Member firms of the KPMG network of independent firms are affiliated with KPMG International. KPMG International provides no client services. No member firm has any authority to obligate or bind KPMG International or any other member firm vis-à-vis third parties, nor does KPMG International have any such authority to obligate or bind any member firm. All rights reserved.

Overview of Major Problems

The obvious question to ask is why these various organisations are so vulnerable in the face of cyber attackers.

In 2012, Carnegie Mellon University conducted their yearly survey for largest American companies. The results indicated that more than 70 percent of C-Suite executives and members of the board are not actively involved in the protection of their company data. They are also rarely involved in the inspection of key employees working on information security or the revision of corporate-wide policies in this aspect.

A similar trend has been observed by the Government Accountability Office in American government agencies. Despite receiving numerous security recommendations each year, companies were not implementing these properly. Key personnel were also not being trained adequately. In addition, there is a lack of proper monitoring on security controls or appropriate key performance indicators to assess improvement.

The ENR sector is critical as it powers the growth of almost every economy in the world. The sector can be broadly divided into three categories: electricity, petroleum and natural gas. In the electricity category, both automation systems and utilities controls of electricity infrastructure are built on a complicated system known as the Supervisory Control and Data Acquisition (SCADA). Similarly, the production and distribution of petroleum and natural gas are heavily dependent on systems similar to SCADA.

Unfortunately, such industrial infrastructure control systems have been facing a severe legacy problem in recent years. They have been rashly connected to the Internet for remote accessibility without implementing adequate security measures. This has in turn led to higher chances of such systems falling prey to cyber attacks.

© 2013 KPMG International Cooperative ("KPMG International"), a Swiss entity. Member firms of the KPMG network of independent firms are affiliated with KPMG International. KPMG International provides no client services. No member firm has any authority to obligate or bind KPMG International or any other member firm vis-à-vis third parties, nor does KPMG International have any such authority to obligate or bind any member firm. All rights reserved.

The who & why of cyber attacks

In this era of information and connectivity, malicious hackers are able to easily find information assets as targets in a corporate network.

What is at stake is financially valuable data such as mergers-and-acquisitions plans, transaction records, quarterly/ annual reports and internet banking details. Strategic information including intellectual property, contact details of senior executives, records of legal disputes and various trade secrets are also at risk.

In addition, personal data like employees' addresses and date of birth, once compromised might very well be used in facilitating identity theft.

Last but not least, process control networks are being increasingly favoured by attackers given their vast potential in bringing about significant impact, as proven in the famous Stuxnet case[4] and other incidents described earlier. Given how the numerous production and exploration activities carried out by energy companies are dependent on these networks, this trend is of particular relevance and importance to the ENR sector.

A 2011 report by KPMG has shown that oil and gas operations are amongst the top 10 sectors which suffer from the most information leakages worldwide. Information leakages involving oil and gas operations account for six percent of all security incidents.

Some of the sources of leakage are within the direct control of the corporation and can be prevented if companies put in the effort. These sources include websites, documents and web servers. However, there are also other channels such as popular search engines and forums which are outside of the usual enterprise security curtain and pose a much more complex challenge.

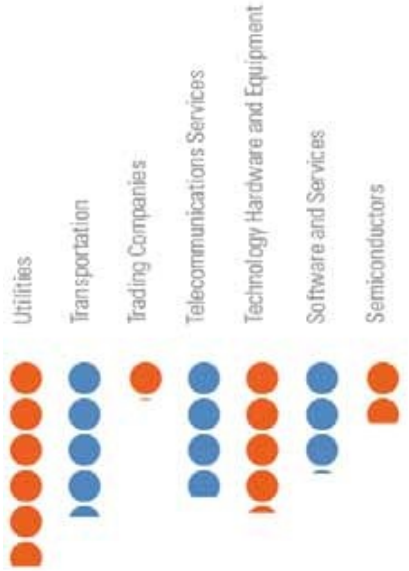
The KPMG report also revealed that 78 percent of Forbes 2000 corporate websites leak some form of potentially useful information through their document meta-data.

Document meta-data is information 'about' a document, or information on its properties. It often informs who created a document, when and where on a device or network.

According to version information retrieved from document meta-data, 71 percent of the 2000 companies may be using potentially vulnerable and out-dated versions of Microsoft and Adobe software.

Furthermore, 16 percent of corporate web servers may be vulnerable to attack due to missing security patches or out-dated server software. Many instances of un-patched and unsupported web server software were found to be serving Forbes 2000 corporate websites.

Figure 2: Number of potentially sensitive



[4] Stuxnet is a computer worm discovered in June 2010 that is believed to have been created to attack Iran's nuclear facilities. Stuxnet initially spreads via Microsoft Windows, and targets Siemens industrial software and equipment. Kaspersky Lab concluded that the sophisticated attack could only have been conducted "with nation-state support". Different variants of Stuxnet targeted five Iranian organizations, with the probable target widely suspected to be uranium enrichment infrastructure in Iran

© 2013 KPMG International Cooperative ("KPMG International"), a Swiss entity. Member firms of the KPMG network of independent firms are affiliated with KPMG International. KPMG International provides no client services. No member firm has any authority to obligate or bind KPMG International or any other member firm vis-à-vis third parties, nor does KPMG International have any such authority to obligate or bind any member firm. All rights reserved.

Part of KPMG's research focused on the structure of the Forbes 2000 corporate websites to identify any potentially sensitive file locations or hidden functionality that may be useful to cyber attackers. A number of file locations marked 'private' were also identified, hosting documents that were not intended for public consumption (See Figure 2 below).

