"A CYBER ATTACK PERPETRATED BY NATION STATES OR VIOLENT EXTREMIST GROUPS COULD BE AS DESTRUCTIVE AS THE TERRORIST ATTACK OF 9/11,"

LEON PANETTA, US SECRETARY OF DEFENSE, OCTOBER 11TH 2012

CYBER 9/11: IS THE OIL & GAS INDUSTRY SLEEPWALKING INTO A NIGHTMARE?

TIM HAÏDAR | EDITOR IN CHIEF | OIL & GAS IQ | 2015

FOREWORD

Oil and Gas Cyber Security: The Mammoth Cost Of Not Being Prepared

Cyber Security within the oil and gas industry is a threat that is, in many cases, being ignored. It has a direct effect in the creation of government regulation and legislation, can have deep financial impact and – in some cases – can even cost lives.

The US ICS-CERT recognises these trends and are listing a growing number of attacks launched on Industrial Control systems. It further states that:

- 53% of cyber-attacks in the USA are aimed towards the energy sector
- 30% of malware gets through precautionary measures
- 55% of incidents involved advanced persistent threats (APT).

The 2014 Verizon Data Breach report states that 40 per cent of the attacks performed in the manufacturing and mining industry are cyber espionage based. A UK survey revealed that 81 per cent of large companies were digitally attacked, at an average cost of £1 million per company. Similarly, 62 per cent of small and medium-sized enterprises (SMEs) were digitally attacked in 2014 at an average cost of more than £100,000 per incident. Eventually, even your company will be a target and the cost of unpreparedness could be crippling.

We have to realise that the reasons why people, governments and critical infrastructure are attacked via computers is fivefold:

- It is relatively easy
- It is cheap
- It can be catastrophically effective
- It is forensically difficult to trace
- It pays no heed to state jurisdictions of frontiers.

IT Security is a continuous process. And it is necessary to focus your investment not only on solutions helping you to **protect** your valuable assets but also to **monitor, detect** and **respond** to cyber threats. **Simply putting more locks on your door will not make it more secure...**

Maturing a company's security infrastructure is a challenge but can be made efficient by applying a so-called Cyber Security Maturity Model. A step-by-step model that helps to achieve the desired level of risk mitigation and cyber security resilience. So you can be prepared!

Ronald Prins
CTO &Co-founder
Fox-IT

FOX IT
FOR A MORE SECURE SOCIETY

> *"A CYBER ATTACK PERPETRATED BY NATION STATES OR VIOLENT EXTREMIST GROUPS COULD BE AS DESTRUCTIVE AS THE TERRORIST ATTACK OF 9/11,"*
>
> **LEON PANETTA, US SECRETARY OF DEFENSE, OCTOBER 11TH 2012**

Thus spake the former White House Chief of Staff to President Clinton, Director of the Central Intelligence Agency and Chief Executive Officer of the most powerful defense establishment on Earth.

And that was three years ago.

In the 29 months after Panetta's warning, the energy industry has been cited as the most vulnerable sector of global business to the threat of cyber attack. Statistics out of the US show that between April 2013 and 2014, threat actors hit 53 per cent of energy companies.

Cyber attacks are costing the energy sector in the UK some $700 million a year. The Shamoon virus took the world's largest oil producing company out of action for almost a fortnight. A lot can happen in three years.

In this special report, we seek to analyse the clear and present danger presented by the "ticking time bomb" that is the threat of cyber warfare, cyber espionage, cyber crime and hactivism in the oil and gas industry. If it is a case of "if" and not "when", what are the solutions to mitigate disaster? And will we even know what has hit us until we are reeling in shock?

The present day

The dawning of the Information Age has brought untold advantages to global business, with the ability to communicate hitherto inconceivable amounts of data to the four corners of the Earth in the blink of an eye.

The digitisation or "computerisation" of the work environment has allowed for the flow of information to be both seamless and instantaneous, creating the phenomena that we have come to know as "big data" and the "Internet of Things".

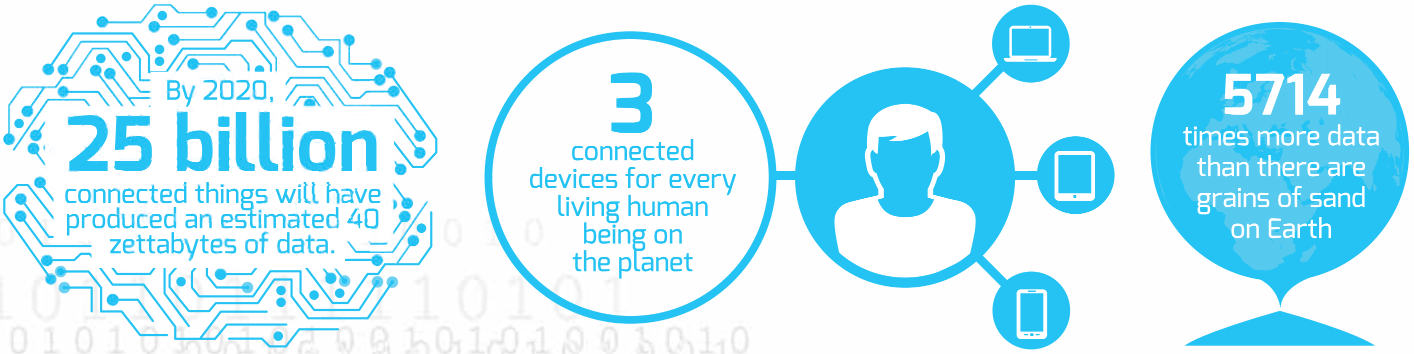
The digital universe is set to double every two years[1], and by 2020, 25 billion connected things[2] will have produced an estimated 40 zettabytes of data[3].

To put that into perspective, that is three connected devices for every living human being on the planet, and 5714 times more data than there are grains of sand on Earth

Within the oil and gas industry itself, the amounts of data handled on a daily basis is enormous. That advent of the digital oilfield has meant that companies that used to keep logs on reams of paper, now have to warehouse electronic information in super-cooled data centres.

