PROTECTING
OPERATIONS
IN THE
ENERGY
SECTOR
AGAINST
CYBER
ATTACKS
Simple | Smart | Speed
CHOOLS

Driven by rising costs in exploration and production as well as by increasing competitive intensity and regulatory pressures, oil and gas companies are looking for new ways to increase production capacity and operational efficiencies. This has led to the rapid adoption of digital technologies to help run their organisations.

As these technologies are implemented across oil and gas operations, they are creating what is now called the Digital Oilfield. It is the result of a convergence between IT and operational technology (OT), and represents a new way of doing business that is helping oil and gas companies reduce operational costs, improve efficiency and production, and comply with regulations.

At the same time, this transition to the Digital Oilfield is exposing companies to serious risks from cyber attacks, putting production, reputation, and ultimately profits at risk. Today, more than ever before, a successful attack can lead to devastating consequences for infrastructure, intellectual property and corporate profitability.

THE ENERGY SECTOR'S VULNERABILITY TO CYBERCRIME

Security threats are expected to grow in the future. In the past four years alone, the financial impact of cybercrime has increased by nearly 78% and the time it takes to resolve a cyber attack has more than doubled.1 Across all industries and geographies, it has been estimated that cybercrime costs some $400 billion in lost time and assets.2

The oil and gas industry is certainly not immune to this threat. According to Ponemon, companies in energy and utilities recorded average annual costs due to cybercrimes of $19.78 million, second only to firms in the defence industry. An ABI Research study predicted that globally, cyber attacks against oil and gas infrastructure will cost companies $1.87 billion by 2018.

Given that a US survey3 found that 40% of all cyber attacks have been against energy sector companies, it is hardly surprising that this state of affairs is poised for change. According to IDC Energy Insights, security concerns are already ranked number nine among its "Top 10" oil and gas industry issues in 2012.4

Oil and gas companies are high-risk targets for many reasons. Malicious actors seek to accomplish political or economic goals. Disgruntled employees want revenge. Others want financial gain or access to valuable, proprietary data on reserves and discoveries. Whatever the motivation, high downtime costs and attack frequency rates necessitate strong cybersecurity protocols.

MIGRATING TO THE DIGITAL OILFIELD

The Digital Oilfield fuses two different technologies together using open IT protocols: operational technology (OT) with supervisory control and data acquisition (SCADA) and back office enterprise IT systems.

SCADA controls complex industrial processes, from oil and gas production and centralised monitoring to the control of hundreds of thousands of geographically dispersed meters and sensors. They are connected via IP networks to allow companies to continuously process real time information.

Oil and gas companies also depend on digital distributed control systems (DCS) to control refining processes and PLCs (programmable logic controllers) for industrial equipment and processes.

Companies are realizing vast gains from insights and actions as data is integrated and analysed in real time. For example, Digital Oilfield instrumentation is enabling horizontal drilling and multilateral wells. Sensors allow superior surveillance of pipelines. And real-time visibility into operations allows companies to better control costs and optimise the performance of employees, assets and facilities.

Modern two-way radio technologies are IP-based and are enabling greater workforce efficiency and safer work practices by offering integrated field voice and data communication services. Advanced radio systems such as P25 and TETRA can be integrated with SCADA and back office IT systems to promote efficient work processes and enhanced management of critical assets.

But the combination of open standard based IP protocols and integration into back office systems also puts companies at considerable risk to cyber attacks.

78%

FINANCIAL IMPACT OF CYBERCRIME

$19.78 MILLION

ANNUAL COST OF CYBERCRIMES IN ENERGY AND UTILITIES COMPANIES

40%

ATTACKS HAVE BEEN AGAINST ENERGY SECTOR COMPANIES

COMPANIES ARE REALISING VAST GAINS AS DATA IS INTEGRATED AND ANALYSED IN REAL TIME

CYBER THREATS ARE GROWING IN NEW WAYS AND PLACES

The convergence of SCADA and IT environments is not the only security issue causing concern. Successful attacks in the form of viruses and worms have demonstrated that companies often underestimate the vulnerability of diverse systems.5

Newer technologies such as those controlling drilling rigs and cloud-based services are subject to probes or attacks. So too are once-isolated plant control systems that are now integrated with corporate networks or vendors. Even private smartphones and devices used by company employees potentially open up business's network to an increasing number of threats and malicious behavior. Such threats can target data at rest on the device and can be introduced through online web surfing (96% of all mobile devices do not have encryption protection6).