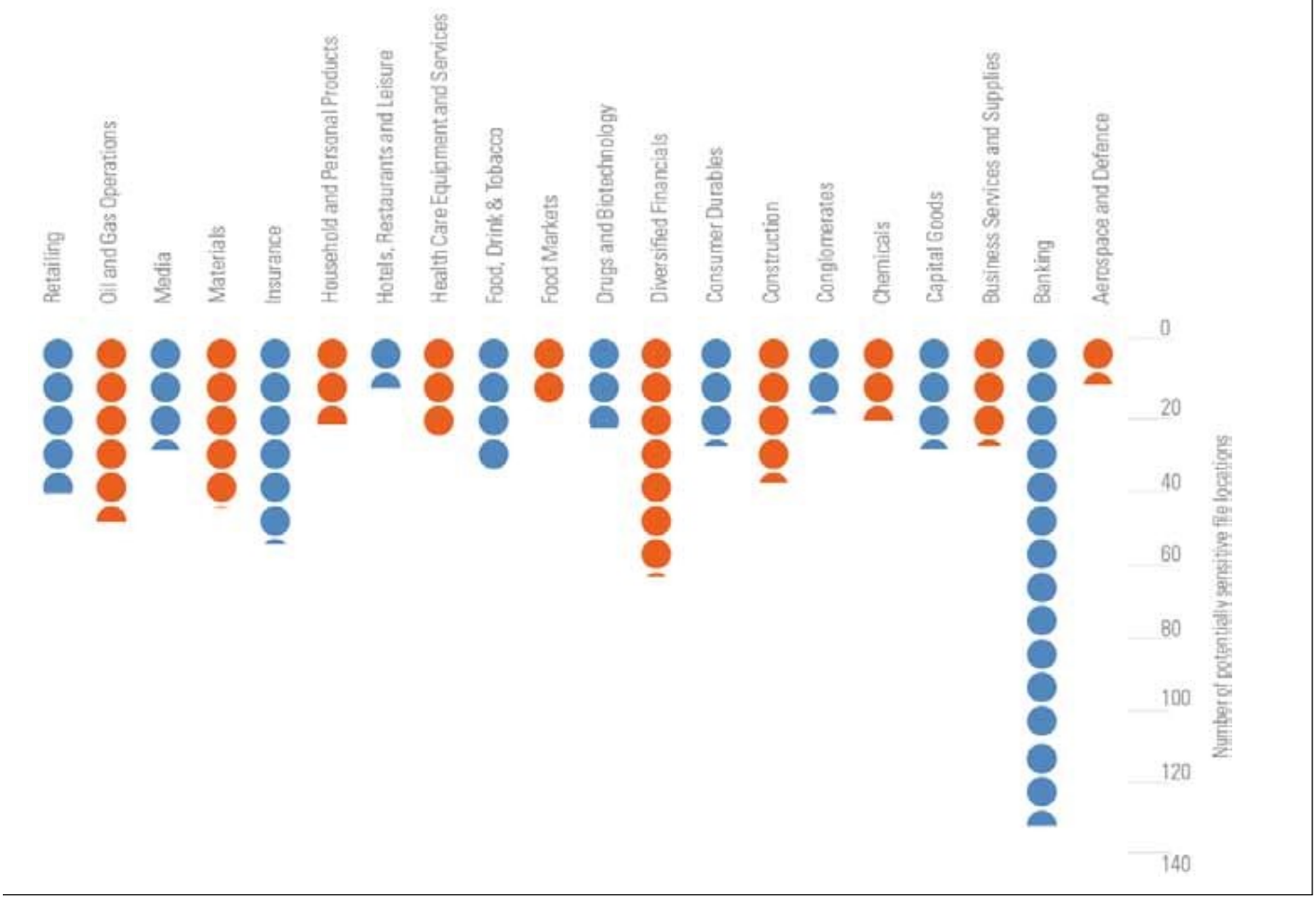
The direct result is that out of all the servers used for corporate websites, 15 percent offer hacker access to test functionality and private login portals that potentially allow file upload capabilities that could likely lead to full take-over of servers by cyber attackers.

Oil & Gas operations have also emerged in the list of top 10 sectors that post most information to public forums and newsgroups. There are as many as 88,681 of such postings in newsgroup alone, according to the report.

If past experience has taught us anything, it is that cyber attackers and organised crime do not target one avenue of attack. Instead, they use a combination of available information leaks to profile a target, and map out the target's internal systems and their components.

It is important to emphasise that the processes used to gather the information leaks mentioned above are not sophisticated and available to anyone with access to the Internet and little more than a web browser.

file locations on the Forbes 2000 corporate websites by sector



© 2013 KPMG International Cooperative ("KPMG International"), a Swiss entity. Member firms of the KPMG network of independent firms are affiliated with KPMG International. KPMG International provides no client services. No member firm has any authority to obligate or bind KPMG International or any other member firm vis-à-vis third parties, nor does KPMG International have any such authority to obligate or bind any member firm. All rights reserved.

Industrial Control System

The problem is even worse when it comes to control systems which are widely adopted by ENR industries, as explained by chief cyber security strategist from Computer Sciences Corporation (CSC), Donald Purdy. Purdy, formerly a cyber official at the Department of Homeland Security, mentioned during a major security conference in San Francisco in 2012:

"These are older systems so they are harder to control. And for convenience and cost savings, people have connected them to the internet in order to control them from remote locations. So this is almost a perfect storm in terms of vulnerability because the nation is so dependent on these systems… This is a significant security issue for the United States and frankly for the world."

In the monthly monitor report released last September by the US Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), it was also mentioned that "the positive aspects of better connectivity were overshadowed by the introduction of significant vulnerabilities".

For instance, Justin W. Clarke, a 30-year-old cyber security researcher and electric utility expert discovered two major vulnerabilities in 2012 on Siemens' RuggedCom equipment which is extensively used by companies in communicating with power stations situated in different locations.

The first vulnerability is essentially a secret "back door" which would easily allow hackers remote access into the equipment. The second vulnerability makes it possible for hackers to intercept the network traffic between operator and devices which may contain authentication credentials. Potential attackers could take advantage of such flaws to manipulate power stations or use these flaws to launch another set of attacks on a much larger scale.

The situation is made even worse when independent researchers release and circulate system flaws and vulnerabilities for reference and countermeasure studies. While the intention behind such documents might be good, the direct consequence is that many could now easily gain access to dangerous and powerful "weapons" such as the code of Stuxnet, which can cause immense damage to critical infrastructures.

In contrast to the published vulnerabilities, certain manufacturers of critical system controllers are reacting way too slowly which have resulted in research groups like Digital Bond, releasing exploits for these vulnerabilities in order to "stimulate" the patching and upgrading efficiency.

When it comes to electrical power, technology is also a double-edged sword. While advances in smart grid technologies have helped better detect power theft and reduce power loss with smart meters been recently deployed in countries such as in Serbia and Brazil, these technologies also give rise to possibilities of their advanced functionalities being used for shady purposes.

For instance, two demonstrations at Security B-Sides and Black Hat conferences illustrated that hackers could basically tweak the smart metres currently in use to perform functionalities as they wish, which include changing of temperature, controlling of lighting and even cutting of power during emergencies.

As a side note on corporate security policies and procedures, the Saudi Aramco incident where large number of business computers were disabled, also highlighted importance of monitoring network attacks initiated by inside personnel and the potential danger of using portable storage media like thumb drives.

Categorised Active Players

Over the years, two major shifts in trends have been observed in terms of cyber attacks.

Firstly, the targets are shifting from individual organisations to chains of related companies. Secondly, the main components of attackers have shifted from script kiddies to criminal groups, with the latter being much more specialised and coordinated.

Some of the major players include:

- organised cyber criminals who are most known for mass stealing of personal identities and financial data,
- state or corporate sponsored espionage like the Night Dragon operation which aims to steal critical intellectual and business information,
- hacktivists such as Wikileaks, Anonymous and LulzSec who have amassed a large number of supporters and participants,
- malicious inside personnel, as in the case of Bradley Edward Manning, a United States Army soldier who was arrested in May 2010 in Iraq on suspicion of having passed classified material to the website WikiLeaks.

Just as attacks have evolved, companies too must evolve by re-evaluating their own ability to detect, defend and respond to cyber attacks.