In 2011, Jay R. Pryor, VP of Sales for supermajor, Chevron, disclosed that his company's data footprint was growing at a rate of two terabytes a day, when the entire company only held five terabytes of data in 1997. A large oil field may be outputting as much as 10 gigabytes of data a day, and a large refinery up to a terabyte. Pryor asserted that Chevron was managing "as much data as Google", and that amount will have at least quadrupled in the past four years..

But with new opportunities come new threats. Multinational professional services network, PricewaterhouseCoopers, published that in 2014 there were 6,500 reported cyber attacks involving companies in the oil and gas industry. That is an attack rate of some 540 per day and a 179 per cent increase on the year before.


By 2020,
25 billion
connected things will have produced an estimated 40 zettabytes of data.
3
connected devices for every living human being on the planet
5714
times more data than there are grains of sand on Earth

[1] http://www.emc.com/collateral/analyst-reports/idc-the-digital-universe-in-2020.pdf
[2] http://www.gartner.com/newsroom/id/2905717
[3] http://www.emc.com/collateral/analyst-reports/idc-the-digital-universe-in-2020.pdf

A history of violence

Although digitisation has been a growing trend for the past two decades, the history of cyber attacks - both self-inflicted and of external origin - has long been a feature of the oil and gas industry. Here are some of the most prevalent and insidious attacks to date.

1982 - Siberian pipeline sabotage

The CIA placed deliberate flaws in control system software stolen by Russia, leading to a massive pipeline explosion in June. Leaked extracts in the Washington Post describe how the operation caused "the most monumental non-nuclear explosion and fire ever seen from space". The chip which caused the explosion is named "The Logic Bomb".

1992 - Disgruntled employee strikes back

A sacked Chevron employee manages to disable emergency alert protocols spanning 22 states in the contiguous USA. This is only noticed once an emergency situation is underway and the alarm is not triggered.

2000 -Gazprom network nullified

A spokesperson for OAO Gazprom, the world's largest extractor of natural gas, announced that hackers within the Russian state had managed to seize control of the company's entire natural gas pipeline network.

2009 - In the lair of the Night Dragon

Beginning in November 2009, a series of on-going cyber attacks based out of China were targeted at the global oil and gas sector. Involving a host of tools and techniques from spear-phishing attacks to exploitation of Microsoft Windows operating system vulnerabilities and the use of remote administration tools (RATs), these attacks were calculated not to maim but to purloin.

Night Dragon sought to harvest sensitive information pertaining to everything from specific field operations to upcoming licensing bids and project tenders. The objective of this illicit data acquisition? Ransom or sale to the highest bidder.

2009 – The dawn of Operation Aurora

A sophisticated cyber espionage operation based out of the People's Republic of China attempted to siphon intellectual property from major multinationals including Exxon Mobil, ConocoPhillips, and Marathon Oil.

2010 Stuxnet - The game changer

The Stuxnet worm attacked automation systems at Iran's Natanz nuclear facility, halting progress on the country's uranium enrichment program. The computer worm is considered the world's first cyber weapon, infecting up to 12 million computers in China. Supermajor, Chevron, later reveals that it too was a victim of Stuxnet.

Stuxnet changed the playing field because it was the first malware agent to be discovered that could hide from, spy on and subvert industrial automation systems with its own programmable logic controller (PLC) rootkit.

Stuxnet could attack SCADA and industrial control systems (ICS) and reprogram them to gradually self-destruct, which is exactly what it did to centrifuges at the heart of the Iranian nuclear programme.

2012 - Setting the world aFlame

This modular computer malware burrowed into Iran's oil ministry, severing internet links to rigs and the hub for nearly all the country's crude exports, causing widespread data loss. At the time of discovery, Flame was described by the CrySyS Lab as "the most sophisticated malware we encountered during our practice; arguably, it is the most complex malware ever found."

2012 - Shamoon landing

This "Trojan Horse" stole data and wiped files, in an attack that disabled 30,000 terminals at Saudi Aramco, the national oil company of Saudi Arabia and world's largest oil producing corporation. Shamoon takes RasGas, the second largest producer of liquefied natural gas (LNG) in Qatar completely offline. This attack was referred to by U.S. Defence Secretary, Leon Panetta, as the most destructive to have ever hit any sector of business.

2013 - Cyber DEFCON 2

The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), part of the U.S. Department of Homeland Security, issued a series of three "amber alerts" to warn of ongoing cyber attacks against natural gas pipeline companies. These attacks are spread over a period of two weeks and target the operators of gas compressor stations.

2014 – HAVEX has a go

A hacking group based out of Russia and calling itself "Energetic Bear", launched a campaign to infect energy and industrial firms around the world with a malicious remote access Trojan (RAT) codenamed HAVEX. This malware had the ability to shut down major power grids, and oil and gas pipelines.

2014 – Norway succumbs

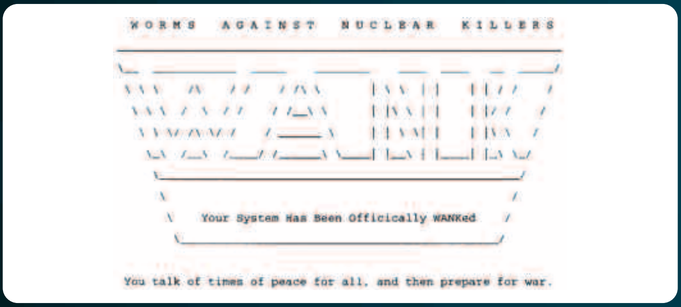
The Norwegian government announced that more than 50 Norwegian oil and energy companies were hacked by unknown assailants. Another 250 firms were advised by the authorities that their networks and systems may have been compromised in the largest cyber attack to have taken place in the country's history.

