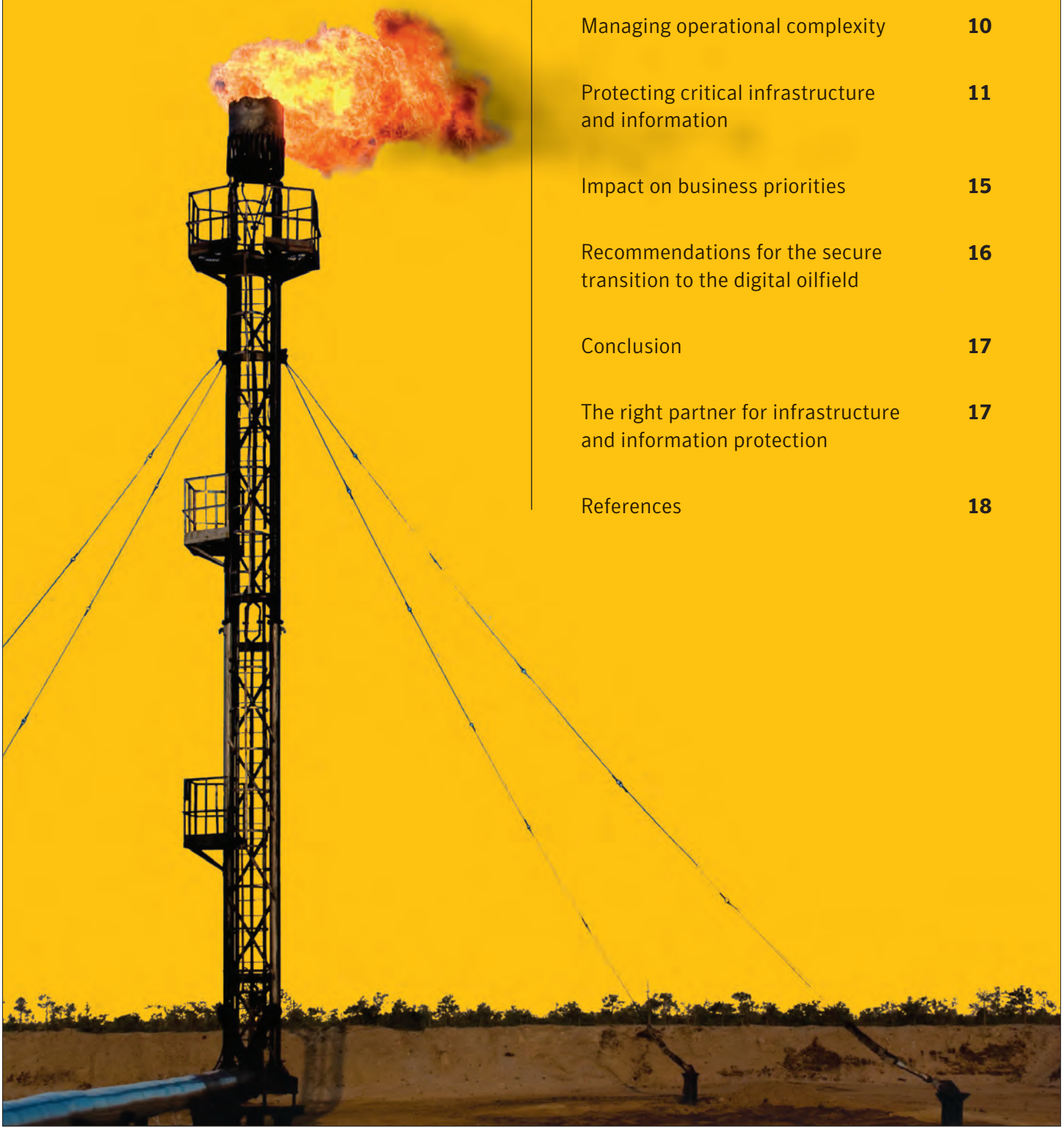
# Protecting critical systems while promoting operational efficiency