© 2013 KPMG International Cooperative ("KPMG International"), a Swiss entity. Member firms of the KPMG network of independent firms are affiliated with KPMG International. KPMG International provides no client services. No member firm has any authority to obligate or bind KPMG International or any other member firm vis-à-vis third parties, nor does KPMG International have any such authority to obligate or bind any member firm.
All rights reserved.

Various Attack Vectors

Cyber incidents can be loosely divided into three categories. The first category is accidental events due to human error, system failure or unanticipated accidents. The second category refers to unauthorised access into networks and systems by hackers or employees. The third category does not require actual access as it usually causes denial of service or loss of data.

Attack methods could involve complicated and coordinated efforts to beat the cyber security protection mechanism and intelligence reconnaissance, followed by social engineering techniques for acquiring of target information.

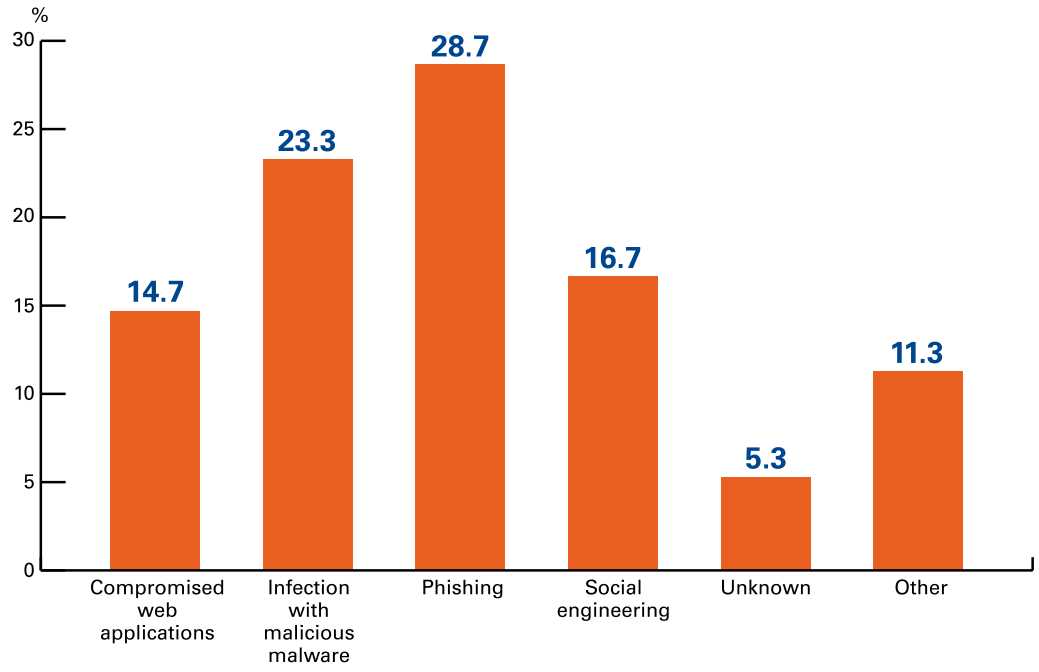
There are six most common types of security failings. These are shared accounts, weak passwords, lack of effective network monitoring, lack of effective Web monitoring, absence of logging and absence of log analysis. Lack of user awareness also provides more opportunities for social engineering attempts to succeed. Examples of such attempts include luring Internet users into execution of malware and Spear Phishing. (See Figure 3 below).

A group of attackers who are particularly good at social engineering is Anonymous. These hackers typically exploit easy-to-guess passwords of users or use emails to trick users into revealing confidential information or into clicking links which lead to the download of malicious software.

However, Anonymous is not the only group of people who are familiar with this technique. In fact, cyber criminals and state-sponsored attackers have been practising it for a far longer time. The stakes are also bigger for them as they stand to gain a whole lot more of important information.

Eddie Schwartz, chief security officer of the security firm RSA summed it up best during a security conference in San Francisco in 2012 when he said: "The attacks by them (Anonymous) pale in comparison to the nation-state stuff and the criminal element… The more eyes, the greater chance of success (for an attack)", which accurately depicts the cyber environment nowadays.

Figure 3: Methods of attack



Source: 2012 KPMG paper "A nuanced perspective on cybercrime".

© 2013 KPMG International Cooperative ("KPMG International"), a Swiss entity. Member firms of the KPMG network of independent firms are affiliated with KPMG International. KPMG International provides no client services. No member firm has any authority to obligate or bind KPMG International or any other member firm vis-à-vis third parties, nor does KPMG International have any such authority to obligate or bind any member firm. All rights reserved.

Impact on companies who fall prey to such attacks

The objectives of cyber attacks can be divided into two distinct categories. These are

- misappropriation and theft of intellectual property, financial data or other confidential information for monetary gain or to gain a competitive edge;
- corruption or disturbance of key business assets and processes for strategic purposes or to make an activism statement,

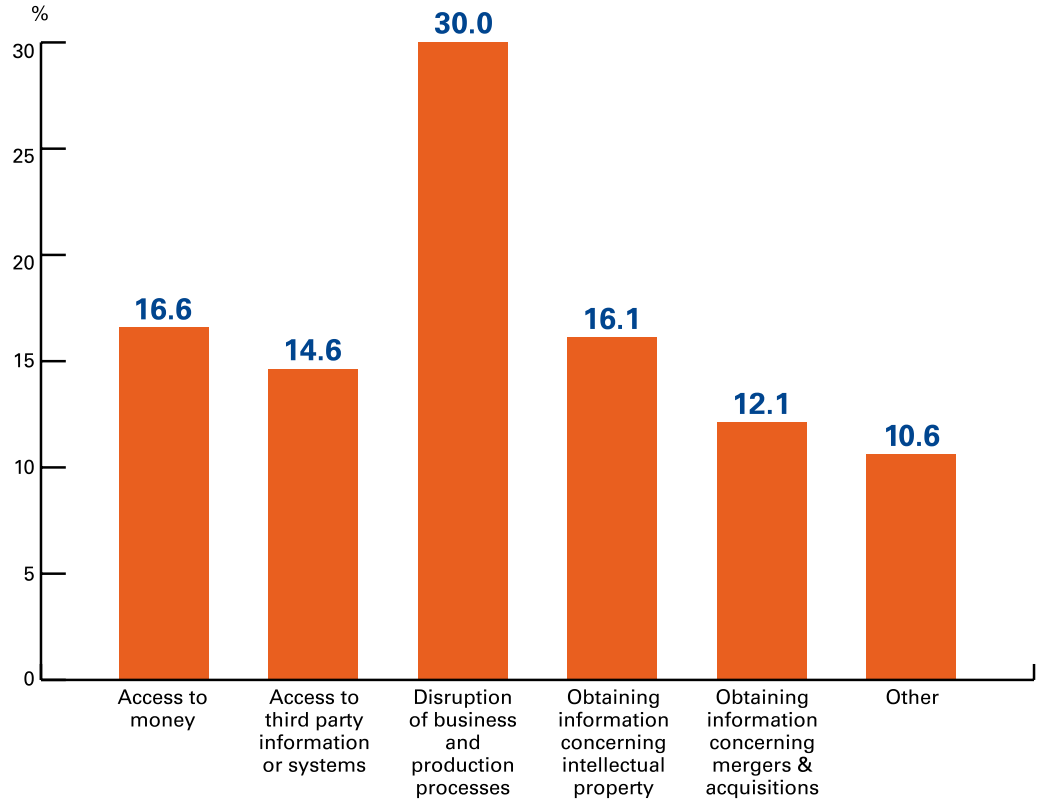
However, the actual impact on victim companies could be much broader and more profound.