The Four Horsemen of the Cyberpocalypse

All of the major attacks that have been perpetrated since the Logic Bomb exploded some 33 years ago fall into four categories of assault. Some are more prevalent than others in the 21st century cyberspace and are the province of state rather than civilian actors.

Hacktivism

Defined as the act of "breaking into a computer system for a politically or socially motivated purpose", the term was coined in 1994 by "Omega" of computer hacker and media organisation, "Cult of the Dead Cow". Despite this, the first instance of hacktivism occurred some five years earlier in 1989, when anti-nuclear campaigners attacked DEC VMS computers over the DECnet with the so-called "WANK worm". The attack bore the following message:



```
WORMS    AGAINST    NUCLEAR    KILLERS

     Your System Has Been Officically WANKed

You talk of times of peace for all, and then prepare for war.
```

Hackers can loosely be assigned into three groups:

- **White hat hackers** – These so-called "ethical hackers" are computer security specialists who infiltrate protected systems and networks to assess their security.
- **Grey hat hackers** – These individuals or entities have an ambiguous code of ethnics, and neither commit acts of hacktivism for their own personal gain nor to cause damage.
- **Black hat hackers** – The bad guys. This genre of hacktivist violates computer security for personal gain or with malicious intent.

Hacktivism really came to the fore in 2008, when the international network of hacking entities known as Anonymous perpetrated "Project Chanology"[4], a campaign of damaging online activities aimed at the Church of Scientology.

Better connectivity, the expansion of social media and the availability of ready-made hacking tools across the worldwide web has exponentially widened the franchise of the wannabe hacktivist. Since 2011, the hacktivism landscape has moved away from Anonymous and towards regionalised combines of state and/or civilian actors with a particular geopolitical bent[5].

Cyberwarfare

The information-based equivalent of conventional warfare, this is internet-centred conflict involving politically-motivated attacks on information and information systems.

Conducted by both state and civilian actors, cyberwarfare can target national militaries, and the state, private and non-governmental sectors for the purpose of sewing the seeds of discontent and destruction at home or abroad.

In 2013, Peter W. Singer, former Director for 21st Century Security and Intelligence at the Brookings Institution asserted that there were 100 nations in the world today "building some kind of cyber-military capability"[6], and when it came to those countries that would be able to carry out a prolonged cyberwar rather than a single devastating attack, there were "less than 20 and maybe even fewer than 10"[7].

Cyber espionage

The practice of obtaining information by unauthorised and clandestine means from individuals, groups and governments for personal, economic, political or military ends via a range of internet and network-based techniques.

Unlike one-off cyber attacks, these are lengthy, persistent and target-explicit incursions conducted using Trojans and spyware to procure specific sensitive information.

Cybercrime

The broad-brush definition of a cybercrime is "any criminal activity that is facilitated by means of a computer or network."

In 2014, global computer security software company, McAfee gave a conservative estimate for the cost of global cybercrime at $375 billion[8] - that is roughly the same as the GDP of Thailand[9]. The majority of cybercrime consists of fraudulent financial behaviour based around phising and social engineering scams.

> "McAfee gave a conservative estimate for the cost of global cybercrime at $375 billion - that is roughly the same as the GDP of Thailand."

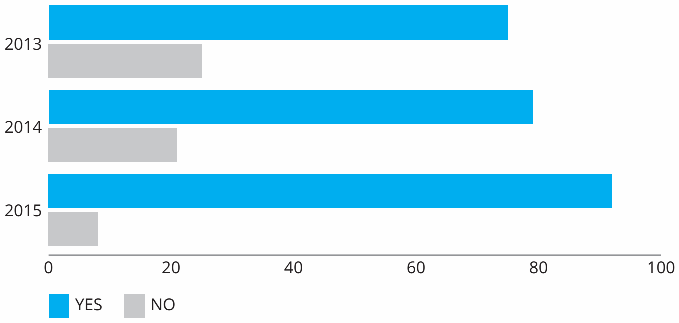
[4] http://en.wikipedia.org/wiki/Project_Chanology
[5] https://www.rsaconference.com/writable/presentations/file_upload/ht-t10-hacktivism-in-2015-_it-isnt-just-for-the-_lulz-anymore_final.pdf
[6] http://www.popsci.com/article/gadgets/few-questions-peter-w-singer-about-future-cybersecurity
[7] http://intercrossblog.icrc.org/blog/what-everyone-needs-know-about-cyber-warfare
[8] http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf
[9] http://bit.ly/1aG7zoC

The industry speaks

In the course of the past three years, we have concentrated on asking the IT and cyber security portions of the oil and gas community about the current state of play within their sphere of influence. The findings of these surveys show the evolving nature of threats within the sector and uncover some alarming trends within the cyber security space.

Threat levels

DO YOU DEEM CYBER ATTACKS TO BE A MAJOR THREAT TO THE OIL AND GAS INDUSTRY?

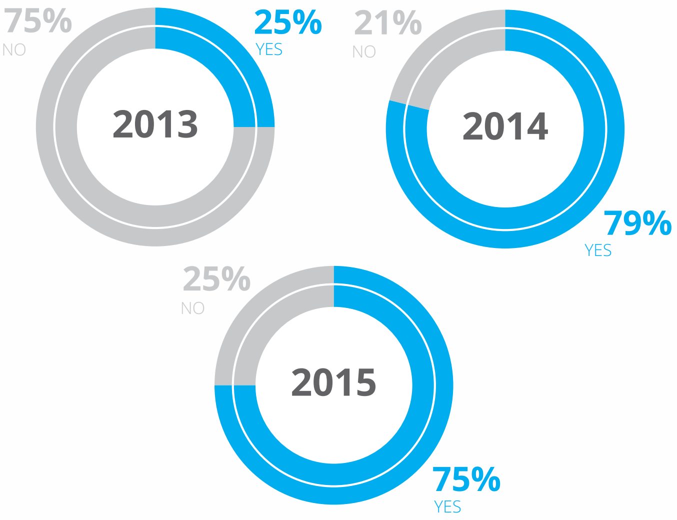


When we began our ongoing series of cyber security investigations in 2013, it is debatable which of the statistics involved in our lead question is the most disquieting: the fact that three quarters of the IT professionals surveyed found that there was, indeed, a clear and present danger presented by cyber attacks on the oil and gas sector, or the fact that one quarter did not.