In short, wherever there is digitally enabled technology or an intelligent device, even a simple device that controls a valve on the pipeline, there is a risk of it being used as a portal and taken over without authorization.7 Cyber criminals are targeting the entire spectrum of potentially valuable data: data at rest, data in transit, and data in use.

While IT and OT share many similarities, it is important to highlight some unique characteristics of OT systems. OT comprise SCADA systems that monitor and control critical infrastructure, threats against which have real consequences such as: personal injury, catastrophic equipment damage, lost production capacity, environmental impact or violation of legal and regulatory requirements.

THREATS AGAINST IT AND SCADA SYSTEMS

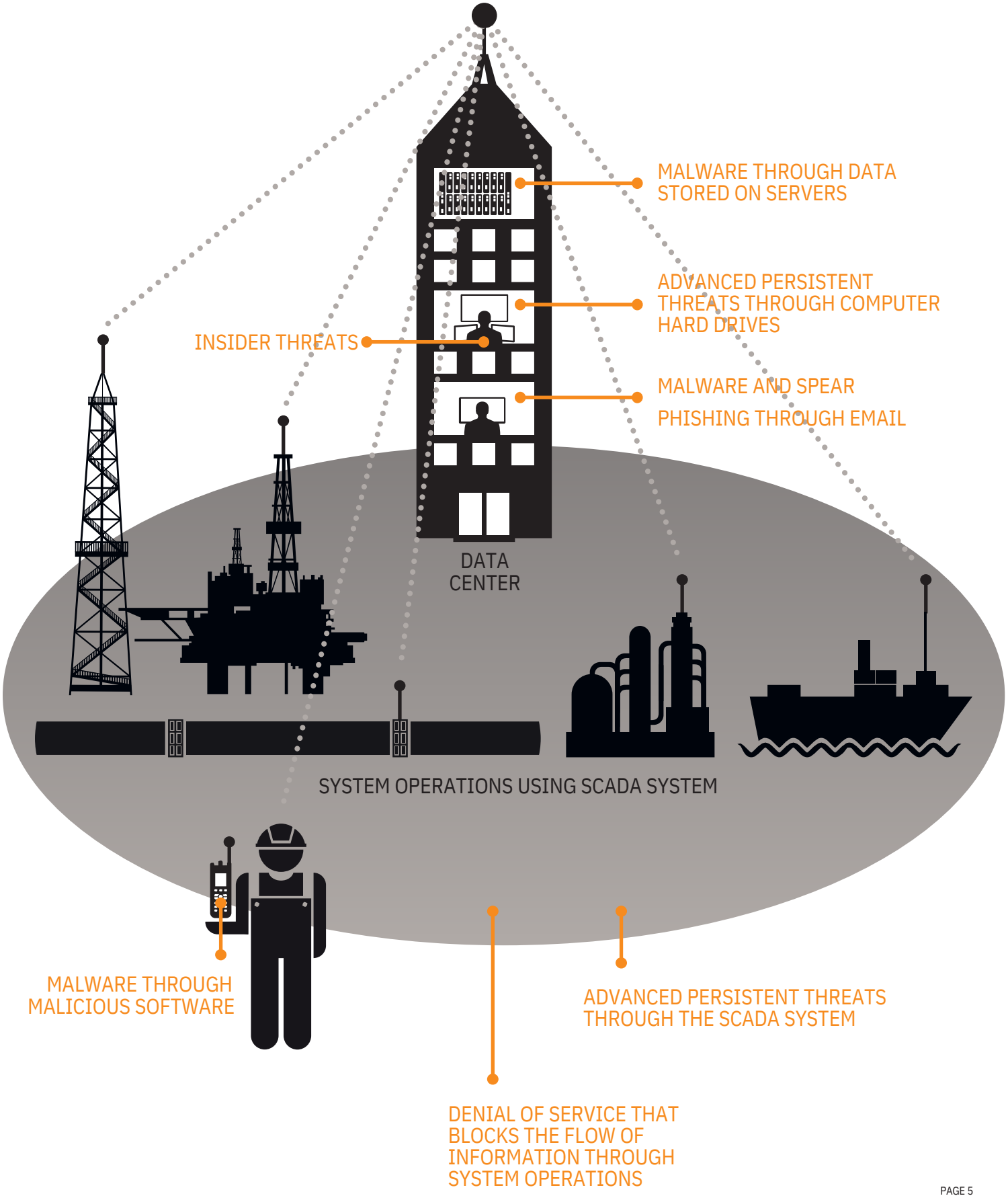
Threats against IT and SCADA systems can come from a wide range of sources, some of which are adversarial such as hostile governments, while others are from natural sources such as human errors and accidents. Data breaches committed by these sources can come from a variety of threat actions, some of which are discussed below.