More specifically, direct consequences of such attacks comprise disruption of business and production processes, unauthorised access to monetary operation, loss of intellectual property, disclosure of merger-and-acquisition deals, identity theft and compromising of customer data. Such attacks can also adversely affect third party partners in the industrial chain. (See Figure 4 below).

But all the above consequences are just the tip of the iceberg. Deeper financial and reputational impact further includes loss of competitive advantage in accessing new fields, failure to keep current clients and investors, losing deals and disputes (or winning them on unfavourable terms), regulatory fines, liability lawsuits, share price drops, costs involved in fixing business relationships and even negative international publicity.

In addition, the company would very likely be forced to spend more than usual to fix systems and repair damages. It is also very likely that costly fees will be incurred from services of third party experts and consultants for mitigation and recovery services. There could also be forced expenditure on personnel change, organisational restructuring and additional training.

Figure 4: Purpose of attack



Source: 2012 KPMG paper "A nuanced perspective on cybercrime".

© 2013 KPMG International Cooperative ("KPMG International"), a Swiss entity. Member firms of the KPMG network of independent firms are affiliated with KPMG International. KPMG International provides no client services. No member firm has any authority to obligate or bind KPMG International or any other member firm vis-à-vis third parties, nor does KPMG International have any such authority to obligate or bind any member firm. All rights reserved.

How companies can cope

The need for action

However, effective awareness requires continuous effort to remain vigilant. In this aspect the financial institutions seem to be doing a better job in understanding the potential "enemy" compared to the other industries, including the ENR sector.

The Obama administration submitted a cyber security proposal to Congress last May to outline its priorities for cyber security and to press lawmakers to pass comprehensive legislation to protect critical U.S. infrastructure that powers the Internet, utilities, and other control systems that are vulnerable to attack.

Feds Simulate Crippling Cyber security Attack On NYC Electricity [March 2012]

Advances in technology and mounting concern about the potential for a cyber attack to damage power stations, water-treatment plants and other critical systems have prompted senior officials to seek a more robust role for the department's Cyber Command. For one thing, cyber attacks can take place in milliseconds. The assailant may be unknown. The attack route may be hard to trace, crossing multiple countries.

Pentagon proposes more robust role for its cyber-specialists [August 2012]

Iran is to move key ministries and state bodies off the worldwide internet next month in an effort to shield them behind a secure computer wall from disruptive cyber attacks like the Stuxnet and Flame viruses. "The establishment of the national intelligence network will create a situation where the precious intelligence of the country won't be accessible to these powers."

Iran to unplug from Web to escape 'Internet monopoly' [August 2012]

The key is to be able to understand the motives behind a cyber attack. It must be made clear the cyber world is no longer playing in the "minor league", but rather the "major league" with players who potentially have access to unlimited resources and endless patience in achieving an aforementioned objective.

On a second note it is extremely necessary to conduct thorough analysis of risks and have a clear understanding of the different asset value perception. What seems of little value to one firm might be worth a lot more to attackers who have a totally different perspective or who are planning an attack on a chain of companies.

As a result, consideration should be given to the relationship between the costs for implementing detective controls and costs of incidents. The latter should include indirect damages incurred on consumer confidence and reputation, the two most valuable assets of a company.

A 2012 survey titled "A nuanced perspective on cybercrime" which was conducted by KPMG in Netherlands, stated that out of the 170 responding organisations under various sectors including ENR, approximately 19 percent of them spend more than 1.5 million euros on cybercrime prevention, detection and response per year.

Thirdly, whether short term measures or long term controls have been implemented, the upper management of companies should never be complacent and believe that they enjoy 100 percent security. The IT landscape in many modern organisations is simply often too complex for complete protection.

The same 2012 KPMG survey also revealed that 45 percent of companies experienced attempts of cybercrime attacks in 2011. In addition, 55 percent of respondents were unsure of whether they can effectively respond to a cybercrime attack, and only 20 percent said they can respond effectively to an attack but unfortunately do not have an attack response plan in place. Among all the responding corporates, approximately 30 percent have forensic capabilities as a control and only 55 percent have central incident and event monitoring capabilities.

Most importantly, it is vital for the management to set the correct tone. KPMG's experience with clients has shown over and over again that security is largely a management issue.

The survey also showed that more than 75 percent of respondents believe that fighting cybercrime goes beyond installing the needed technology to curb it. Some 90 percent of them also agree that cybercrime should be discussed at the board level.

© 2013 KPMG International Cooperative ("KPMG International"), a Swiss entity. Member firms of the KPMG network of independent firms are affiliated with KPMG International. KPMG International provides no client services. No member firm has any authority to obligate or bind KPMG International or any other member firm vis-à-vis third parties, nor does KPMG International have any such authority to obligate or bind any member firm. All rights reserved.

So are companies in the ENR industry up to the challenge?

Most respondents from the ENR sector of the same KPMG survey do not think so. They believe that hackers are more likely to win in this sector compared to other industries.

If a company does not consider itself to be ready, actions must be taken. Management should endorse prevention efforts and start seeking a structured approach.

There also has to be effective use of security monitoring and seamless cooperation between the different parties involved so that knowledge and expertise can be shared among government, business communities, IT security groups and even cross-border organisations.

Beyond the prevention of incidents, timely detection and an adequate response are also critical. If there is any major gap or deficiency in the policies, procedures and tools of a company, the worst time to discover these would be when a cyber security incident is already set on its course.