In 2014, the number that believed that the oil and gas sector was not in major danger from cyber attacks waned to one in five people, and more than halved in 2015 to a mere eight per cent of respondents, with nine out of every ten IT professionals believing that the hydrocarbons industry was firmly in the crosshairs for a major cyber event.

Increasing frequency

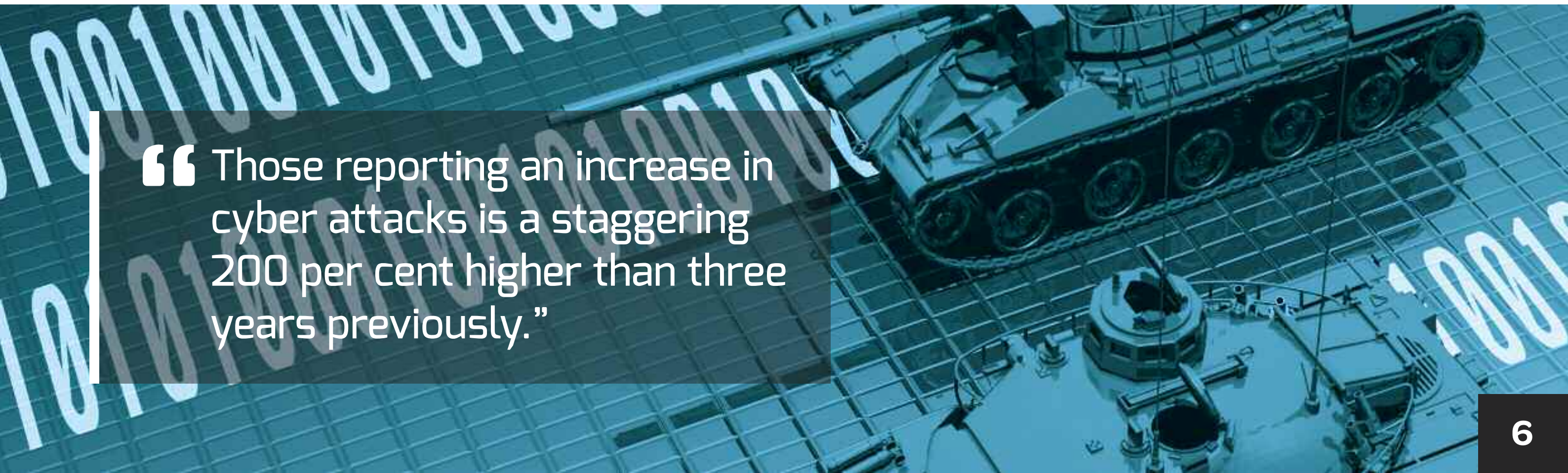
HAVE YOU SEEN A SIGNIFICANT INCREASE IN CYBER ATTACKS IN THE PAST 12 MONTHS?



It is no wonder that the most recent set of statistics has seen 92 per cent of IT professionals ascribing to the major threat stance.

The trend in the frequency of cyber attacks since our first inquest in 2013 has been nothing short of parabolic. A 25 per cent increase from 2012 to 2013 was eclipsed the very next year; when respondents saw a further 79 per cent rise in attacks in the 12 months from 2013 to 2014.

By 2015, the statistics for increased cyber attacks had become the inverse of their 2013 levels. In the year of this report's publication, the rise in those recording an increase in cyber attacks is a staggering 200 per cent higher than three years previously.

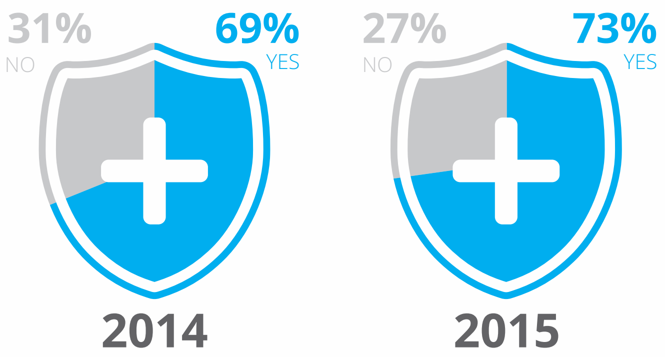


> Those reporting an increase in cyber attacks is a staggering 200 per cent higher than three years previously."

The industry speaks

Fighting back….or not

DOES YOUR ORGANISATION HAVE A CYBER SECURITY TEAM?

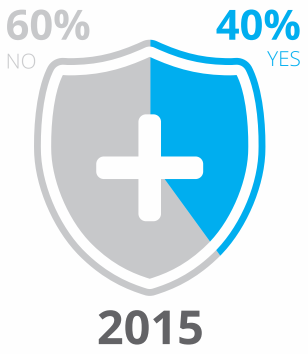


So, despite three successive years of increasing cyber attacks and 92 per cent of IT professionals believing that the oil and gas industry is under major threat in the cyber realm, statistics garnered in the last two years have shown that some 27 per cent of companies still do not have an in-house cyber security team.

Although seemingly counter-intuitive, this is another reflection of a sector where IT capabilities have long been seen as a contractor-worthy function rather than a core internal process.