Towards the **digital oilfield**

# Contents





# Introduction

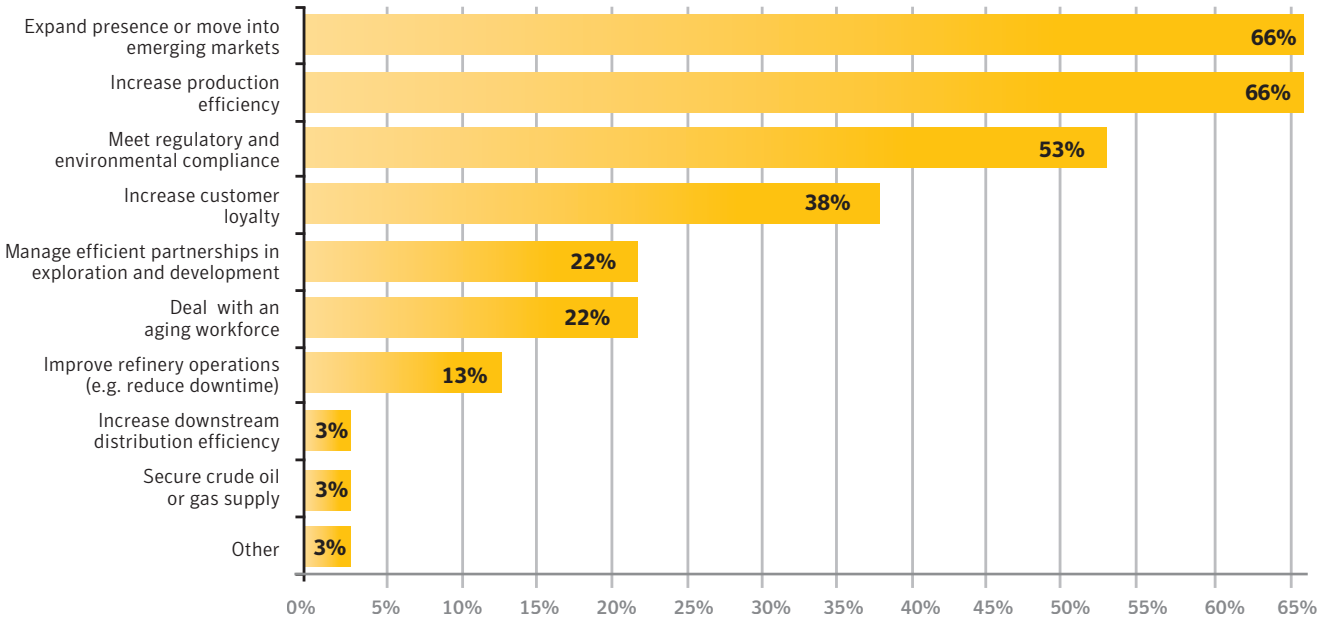
The oil and gas industry is facing significant structural and organisational changes. Due to limited fossil resources and the exploding costs of exploration and production, the future supply of energy resources has already become a massive challenge for energy firms. New markets are emerging and the International Energy Agency predicts that the world's demand for energy will have increased by one-third from 2010 to 2035. Despite the current focus on developing renewable energies, more than half of the global primary energy demand will need to be met by oil and gas resources[1].

Forrester research in 2011 found that the key industry priorities were to move into emerging markets and increase production efficiency[2].

This requirement to **increase production capacity** and **efficiency** is driving new investments in information technologies (IT) and operational technologies (OT). The ongoing digitalisation of production processes and the convergence between IT and OT towards a future 'digital oilfield' is a key enabler in increasing operational efficiency and optimising supply chains in the oil and gas industry.

But the increasing reliance on IT is a double-edged sword, particularly for industries delivering essential goods and services to businesses and the public, as failures and outages have an immediate impact. In addition, many countries worldwide are dependent on this sector; for example, the oil and gas industry in the Middle East is by far the biggest contributor to the region's GDP. Disruptions in production or the supply chain can not only have a massive impact on the local economy, but also on global prices with potential political repercussions.

**"What are your company's three most important oil and gas industry priorities?"**




**Base: 32 North American and European IT budget decision-makers in the oil and gas industry (multiple responses accepted)**

*Figure 1: Forrester Research, Forrsights Budgets and Priorities Tracker Survey, Q4 2011 – Data for the Oil and Gas Industry*

During the development of this report in September 2012, major cyber attacks against two large oil and gas companies in the Middle East were carried out. The companies were hit by an outbreak of new, precisely targeted malware, which was reported to have caused significant disruption to their internal IT systems.

These two high profile attacks, which might potentially have shared a common attacker, caused great concern within the energy sector. The attacks highlighted weaknesses in security and demonstrated the capability of sophisticated and motivated hackers to cause significant disruption. Although the attacks reportedly did not affect the production and delivery systems in the supply chain, they highlighted major challenges in the security of both enterprise information systems and operational control systems.