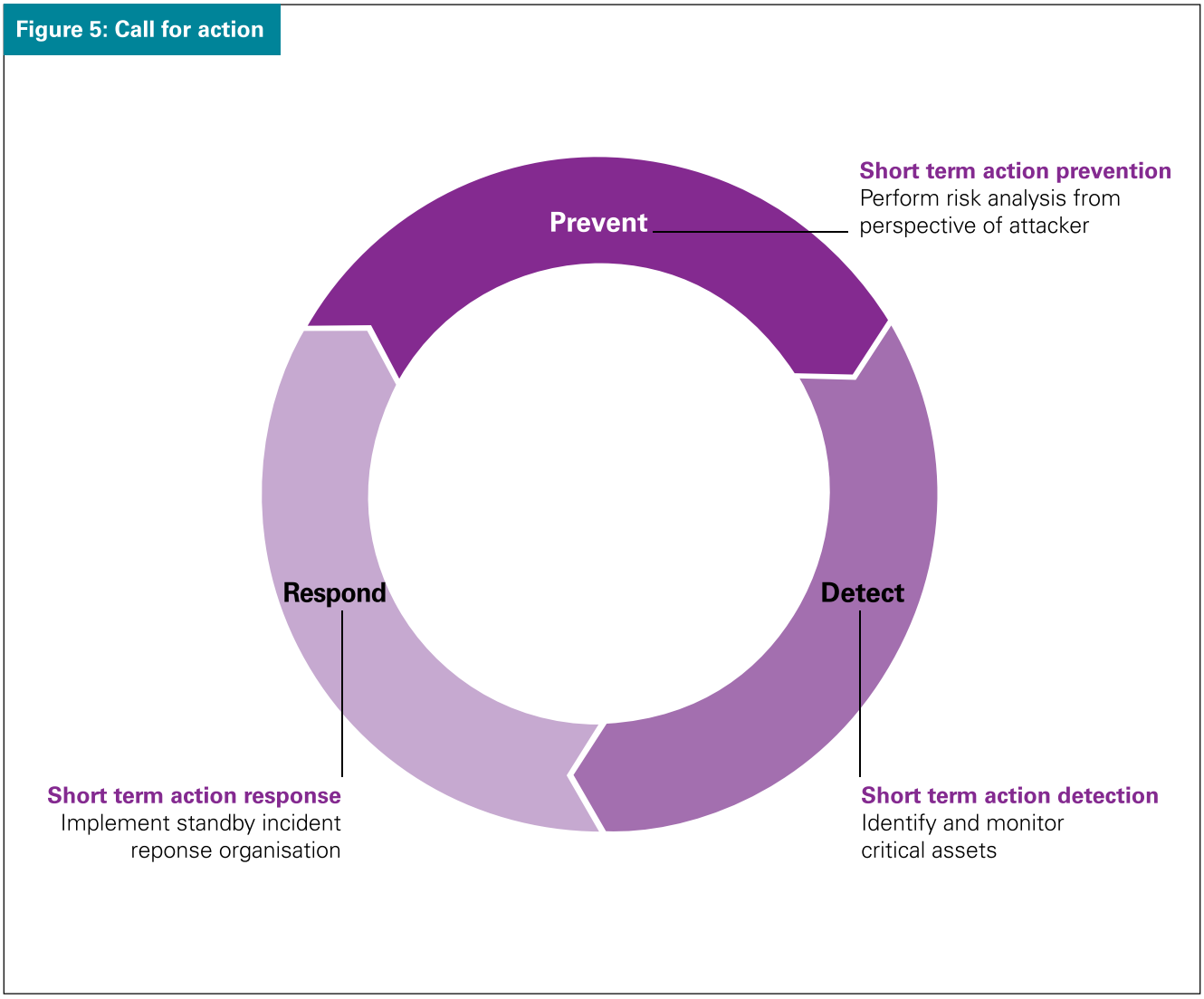
In terms of short-term actions, the company could perform risk analysis from the perspective of an attacker, identify and monitor critical assets as well as begin implementing a standby incident response team.

In the long run, companies should strive for cost-effective control of the cyber environment by addressing the domains of people, processes and technology.

Yet, even the most comprehensive security control system cannot guarantee the complete prevention of cyber incidents. An incident response plan and an emergency action plan is therefore also of paramount value in the proper handling of a security compromise and reducing the subsequent damage.

If a thorough and detailed plan is not available, the very least an organisation should do is to be familiar with some basic concepts and simple primary actions to respond to an incident. (See Figure 5 below). This helps the company achieve more effective business resilience, which is important especially for the protection of the most critical assets. The fundamentals of cybersecurity are probably best summed up by Ron Ross, National Institute of Standards and Technology (NIST) Senior Fellow, who said during a launch of NIST's latest guidance on security controls: "The fundamentals of cyber security … I call it the physics of security … don't change over time … how we apply those controls ... is a little bit different, but the same fundamentals."

Figure 5: Call for action



Source: 2012 KPMG paper "A nuanced perspective on cybercrime".

© 2013 KPMG International Cooperative ("KPMG International"), a Swiss entity. Member firms of the KPMG network of independent firms are affiliated with KPMG International. KPMG International provides no client services. No member firm has any authority to obligate or bind KPMG International or any other member firm vis-à-vis third parties, nor does KPMG International have any such authority to obligate or bind any member firm. All rights reserved.

Suggested frameworks

Given the shifting perspective of the defence against cybercrime, a more modern approach to cyber security therefore also focuses on the perspective of the criminals.

In terms of risk assessment, the organisation must not only consider itself as an attractive end target, but also consider its part in the supply chain. It should also not view itself as one entity that should be protected, but as a collection of processes, users and IT infrastructure.

Companies should focus on being well informed of (the character) of possible threats and invest in a proper defence. They should not do this in an isolated way, but rather use the knowledge and experience of colleagues in both the public and private sector. A joint response is essential for protection against cyber espionage, terrorism, crime and disruption of information and communication systems.