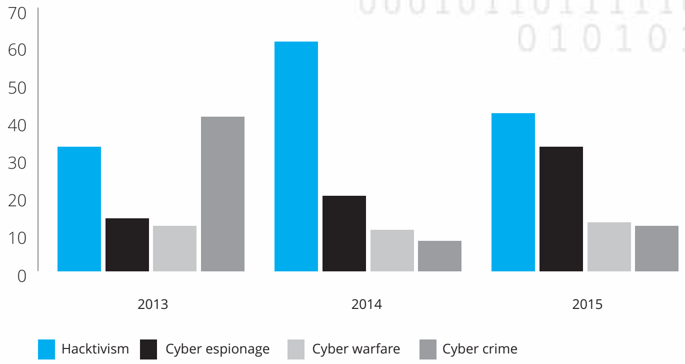
Add to the mix the fact that almost two thirds of oil and gas companies do not have an organised framework to address and manage the aftermath of a security breach or attack, and you have the ideal witches brew for the inability to correctly combat a cyber incursion.

DOES YOUR ORGANISATION HAVE AN INCIDENT RESPONSE PLAN IN PLACE?



The lead Horseman

WHICH CYBER THREAT SOURCE ARE YOU MOST CONCERNED ABOUT?



In the past three years we have seen a dramatic change in which of the Four Horsemen have spooked the oil and gas industry the most. Despite 2012 seeing the Shamoon attack wreak havoc in the Middle East, the single most pressing concern for cyber professionals within the oil and gas sector was the threat of cyber crime, with two out of every five respondents affirming that this was their main focus. Despite the hacktivist group, "The Cutting Sword of Justice", claiming responsibility for the Shamoon incursion[10], only a third of those surveyed deemed hacktivism to be their biggest concern.

A year later, this viewpoint had radically changed. In 2014, cyber crime had dropped to become the least threatening of the Four Horsemen for IT professionals, supplanted by the scourge of hacktivism, which three in five cited as their main preoccupation. Cyber espionage grew by six percentage points to worry a fifth of respondents, and the threat of cyber warfare lost one per cent to be the prime worry of around one in ten of those surveyed.

At 42 per cent, hacktivism was still the most menacing Horseman of 2015, although its perceived threat had dropped by some 19 per cent. Cyber espionage continued its upward trend becoming the greatest concern for one in three IT professionals, up from one in four the previous year. Cyber warfare and cyber crime increased by two and four percentage points respectively, to become the key tribulations of approximately one in ten people.

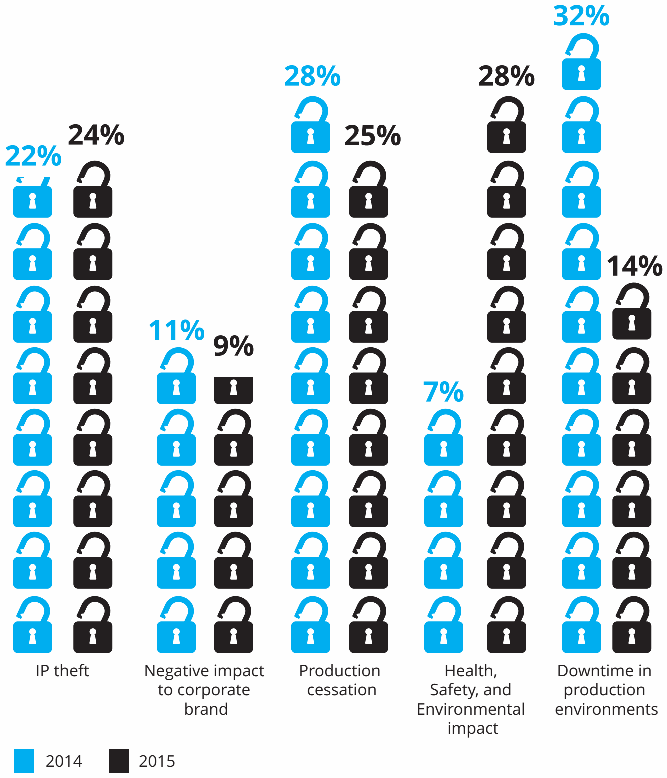
Interestingly, cyber warfare, one of the most widely hyped and reported forms of cyber malfeasance, was the least of our respondents' fears across all three years, averaging just 12 per cent from 2013 through 2015.

[10] http://www.nytimes.com/2012/12/10/business/global/saudi-aramco-says-hackers-took-aim-at-its-production.html

The industry speaks

Biggest fear

WHAT ARE YOU MOST AFRAID OF IF A CYBER ATTACK HAPPENS?



Now we look at the results when we asked IT professionals about their nightmare scenario: what happens if and when a cyber attack actually hits a company. In 2014, just less than a third of IT professionals surveyed believed that production downtime was the worst possible outcome of a successful cyber assault on their organisations, followed by total production cessation, which scored 28 per cent of the votes.

Intellectual property theft, the target of the Night Dragon attacks in 2009, came in as the third of the five concerns outlined in the survey, followed by brand denigration and health and safety (HSE) issues.

In 2015, these opinions had shifted dramatically. Heading up the nightmare list was the possibility of HSE-related breaches, four times more prevalent amongst our respondents than the year before. This may well have to do with the low oil price environment and the fact that oil price downturns usually entrain periods where health and safety is compromised[11].

Across both years, the potential for IP theft and negative repercussions on brand remained at the same level, being the primary anxiety for around one quarter and one tenth of respondents respectively. In both years, three of the five categories scored more than 20 per cent, showing that the industry's preoccupations are evenly focused on several core business capabilities.

Conclusion?

Cyber attacks have increased 200 fold since 2012, to the extent where now only eight per cent of IT professionals consider their companies to be impervious to a major cyber incident. Despite this alarming statistic, one in four oil and gas companies still lack an in-house cyber security department, and almost two in three have no codified incident response plan.

The principal form of cyber attack that companies are worried about is hacktivism, with just under half of all respondents over a three year period signalling that the threat of growing and evermore pervasive individuals and organisations in this space was their most pressing concern.