TOP 10 MOST CRITICAL SCADA VULNERABILITIES

VULNERABILITY	SCADA IMPACT
Unpatched Published Vulnerabilities	Most Likely Access Vector
Web Human-machine Interface (HMI) Vulnerabilities	Supervisory Control Access
Use of Vulnerable Remote Display Protocols	Supervisory Control Access
Improper Access Control (Authorisation)	Access to SCADA Functionality
Improper Authentication	Access to SCADA Applications
Buffer Overflows in SCADA Services	SCADA Host Access
SCADA Data and Command Message Manipulation and Injection	Supervisory Control Access
SQL Injection	Data Historian Access
Use of Standard IT Protocols with Clear-text Authentication	SCADA Credentials Gathering
Unprotected Transport of SCADA Application Credentials	SCADA Credentials Gathering

Source: Idaho National Laboratory.

CYBER THREATS WITHIN THE DIGITAL OILFIELD

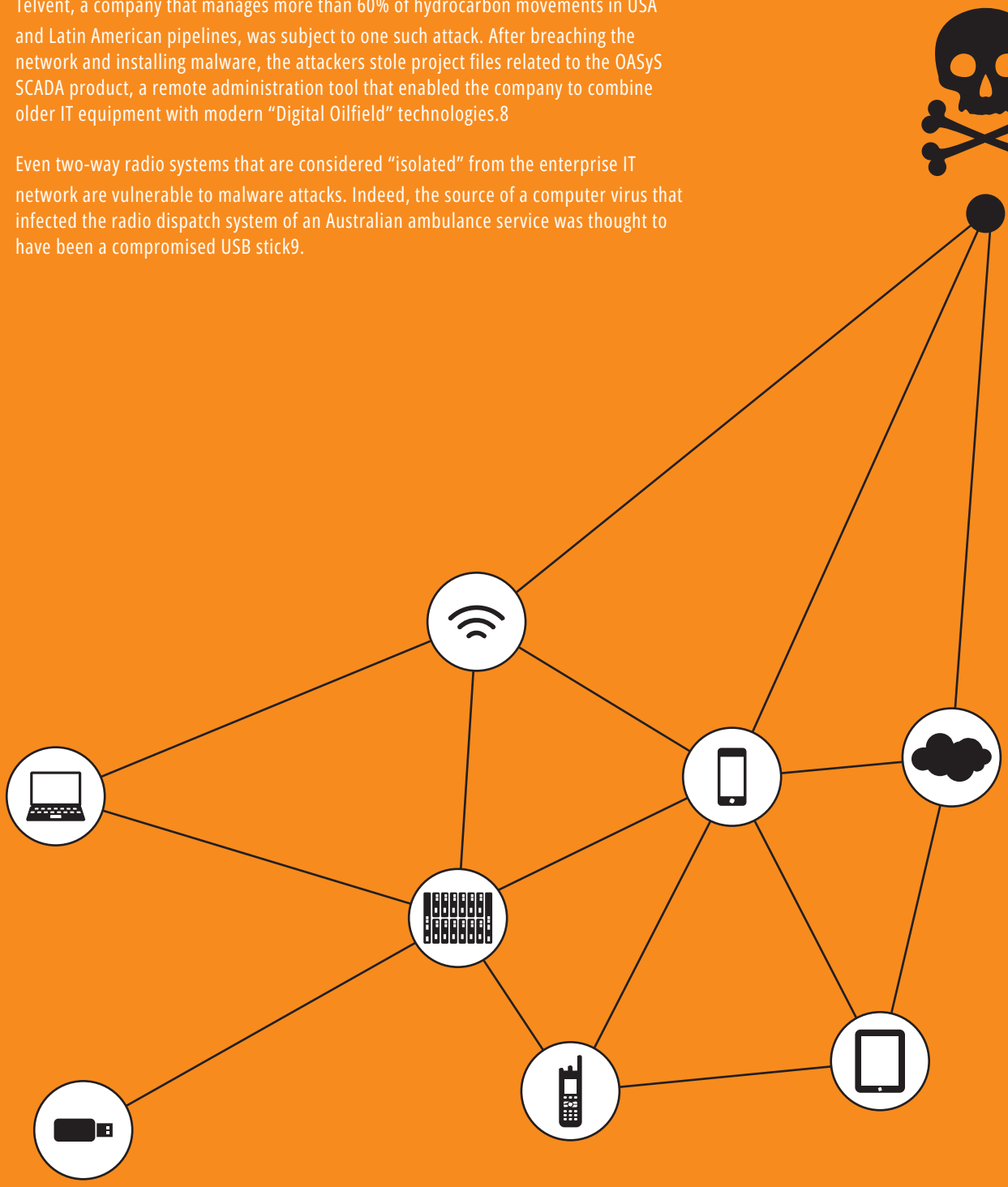


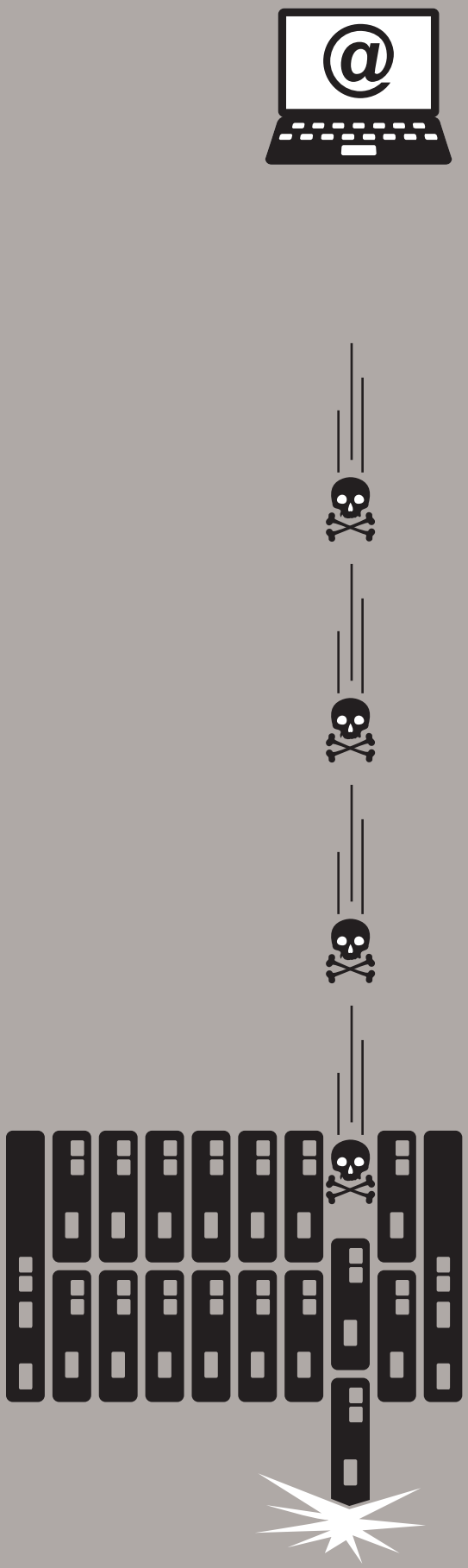
MALWARE

Malware is any malicious software that has been developed for the purpose of compromising or harming information assets without the owner's consent. Cyber criminals often target IT data assets such as those stored on servers, data sent by emails and stored on mobile devices and even information backed up on USB memory sticks. If a competitor steals blueprints to a company's power grid or key pipelines, it could disable operations and cause serious economic damage.

Telvent, a company that manages more than 60% of hydrocarbon movements in USA and Latin American pipelines, was subject to one such attack. After breaching the network and installing malware, the attackers stole project files related to the OASyS SCADA product, a remote administration tool that enabled the company to combine older IT equipment with modern "Digital Oilfield" technologies.8