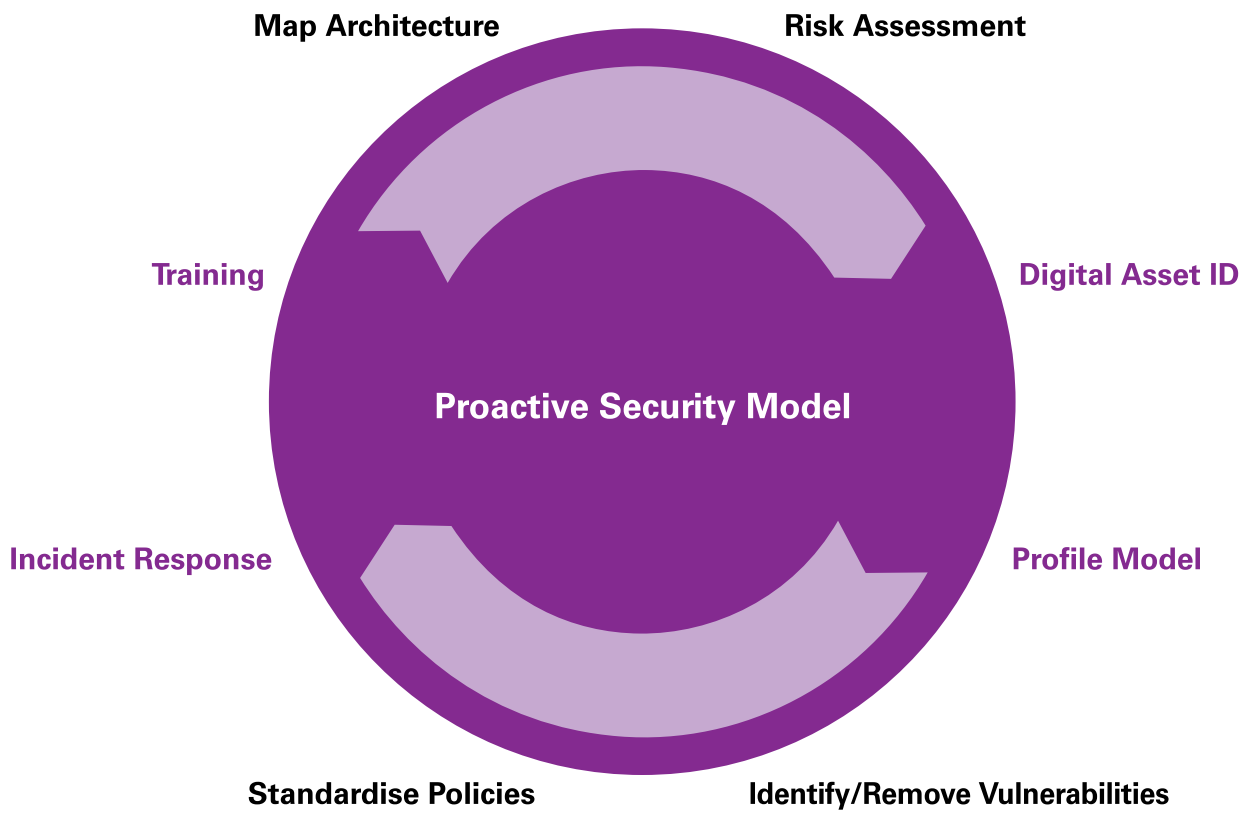
ICS-CERT Recommendation

With respect to the industrial control system, ICS-CERT[5] suggests a proactive security model as depicted in the Figure 6 below.

This model can be further complemented with a more detailed five-step approach in protecting information and records:

- Obtain executive sponsorship, establish a team, and determine the team's goal, objectives, and milestones - ensuring that these efforts are aligned with the goals of the business.
- Develop a training and awareness campaign. Policy content should be comprehensive, consistent and implemented with process changes and the introduction of appropriate controls and metrics to measure effectiveness and compliance.
- Assess the current state of the organisation's information protection efforts. Classifying the sensitivity of information should be a key goal.
- Design the desired state of information integrity protection, with the goal of establishing improved handling and protection practices that achieve policy requirements, lower business risk, and increase productivity.
- Implement the desired state. Enhanced process and data workflows, controls, and processes are a key outcome. The result is a programme that helps leaders ensure the risk-based protection of information assets.

Figure 6: Proactive Security Model



[5] The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) is part of the US Department of Homeland Security (DHS) and works to reduce risks within and across all critical infrastructure sectors.

© 2013 KPMG International Cooperative ("KPMG International"), a Swiss entity. Member firms of the KPMG network of independent firms are affiliated with KPMG International. KPMG International provides no client services. No member firm has any authority to obligate or bind KPMG International or any other member firm vis-à-vis third parties, nor does KPMG International have any such authority to obligate or bind any member firm. All rights reserved.

Real life case studies

There have been quite a few cases worldwide where KPMG applied the use of frameworks and helped different clients with their needs in achieving the goal of cyber security.

In the Dutch market, joint efforts of the financial sector are pretty successful in boosting awareness. Aside from cooperation between financial institutions and the Government, KPMG also actively shares experiences as part of the focused joint efforts.

Generally, there are three types of security controls: prevention, detection and response.

"KPMG in the Netherlands provides the banks with an update on the trends in cybercrime threats and potential solutions twice a year.

KPMG employs a global network of hundreds of information security specialists, which reaches virtually all major financial institutions worldwide.

Attack patterns observed at other banks and solutions applied by these institutions help to shape an image of upcoming attacks and solutions relevant for Company B.

Knowledge of the latest cybercrime attack trends and defence measures helps Company B to update the bank's defences on time in order to adequately respond to attacks."

© 2013 KPMG International Cooperative ("KPMG International"), a Swiss entity. Member firms of the KPMG network of independent firms are affiliated with KPMG International. KPMG International provides no client services. No member firm has any authority to obligate or bind KPMG International or any other member firm vis-à-vis third parties, nor does KPMG International have any such authority to obligate or bind any member firm.
All rights reserved.

In general, preventive controls are more popular than detective controls whereas detective controls are used more often than responsive controls, as in this case of how KPMG helped a company in the ENR industry.

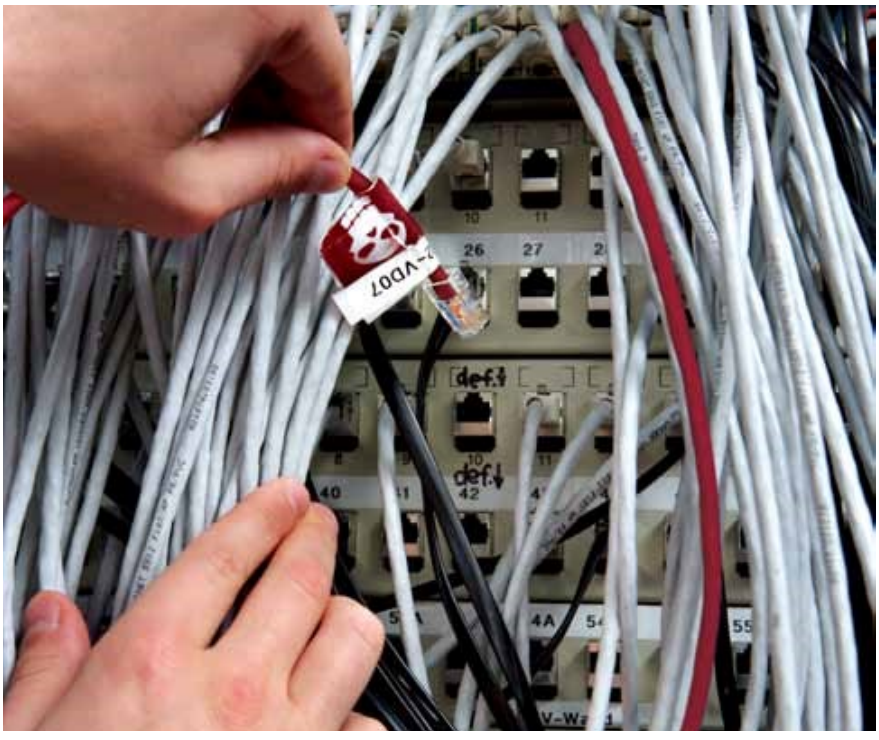
However, as discussed earlier, incidents cannot be avoided 100 percent of the time. This implies that detection and response are equally important and are thus the areas with the biggest room for improvement.

"Company Z is a well-known company in the oil, gas and natural resources industry.

KPMG firms' teamed with a technology partner provider to supervise one of the largest global implementations of a security monitoring platform. The platform correlates information about thousands of security events from numerous systems spanning across the globe.

A list of the most relevant cybercrime risks for Company Z was drafted in close cooperation with the organisation. For each risk, a set of detection rules was defined.