[11] [THE BOARDROOM] "Watch This Space….A Lower Oil Price Could Mean More Fatalities"

Living The Worst Day

Beginning in the 1970s and crystallised in the seminal "Scenarios: Uncharted Waters Ahead" , and "Scenarios: Shooting the Rapids" , Shell's French strategist, Pierre Wack, laid down the roots for scenario planning in the oil and gas industry.

In the operational excellence fold, many professionals suggest that working to the ideal of your "best day" is the most beneficial way to go about shaping the organisation that you want and not the one you get left with.

Aiming for a take on both of these tropes, we are looking at "The Worst Day" in a cyber security context: what this may look like as it unfolds and what mitigation efforts should be in the event of this nightmarish situation occurring.

We asked Ronald Prins, Chief Technology Officer & Co-founder of information technology security consultancy Fox-IT, what he believed to be the constituent parts of "The Worst Day" and the fight back afterwards.

Ronald was a scientific researcher at the Netherlands Forensic Institute (NFI), where he gained recognition by breaking codes on cryptographic security systems encountered by law enforcement in criminal investigations. He co-founded FOX-IT with fellow NFI forensics specialist, Menno van der Marel, in 1999.

SPEAKER KEY

TH - **Tim Haïdar,** *Editor in Chief,* Oil & Gas IQ

RP - **Ronald Prins,** *Chief Technology Officer & Co-founder,* FOX-IT

TH **Ronald, 92 per cent of IT professionals believe that their companies are living in the shadow of a serious cyber threat. How should we be going about cyber security to make sure our businesses are safe?**

RP I think, first of all, that we should be defining the difference between what we mean by "safety" and "security". Safety involves the accidental and unplanned, security is where you have actors actively trying to abuse your environment. What you are seeing more and more is actually that maintaining "security" codes for "safety".

We all know what happened recently with the Germanwings plane. The typical political response to that kind of incident is asking if we can replace the pilot with a computer which would have prevented this happening. This is something which is happening in oil and gas - especially if you focus on your operational excellence. You want to run cheaper and more effectively so a common response will be to introduce more computers.

This is something we see across all sectors - replacing people with a technique or technology. People seem to forget that process itself introduces a new inherent security risk.

Computer systems are multiplying at the core of global businesses - even using standard Windows systems. Take TV5Monde: this French TV station went black because they had a Windows computer in the master control room where they combine all their television feeds. Five years ago it was still an analogue system, and they replaced this "defunct" technology with modern computers which the hackers also had a backdoor into. They made themselves an easy target.

On the IT structure side, we're actually getting weaker and from the attacker side they're getting stronger and stronger. You are even seeing nation states investing heavily in building up knowledge and skills and buying stuff like Zero-day attacks. In many countries we are seeing nascent military groups building up capabilities in this field. There is a negative movement underway.

RP The worst day really begins with waking up and knowing that things haven't been what they seem for a number of weeks. You've found out there is something fishy going on in your networks and you've tried to stop that and clean it. Then you find out that, actually, once that is done, the next day all of your systems start to go down or misbehave. Then you know you are in the midst of something big. You are no longer in control of your network, somebody has taken it over.

We've seen examples of nation-state actors where they were able to penetrate their viruses not only onto a hard disk as an infectious programme, but also burrow into the firmware of computers. Although you run a re-installation of the computer, the next time you boot it up, the IOS will affect the hard drive again and the same virus will continue to multiply.

The scary thing is that you will have no idea as to the veracity of what's going on with the dashboards in front of you. Readouts these days are nearly all computer-based and not dials and gages. The same as in a modern car - there's no direct connection between your right foot on the gas pedal and the mechanics of the car anymore, there's a computer in between.

[12] https://hbr.org/1985/09/scenarios-uncharted-waters-ahead
[13] https://hbr.org/1985/11/scenarios-shooting-the-rapids/ar/1
[14] Implementing Changes In Leadership Thinking And Behaviours To Drive Operational Excellence In Oil And Gas

You may begin to see strange behaviour in the physical environment - things are not directly exploding but breaking down. However, on your screens everything is green-lit, and you have no way of actually controlling what's happening within the physical facility.

There is a real-world example of this which happened with Stuxnet in the Natanz nuclear facility in Iran. The dashboards said that everything was running as normal but at the physical level there were centrifuges exploding.

People will nearly always respond as if there is the possibility to implement a manual fix - there might be some valve we can shut down or something to that effect. But are you actually going to find people who are willing to step into a facility when they have no idea if it might go up in smoke in the next ten seconds? From a safety perspective it's actually unsafe to go inside and attempt to intervene in the physical environment.

I've had a number of discussions with people working in the downstream oil and gas environment, and the consensus is that if you cannot trust what the computers are saying then there's a potentially hazardous situation going, and you are prohibited from entering the physical environment.

Now, while that might be adequate from a safety perspective, it certainly is not from the security point of view. If system A is being affected, it is just as easy to affect system B.

TH **Yet our research has shown that as much as 60 per cent of oil and gas companies do not even have an incident response plan in place.**

RP That is a truly frightening statistic. An oil and gas company would always have a contingency plan if there was a loss of containment, or if a physical attack took place, why not a cyber attack?

A lot of IT experts are investing in continuity - a backup system which can take over in the case of a primary system failure - but in an overwhelming number of cases, these backup systems are just a carbon copy of the primary system.

Now while that might be adequate from a safety perspective, it certainly isn't from the security point of view. If system A is being affected, it is just as easy to affect system B.

TH **So what should Plan B look like?**

RP I always try to explain to people that your fallback option should be something from the past, a throwback to ten years ago, for example: a piece of kit from a different technological era which you can trust in a different way. People may think that, from a resource perspective, this may not be effective because it will mean you need different people to manage, test and operate that obsolete system, but it's actually your best chance of surviving.

TH **As a journalist, you might have a tablet or laptop, but it's always good to have a pen and paper as a fallback option. You can't crash a notepad.**

RP Exactly!