Even two-way radio systems that are considered "isolated" from the enterprise IT network are vulnerable to malware attacks. Indeed, the source of a computer virus that infected the radio dispatch system of an Australian ambulance service was thought to have been a compromised USB stick9.





SPEAR PHISHING

Humans are notoriously susceptible to social tactics such as deception, manipulation and intimidation. A spear phishing attack exploits this weak point by using an email that appears to be from an individual or business known to the target. Data breaches based on social tactics have had a devastating impact on businesses, accounting for 37% of data stolen during cyber incidents in 2012.10

In October 2012, a spear phishing campaign used publicly available information to customise an attack against members of the energy sector. This publically available information was used by the attacker to craft malicious emails informing the recipients of the sender's new email address asking them to click on a link that contained malware.11

ADVANCED PERSISTENT THREATS

Advanced Persistent Threats (APTs) use targeted attacks as part of a longer-term campaign of espionage and sabotage, typically targeting high value assets such as critical infrastructure. APTs are sophisticated and adapt to defenders' efforts to resist their attacks.

In the Shamoon attack, nearly 30,000 hard drives were subject to a massive cyber attack at Saudi Aramco. The crime destroyed data on the oil and natural gas company's Windows-based machines, and the hardware had to be replaced.12

Oil and gas companies depend on the transmission of data to apprise management of new oil field discoveries, productivity levels and other mission critical data. Imagine the damage that could be done if a competitor accesses an oil company's system and finds out where it has discovered vast oil or natural gas reserves. Cyber criminals try to gain unauthorized access to this goldmine of data as it's being transmitted within SCADA systems and through corporate or enterprise Local Area Networks (LANs).

The malware known as Dragonfly, also known as Energetic Bear, allows its operators to monitor energy consumption in real time, or to cripple physical systems such as wind turbines, gas pipelines and power plants at will.13

Iranian oil facilities were forced to disconnect key oil facilities after a virus called W32.Flamer attacked against internal computer systems. Equipment at Kharg Island and other sites had to be disconnected from the Internet and the websites of the Iranian oil ministry and national oil company were forced offline. Data about users of the sites was stolen as well.14

Data is the lifeblood of the Digital Oilfield. It commands production systems and controls every operational application. One of the biggest breaches of operational systems occurred when the Stuxnet worm attacked a company's Windows-based systems, initially spreading using infected removable drives such as USB flash drives, and threated the PLCs and RTUs that controlled production. Stuxnet targeted Siemens software and equipment and infected PLCs. The virus was used to compromise Iran's nuclear facilities.15

INSIDER THREATS

A US Central Intelligence Agency analyst told an international group of government officials and engineers, as well as US security managers from electric, water, oil and gas and other critical industry asset owners, that "We have information, from multiple regions outside the United States, of cyber intrusions into utilities, followed by extortion demands. We suspect, but cannot confirm, that some of these attackers had the benefit of inside knowledge."16