The ability to adequately respond is mainly achieved by properly established processes and governance. KPMG advised on governance structure, engineered new incident response processes and established training programmes for security personnel."



© 2013 KPMG International Cooperative ("KPMG International"), a Swiss entity. Member firms of the KPMG network of independent firms are affiliated with KPMG International. KPMG International provides no client services. No member firm has any authority to obligate or bind KPMG International or any other member firm vis-à-vis third parties, nor does KPMG International have any such authority to obligate or bind any member firm. All rights reserved.

Below is another example illustrating KPMG's experience in adequate and systematic response after a security incident has taken place:

"Company A was informed by a whistleblower that an attacker gained access to the company's website and/or closed environment. In response to this news the website was taken offline and KPMG was asked to assist.

- A collaboration of Forensic technology and IT security experts captured forensically sound images of the most critical servers to make sure no traces or evidence were lost.
- The images were analysed for traces in system files and properties, logs from firewalls were secured and analysed, KPMG also analysed all traffic to and from the compromised servers.
- The analysis showed that the perpetrator succeeded in creating and uploading several files to the web server that contained malicious code, allowing the perpetrator to send commands to the server from a remote location.
- KPMG helped the client by implementing remedial procedures and additional security measures, thus mitigating the risk of further damage and bad publicity."

Even if it is within an organisation itself, one way of improving the handling of specific cyber incidents related to industrial control systems would be to gather a group of staff to conduct brainstorming and collaboration exercises

During such sessions, staff from various departments will get to receive more adequate cyber security training, initiate effective inter-departmental interactions, and update antiquated policies and procedures. They can also get to identify and fix any security flaws found in the system, so as to create a corporate and organisational environment that is more resistant to cyber attacks.

© 2013 KPMG International Cooperative ("KPMG International"), a Swiss entity. Member firms of the KPMG network of independent firms are affiliated with KPMG International. KPMG International provides no client services. No member firm has any authority to obligate or bind KPMG International or any other member firm vis-à-vis third parties, nor does KPMG International have any such authority to obligate or bind any member firm. All rights reserved.

Conclusion

The battle against cyber crime is one which is difficult to win.

From the perspective of the Asia Pacific region, we understand that data security is not an easy concept for most business leaders to fully grasp. In part, this is because many organisations do not have a clear view on the actual value of their data and as a result, tend to follow a one-size-fits-all approach to data security.

At the same time, organisations in this region have also seen a gradual migration of their corporate value away from physical assets (such as facilities, products and people) towards digital assets (such as bid information, technology designs or customer data). Therefore, most businesses have robust crisis plans for events like floods, fires or sudden executive departures, but have very few for digital security issues.

An organisation in the ENR industry must stay as up-to-date as possible with security issues and set in place effective security measures. Beyond doing so, an ENR organisation must evaluate itself through the eyes of potential attackers so as to identify and protect parts which represent the highest substantial value.

The importance of executive leadership and support in developing a data security strategy cannot be overstated. The risk of data loss should be a board-level issue and not a challenge isolated to the IT department and risk managers. This means that executives must not only 'walk the walk' when it comes to complying with protocols, but also actively participate in the development of security to ensure that the rules reflect the priorities of the business. Most importantly, executives must strive to institutionalise continuous improvement mechanisms to ensure that they learn from hard-earned lessons of the past.

Should a cyber security transformation be undertaken, the five recommended objectives would be to Prevent, to Prepare, to Protect, to Remediate and to Integrate and Transform.

However, given the scope and complexity of the challenge, it is not surprising that most executives are left wondering how best to approach the issue without dampening productivity or expending scarce resources.

It is important that executives in the Asia Pacific region balance a cautious approach to IT security with the downside and damage that can be caused by the lack of being able to carry on business as normal and the loss of confidential and sensitive information.

© 2013 KPMG International Cooperative ("KPMG International"), a Swiss entity. Member firms of the KPMG network of independent firms are affiliated with KPMG International. KPMG International provides no client services. No member firm has any authority to obligate or bind KPMG International or any other member firm vis-à-vis third parties, nor does KPMG International have any such authority to obligate or bind any member firm. All rights reserved.

References

Internal

A NUANCED perspective on cybercrime – Shifting viewpoints — call for action	http://www.kpmg.com/TT/en/IssuesAndInsights/ArticlesPublications/Documents/Nuanced-Perspective-on-Cybercrime-Art.pdf
Publish and be Damned	http://www.kpmg.com/UK/en/IssuesAndInsights/ArticlesPublications/Documents/PDF/Advisory/Forbes-Survey-publish-and-be-damned.pdf
KPMG Global Energy Institute — Shamoon and Cyber Security in the Energy Industry	http://www.visualwebcaster.com/imageSlides/90364/GEI%20Presentation%20110812%20(Color).pdf
Information Integrity — Improving and Protecting Data Quality, Access, and Value	http://www.kpmg.com/US/en/IssuesAndInsights/ArticlesPublications/Documents/information-integrity.pdf

© 2013 KPMG International Cooperative ("KPMG International"), a Swiss entity. Member firms of the KPMG network of independent firms are affiliated with KPMG International. KPMG International provides no client services. No member firm has any authority to obligate or bind KPMG International or any other member firm vis-à-vis third parties, nor does KPMG International have any such authority to obligate or bind any member firm.
All rights reserved.

External

FBI — Combating Threats in the Cyber World Outsmarting Terrorists, Hackers, and Spies	http://www.fbi.gov/news/speeches/combating-threats-in-the-cyber-world-outsmarting-terrorists-hackers-and-spies
Fact Sheet: Safeguarding the U.S. Government's Classified Information and Networks	http://www.whitehouse.gov/the-press-office/2011/10/07/fact-sheet-safeguarding-us-governments-classified-information-and-network
CF Disclosure Guidance: Topic No. 2	http://sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm
INDUSTRIAL CONTROL SYSTEMS — CYBER EMERGENCY RESPONSE TEAM : Monthly Monitor April 2012	http://www.us-cert.gov/control_systems/pdf/ICS-CERT_Monthly_Monitor_Apr2012.pdf
INDUSTRIAL CONTROL SYSTEMS - CYBER EMERGENCY RESPONSE TEAM : Monthly Monitor September 2012	http://www.us-cert.gov/control_systems/pdf/ICS-CERT_Monthly_Monitor_Sep2012.pdf
Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies	http://www.us-cert.gov/control_systems/practices/documents/Defense_in_Depth_Oct09.pdf?
ICS-TIP-12-146-01A—TARGETED CYBER INTRUSION DETECTION AND MITIGATION STRATEGIES	http://www.us-cert.gov/control_systems/pdf/ICS-TIP-12-146-01A.pdf
Security and Privacy Controls for Federal Information Systems and Organizations	http://csrc.nist.gov/publications/drafts/800-53-rev4/sp800-53-rev4-ipd.pdf
National Infrastructure Protection Plan - Energy Sector, published by the Department of Homeland Security in June 2006	http://www.dhs.gov/xlibrary/assets/nipp_snapshot_energy.pdf
Ron Ross on Revised Security Controls	http://www.govinfosecurity.com/articles.php?art_id=4572
Global Energy Cyberattacks: "Night Dragon"	http://www.mcafee.com/sg/resources/white-papers/wp-global-energy-cyberattacks-night-dragon.pdf
Security To Industry – Time To Wake Up	http://www.isssource.com/security-toindustry-time-to-wake-up/
7 Steps to ICS Security	http://www.isssource.com/wp-content/uploads/2012/02/022912WP-7-Steps-tolCS-Security-v1.0.pdf
Iran Blamed for Cyberattacks	http://online.wsj.com/article/SB10000872396390444657804578052931555576700.html
U.S. looks into claims of security flaw in Siemens gear	http://www.reuters.com/article/2012/08/22/ctech-us-cybersecurity-siemens-idCABRE87L02F20120822
Iran to unplug from Web to escape West's 'Internet monopoly'	http://www.rt.com/news/iran-internet-intranet-security-938/