TH **Can you give us a real-life example of the worst day as it happened?**

RP Yes, well, let's take an example of an episode we encountered. We saw a huge infection in the oil and gas industry in the Middle East. It consisted of a wiping action and a destruction action, most probably conducted by a state actor. It was not a direct targeted attack on process control systems but against a Windows-centred office environment - where people were carrying out daily web and email based activities.

However, within the office environment, the company had an SAP system, where employees have the ability to interact with a common corporate database for a wide range of applications. This SAP system is crucial to assets and the process control environment, because that's where people who are working on maintenance get their tickets for pending jobs and find out when and where parts need replacing et cetera. Now, if this system is down for, let's say, four weeks, then there's no way of actually doing maintenance in your refinery and that means that you get pushed into a shutdown. You just have no idea if things could go catastrophically wrong.

That's one example of where you do not even have to perpetrate a direct attack on the downstream environment to have an impact on your physical operations. You can do that with an attack on a 30 man office hundreds of miles away.

TH **We've talked about the things that can go wrong, how do you fight back in the security room?**

RP During a crisis everybody is in the dark, sometimes literally. It can take weeks or months to find out what systems have been penetrated, who's behind the attacks and what their objectives are. The best way to get an answer to these questions is by conducting an "upstream investigation" - tracking back to the source of where the perpetrators initially came from.

This is usually something that law enforcement or intelligence or a government organisation, should be involved with. You can search your own network and do all the analysis you want, but there are legal restrictions on how much you can do to locate the origins of an assailant, and that is where all the answers lie.

Only once we have laid our hands on this part of the attacker's substructure will we get an idea of where they have been inside your networks, what they have stolen, and whether they have still any capability to do something destructive at a later date.

In many countries, this is difficult from the outset, because maybe the attacker's source IP address is in a different country, and we immediately come up against jurisdictional issues. Most countries still lack a mature understanding of how you need to fight back in this instance. In fact, it is only the countries that have explored the potential of online conflict themselves, that are truly aware of how to actually prevent these kinds of attacks coming home.

In 2014, the UK decided to spend £2 billion on cyber security - that's 100 times more than the Netherlands is doing. In the UK there's an accreditation scheme where you have private security companies that have been vetted and screened and accredited to be involved in instant response actions. That's the kind of cooperation that is crucial to solving this problem.

TH **So, would you classify an IT-wary oil and gas sector as an area of global business with an undeveloped understanding of cyber security?**

RP Well, I always say that oil and gas is the most mature sector when it comes to cyber security, and that's because of geopolitical reasons. All of the big companies have former intelligence people working for them to do analysis on the threat side and formulate responses. However, there is a massive difference between the bigger multinationals and the rest of the oil and gas world. And just because the sector might have a mature awareness of the problems, it does not mean they have a mature attitude of how to tackle it.

There are two things you really need to do this well: awareness of what could happen, and experience of having undergone a cyber crisis to see how you respond and what can be done better. Unfortunately, you need disasters to learn from, you can't do it all just sitting behind your desk.

Another big issue is that we are incapable of validating if we are actually prepared. In the oil and gas industry, risk assessment is very much based on what's been learnt in the safety field - a kind of check-box mentality. This doesn't work for the cyber security environment.

People make mistakes. People will still bring in a laptop which contracted a virus in an external office environment into the place of work, where it should never be connected to an internal network. That's how you cause havoc in a facility which has no connection to the outside web. In an age of mobile computer technology, air gap is just a myth.

Things like red teaming are really important and that is what we are increasingly seeing at the more aware oil companies. It's the only way of actually finding out if you are in control of your own cyber security space.

Red teaming is not about assessing whether it is possible for a hacker to get in and actually shut down something; that's always possible. What we need to test is how good your defence and detection mechanisms are. This should be conducted in secrecy so the least number of people know that the red team exercise is going on and it isn't viewed as a simple drill.

TH **Despite all of this, we both know that one of the greatest possible threats to an organisation is presented not from without but from within. That disgruntled employee, that malignant internal force. Can you tackle that?**

RP That's a tough question actually. I think there's always going to be the possibility that employees take matters into their own hands. We should really look at our system administrators or network administrators and try to make sure that no one person is actually tied in to a single account to manage the whole system.

In many cases of cyber espionage, the ultimate end is to try to steal credentials. We should be looking at limiting the influence of the single individual within a network.

TH **Are there any other areas of industry that oil and gas sector can learn from?**

RP The financial sector. Banks actually have very good sharing platforms to discuss this kind of thing. Their platforms are really effective, with the security and fraud teams working together because they have common threat actors. They've made a decision that although they are competitors, they are better off fighting these forces together.

Unfortunately, I think the only way this kind of framework will come together in the oil and gas sector is if there are more focused incidents targeting the industry. Sometimes we have to lose to win.

"In an age of mobile computer technology, air gap is just a myth."

The solutions – thanks, in part, to science fiction

Have an incident response plan (IRP) in place

In 1980, the Alexander J. Kielland platform capsized killing 123 people. On that fateful evening, there were 14 minutes between the initial failure of one of its legs and the rig's eventual capsize. These were 14 minutes in which the majority of those on board could have escaped to safety.[15]

The report into the disaster cited that the majority of those aboard the rig could have survived had there been a codified command structure and emergency response framework to follow. Lack of preparation cost lives on the night, and a lack of preparation will cost you dearly when a cyber attack occurs.

Don't buy into the air gap myth

Air gap refers to computers or networks that are not connected directly to the civilian internet. Traditionally, air-gapped systems were believed to add a layer of security to a network, with an attacker needing to gain physical access to computers within the network to cause a security breach.

The SCADA-focused HAVEX worm attack of 2014 showed that mobility and the "Internet of Things" (IoT) have put paid to the supposed air gap safety net[16], and with the expansion of real-time connectivity capabilities, no network can truly be an island.