That is not surprising. The Global Ponemon Institute report on cybersecurity found that "the most costly cyber crimes are those caused by malicious insiders, denial of service and web-based accounts. These account for 44% of all cyber crime costs per organisation on an annual basis.17

DENIAL OF SERVICE

Oil and gas control system operation can be disrupted by delaying or blocking the flow of information through communication networks, thereby denying availability of the networks to control system operators. This form of Denial of Service (DoS) can be caused by IT resident services such as Domain Name System (DNS) – for example, using spoofed DNS requests.

Clearly, where control systems are involved, DoS can have physical manifestations. For example, the deluge of data that resulted in the Alabama nuclear plant shutdown in 2006 was attributed to a malfunctioning PLC.18

WIDESPREAD VULNERABILITY REQUIRES SYSTEMATIC PROTECTION

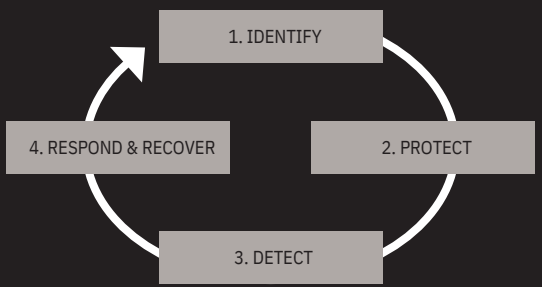
These are all but a few examples of how complexity indicates how much can go wrong if an oil and gas company's systems are hacked or compromised. But there are solutions, providing security measures are tailored to meet the unique real and present dangers of individual companies.

NIST FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY

A 2013 study by the CSIS found that 96%19 of successful breaches could be avoided if the organisations put simple or intermediate controls in place.
In February 2013, The NIST Framework for Improving Critical Infrastructure Cybersecurity was created as the result of a US Executive Order, in response to the growing security, economy, public safety and health risks caused by cybersecurity threats.
The NIST Cybersecurity Framework provides a common mechanism on which organisations can:

- Describe their current cybersecurity posture
- Describe their target state for cybersecurity
- Identify and prioritise opportunities for improvement
- Assess progress toward the target state
- Communicate among internal and external stakeholders about cybersecurity risk

The NIST Cybersecurity Framework consists of four steps:



TODAY'S HARSH REALITIES

ATTACKERS SPEND AN ESTIMATED 243 DAYS ON A VICTIM'S NETWORK BEFORE BEING DISCOVERED.

IN 2013, IT TOOK 32 DAYS ON AVERAGE TO RESOLVE A CYBER ATTACK.

63%

OF VICTIMS WERE MADE AWARE OF THEIR BREACHES BY AN EXTERNAL ORGANISATION.

Cybersecurity involves much more than protection and prevention. It also involves the ability to quickly detect breaches and thoroughly research the extent and impact of those breaches.

Source: IBM,2014. "Cybersecurity Roadshow"

NEW WAYS OF DOING BUSINESS DEMANDS SMARTER CYBERSECURITY:

A BEST PRACTICE FRAMEWORK

So what are the best practices to improve the security posture of the industrial control and IT systems supporting critical infrastructure? What actions need to be taken to secure legacy systems? The cybersecurity strategy below is consistent with the NIST Framework and highlights a set of processes which, when executed concurrently and continuously, serve to improve an organisation's cybersecurity posture.

1

KNOW YOUR CRITICAL ASSETS

Identify your organisation's business objectives and high-value assets, then conduct risk assessments to find any vulnerabilities.

2

PROTEC RADIO AND OT ENVIRONMENTS

Establish defences to block intruders before they reach your critical business assets, and educate your employees to recognise and avoid phishing attacks.

3

DETECT POTENTIAL THREATS BEFORE THEY OCCUR

Use the right tools to gain a comprehensive view of your security environment and monitor potential threats both externally and internally.