© 2013 KPMG International Cooperative ("KPMG International"), a Swiss entity. Member firms of the KPMG network of independent firms are affiliated with KPMG International. KPMG International provides no client services. No member firm has any authority to obligate or bind KPMG International or any other member firm vis-à-vis third parties, nor does KPMG International have any such authority to obligate or bind any member firm. All rights reserved.

External

Iranian state goes offline to dodge cyber-attacks	http://www.telegraph.co.uk/news/worldnews/middleeast/iran/9453905/Iranian-state-goes-offline-to-dodge-cyber-attacks.html
Pentagon proposes more robust role for its cyber-specialists	http://www.washingtonpost.com/world/national-security/pentagon-proposes-more-robust-role-for-its-cyber-specialists/2012/08/09/1e3478ca-db15-11e1-9745-d9ae6098d493_story.html
RSA 2012: Aging industrial control systems increasingly vulnerable to cyberattack	http://www.infosecurity-magazine.com/view/24384/
Federal Cybersecurity Incidents Rocket 650% In 5 Years (October 04, 2011 01:25 PM)	http://www.informationweek.com/government/security/federal-cybersecurity-incidents-rocket-6/231700231?itc=edit_in_body_cross
Feds Simulate Crippling Cybersecurity Attack On NYC Electricity	http://www.informationweek.com/government/security/feds-simulate-crippling-cybersecurity-at/232602280
The Bright Side of Being Hacked	http://www.nytimes.com/2012/03/05/technology/the-bright-side-of-being-hacked.html
Connecting The Dots After Cyberattack On Saudi Aramco	http://bits.blogs.nytimes.com/2012/08/27/connecting-the-dots-aftercyberattack-on-saudi-aramco/
Virus Shuts Rasgas Office Computers	http://www.bloomberg.com/news/2012-08-30/virus-shuts-rasgasoffice-computers-lng-output-unaffected-1-.html
Cyber attack takes Qatar's RasGas offline	http://www.arabianbusiness.com/cyber-attack-takes-qatar-s-rasgasoffline-471345.html
Definition — Spear Phishing	http://searchsecurity.techtarget.com/definition/spear-phishing
CYBER RISK AND THE ENERGY INDUSTRY	http://incelaw.com/ourknowledge/publications/cyber-risk-and-the-energy-industry
Library: Energy and Utilities Industry: Threats, Needs, and the Aanval Solution	http://wiki.aanval.com/wiki/Library:Energy_and_Utilities_Industry:_Threats,_Needs,_and_the_Aanval_Solution

© 2013 KPMG International Cooperative ("KPMG International"), a Swiss entity. Member firms of the KPMG network of independent firms are affiliated with KPMG International. KPMG International provides no client services. No member firm has any authority to obligate or bind KPMG International or any other member firm vis-à-vis third parties, nor does KPMG International have any such authority to obligate or bind any member firm.
All rights reserved.

The KPMG Global Energy Institute (GEI):
Launched in 2007, the GEI, is a worldwide knowledge-sharing platform detailing insights into current issues and emerging trends within the Oil & Gas and Power & Utilities sectors. Energy professionals will have access to valuable thought leadership, studies, events and webcasts, about key industry topics. A regional focus to the GEI provides decision makers tailored insight within the Americas, Asia Pacific and the Europe, Middle East & Africa regions. The GEI strives to arm professionals with new tools to better navigate the changes in this dynamic arena. To become a member of the GEI or for more information please visit kpmg.com/energyaspac

The KPMG Global Energy Conference:
The KPMG Global Energy Conference (GEC) is KPMG's premier event for financial executives in the energy industry. Presented by the KPMG Global Energy Institute, these conferences are held in both Houston and Singapore and bring together energy financial executives from around the world in a series of interactive discussions with industry luminaries. The goal of these conferences is to provide participants with new insights, tools, and strategies to help them manage industry-related issues and challenges.

For more information please visit kpmg.com/energyaspac

#KPMGGEC

Global Power Conference
The KPMG Global Power & Utilities Conference is KPMG's premier event for CEOs, divisional heads and financial executives of the power and utilities sector presented by KPMG`s Global Energy and Natural Resources Practice. For inquiries regarding the KPMG Global Power & Utilities Conference please contact the conference organizing team at gpc@kpmg.com or visit kpmg.com/powerconference

© 2013 KPMG International Cooperative ("KPMG International"), a Swiss entity. Member firms of the KPMG network of independent firms are affiliated with KPMG International. KPMG International provides no client services. No member firm has any authority to obligate or bind KPMG International or any other member firm vis-à-vis third parties, nor does KPMG International have any such authority to obligate or bind any member firm.
All rights reserved.

Contact us

Pek Hak Bin
Partner
Head of Energy & Natural Resources Practice
T: +65 6411 8138
E: pekhb@kpmg.com.sg

Brett Hall
Partner, Management Consulting
Singapore
T: +65 6411 8335
E: bretthall@kpmg.com.sg

Lyon Poh
Partner, Management Consulting
Singapore
T: +65 6411 8899
E: lpoh@kpmg.com.sg

Rajnish Kapur
Director, Management Consulting
Singapore
T: +65 6507 1973
E: rajnishkapur@kpmg.com.sg

KPMG Services Pte Ltd
16 Raffles Quay #22-00
Hong Leong Building
Singapore 048581
T: +65 6213 3388
F: +65 6223 3118

kpmg.com/energyaspac
kpmg.com/social media

The views and opinions expressed herein are those of the author and do not necessarily represent the views and opinions of KPMG LLP. The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity.

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act upon such information without appropriate professional advice after a thorough examination of the particular situation.

© 2013 KPMG International Cooperative ("KPMG International"), a Swiss entity. Member firms of the KPMG network of independent firms are affiliated with KPMG International. KPMG International provides no client services. No member firm has any authority to obligate or bind KPMG International or any other member firm vis-à-vis third parties, nor does KPMG International have any such authority to obligate or bind any member firm. All rights reserved.