Currently, nine per cent of companies in the oil and gas realm are segregating their IT and operational technology (OT) networks by air gap alone[17]. Whilst that is better than the 19 per cent that have no separation between IT and OT at all[18], air gap is by no means a secure method of isolation from malware.

Make sure Plan B is based in "obsolesced technology"

Now, bear with me here. In the cult science fiction blockbuster Independence Day, the world is attacked by a highly-advanced alien civilisation with a mastery of hyper dimensional travel and high-tech weaponry[19]. These alien assailants have a backdoor into the best humanity has to offer in terms of coded transmissions. Their craft are impervious to conventional weapons and even nuclear warheads.

Once the remaining forces of the human race have discovered the key to destroying their extra-terrestrial aggressors, they transmit an attack plan to the four corners of the Earth to assemble for one last ditch offensive. And that message is sent using a system of electrical pulses developed in 1836: Morse code.

When planning for a back up strategy in case your primary network goes down, take the Independence Day route, and roll back to a system from the technological past that is both dependable and dissimilar from your principal operating system.

Don't put all your cyber eggs in one cyber basket

Sci-fi again, and *spoiler alert klaxon* for those who haven't seen a film made 20 years ago. In the cult dystopian classic Twelve Monkeys, a genetically-engineered virus is unleashed on humanity, causing the deaths of 99 per cent of the world's population, and forcing the remainder of the human race to live a troglodytic existence.[20]

A convict has been sent back from the future to try and stop the virus's initial introduction into the biosphere, but said time-travelling jailbird has no prior knowledge of who exactly released the virus in the first place. To cut a long story short, there are a number of suspects implicated in the virus's outbreak, but the perpetrator eventually turns out to be one of the assistants in the virology lab where the virus was created.

The moral of the story is not to give any one person the keys to the kingdom, lest they use said influence for evil, are subverted from a righteous path or unwittingly targeted by those who seek to do evil.

Learn to see the world through the eyes of the opposition

The practice that became known as "red teaming" originated in the military, when the father of the United States Air Force, Brigadier General Billy Mitchell, used bombers to sink battleships in a war game scenario in 1921.

For the past 90 years, the practice of stepping into the enemy's shoes has been a staple of military preparedness. In cyberspace, where conventional warfare is being waged in the digital domain, a similar practice of assuming the guise and gait of your adversaries is an advisable tactic.

To beat 'em, join up – the needs of the many

The old saying goes that two heads are better than one - in the cyber security space, this is no different. Pooling of knowledge to fight common actors is, ultimately, in the interest of all concerned. As Spock once said in seminal sci-fi flick Star Trek II: The Wrath of Khan: "The needs of the many outweigh the needs of the few or the one".[21]

As well as this information sharing taking place in the private sector, it is important to make sure that a corroborative channel is open with the government. We can find an example of this in the recent proactive congressional action on infosharing, enacted in the US to stymie future cyber breaches.[22]

Learn from thy neighbour

The 17th century English poet, John Donne, told us that "No Man Is an Island".[23] Similarly, no business vertical can be judged in remote dislocation from the rest of the corporate world.

The oil and gas industry has a bad rap in terms of cross-sector learning – adoption and adaption from other industries will have to take place should the sector wish to prevent and avoid future cyber calamity.

[15] Never Say Never Again by Derek Park (2011)
[16] HAVEX Proves (Again) that the Airgap is a Myth: Time for Real Cybersecurity in ICS Environments
[17] Is Your Company's Cyber Security Actually Good Enough?
[18] Is Your Company's Cyber Security Actually Good Enough?
[19] Independence Day, Twentieth Century Fox Film Corporation (1996)
[20] Twelve Monkeys, Universal Pictures (1995)
[21] Star Trek II: The Wrath of Khan, Paramount Studios (1982)
[22] White House Cybersecurity Information Sharing Initiative a Positive Step Forward
[23] Meditation XVII, John Donne, Devotions upon Emergent Occasions (1623)

Epilogue

The world, in uncommon unison, was left reeling from the events that took place on that fateful day in September 2001.

As the fourteenth anniversary of that tragedy creeps ever nearer, those who remember the scenes unfold throughout the day will have certain images indelibly emblazoned on their memories.

Cyber 9-11 is coming, and it's a "when" and not "if" scenario. It is debatable whether anybody can be totally prepared for an event of such magnitude, but our research has shown that the oil and gas industry is, unfortunately, often unprepared in its basic prevention and mitigation abilities.

Cyber 9-11 may be ineluctable, but the ability to fight back on 9-12 is scarcely possible in the current state of play.

CYBER 9/11: IS THE OIL & GAS INDUSTRY SLEEPWALKING INTO A NIGHTMARE?

Introducing Oil & Gas IQ

Oil & Gas IQ is the online portal dedicated to producing in-depth, value-adding content for the global oil and gas business. We represent one of the world's fastest growing online communities throughout the oil and gas world.

We provide industry professionals and senior business decision-makers with exclusive information, news and trends through videos, event presentations, articles, podcasts, webinars, online seminars and conferences.

We communicate with over 100,000 premium members weekly, and a wider community of 250,000 senior executives on a monthly basis with timely value-adding content, essential industry analysis and exclusive in-depth insights.

Visit www.OilandGasIQ.com today and become a member of the world's only full spectrum Oil and Gas community

Our Contributors

Shell
Chevron
bp
Schlumberger
BR PETROBRAS
TOTAL

Our Columnists

Our Content

TEN COMMANDMENTS
FOR BUILDING AND IMPLEMENTING AN EFFECTIVE LOCAL CONTENT STRATEGY
urbanpol

Oil & Gas iQ

www.OilandGasIQ.com

Is your company prepared for cyber security threats?

Fox IT, security is a continuous process

- **Protect** your assets
- gather **Intel**
- **Monitor** and **Detect** cyber threats
- Prepare to **Respond**

FOX IT
FOR A MORE SECURE SOCIETY

For more information on Fox-IT and how to become Cyber Security Resilient **www.fox-it.com**