4

RESP RECOVER

With the speed and intelligence of many of today's cyber attacks, cyber breaches may still occur, even in the most secure infrastructure. Having a contingency plan in place can help you respond immediately if a breach should occur.

CYBERSECURITY STRATEGY CHECKLIST:

1. KNOW YOUR CRITICAL ASSETS

- [ ] Identify your business objectives and high-level organisational priorities to determine which cybersecurity implementations would be most advantageous.
- [ ] Identify systems and assets that support business objectives.
- [ ] Conduct regular risk and security assessments to understand criticality, vulnerability and likelihood of threats to your assets. In particular, conduct threat modelling to discern risks specific to your organisation.
- [ ] Adopt a lifecycle approach to security, prioritising and acting on findings.
- [ ] Identify all high value assets across enterprise IT, radio network and OT environments and ensure that they are managed consistently with their relative importance and your organisation's risk strategy

2. PROTECT YOUR IT, RADIO NETWORK AND OT ENVIRONMENTS

- [ ] Follow best practice in basic cybersecurity hygiene. This includes ensuring systems are kept up to date with regular patching and updating cadence.
- [ ] Protect data at rest in SCADA and critical IT systems with data file encryption.
- [ ] Properly classify, isolate and secure all high-value assets.
- [ ] Implement access controls at all entry points to the enterprise IT, radio network, OT and SCADA networks.
- [ ] Implement secure domains or security zones to compartmentalise threats.
- [ ] Protect field units against unauthorised access with a OT/SCADA specific firewall.
- [ ] Use cryptography to protect all sensitive communications, including OT/SCADA and two-way radio communications. Ensure that encryption is based on a strong algorithm..
- [ ] Ensure that physical access to critical assets is managed and protected. Measures include protecting physical locations and implementing access control systems for controlled spaces.
- [ ] Provide OT and IT systems with reliable power. Use appropriate environmental control systems to protect information systems. For example, fire systems must be carefully designed to avoid causing harm due to the mixing of water with incompatible products.
- [ ] Train employees on risky behaviours, how to avoid them, and the potential consequences of security lapses.

3. DETECT POTENTIAL THREATS BEFORE THEY OCCUR

- [ ] Monitor the physical environment to detect potential cyber security events. Consider installing video cameras and alarms where appropriate.
- [ ] Deploy automated auditing, monitoring and remediation technologies.
- [ ] Monitor and assess malicious code trends and attack vectors.
- [ ] Use advanced analytics for detailed insight into each threat, including removal activities.
- [ ] Use automated tools to investigate suspicious files and determine the cause of changes to the operating system.
- [ ] Implement security logs for auditing and logging purposes, and add intrusion detection capability to each security zone.

4. RESPOND AND RECOVER

- [ ] Implement a business continuity/disaster recovery plan ensure that this is periodically tested.
- [ ] Implement backup and recovery mechanisms for all critical systems and data assets.
- [ ] Use malware analysis to gain information on how to eradicate infections, secure endpoints, and prevent future attacks.
- [ ] Provide required training to ensure that personnel know their roles and order of operations when a response is needed.

HOW SECURE IS YOUR SECURITY?

Whether you are protecting the SCADA systems, mobile communication networks, smart meters or other physical assets, system complexity is your biggest cybersecurity challenge.

When combating threats—such as malware attacks —companies can fail to address vulnerable interfaces between their diverse systems or consider how their security infrastructure functions as a whole.

Our cybersecurity solutions for oil and gas are based on global security standards and consistent with the NIST Cybersecurity Framework. We aim to evaluate your systems from end to end and deliver the security solutions companies today need for protection from cyber crime.

STAY AHEAD OF CYBER THREATS

Whatever the age of your current SCADA systems, the equipment you choose going forward should be a bridge to tomorrow. Motorola systems integrate seamlessly and cost-effectively with your existing infrastructure. At the same time, they position you to leverage modern technology and mitigate tomorrow's risks. Secure and adaptable, these products will help you prepare your SCADA systems to ensure uncompromising safety, production and asset security.