## Developing a 'digital oilfield'

The transition to a 'digital oilfield' brings two different technologies and cultures together using open IT protocols: the world of OT, with supervisory control and data acquisition (SCADA), distributed control systems (DCS), and the world of enterprise IT. Inherent threats from open standard based IP networks increase the vulnerability of the traditionally isolated operational control systems against cyber attacks. But it is not just the interconnection between SCADA and IT environments that is a cause for concern. The Stuxnet worm, which attacked the Iranian nuclear programme, has demonstrated that even isolated industrial control systems (ICS) are vulnerable against targeted threats[3].

However, cyber security cannot be considered in isolation as it is closely aligned with other industry issues that need to be addressed during this transition process.

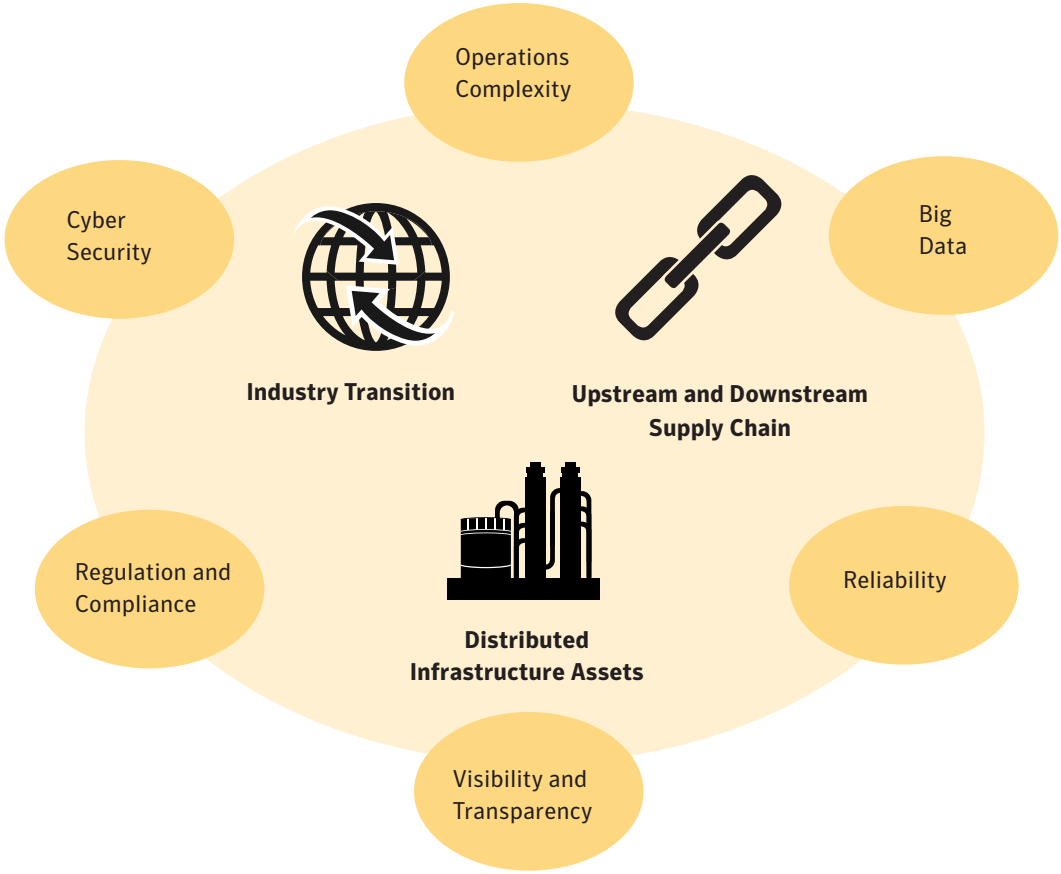



*Figure 2: Overview of information protection and security challenges during the transition process*

## The rise of targeted attacks

Although Stuxnet made the headlines, it is just the tip of the iceberg and prior to this attack, hackers and malicious insiders had broken into SCADA and ICS on multiple occasions.

At least two of these early attacks targeted the oil and gas industry. One involved the Trans-Siberian pipeline explosion in 1982[4]. Although myths and rumours abound, the widely accepted explanation for the incident is that it was caused by a Trojan inserted into SCADA software. Then in 2000, the Russian government publicly announced that hackers had succeeded in gaining control of the natural gas pipeline of Russian's largest gas provider, Gazprom[5].

The 2011 Symantec Internet Security Threat Report saw a dramatic increase in the number of publicly reported SCADA vulnerabilities from 15 in 2010 to 129 in 2011[6]. The report also discovered that the number of targeted attacks increased from an average of 77 per day in 2010 to 82 per day in 2011[7]. These targeted attacks used customised malware to gain unauthorised access to sensitive information. This is the next evolution of social engineering, where victims are researched in advance and specifically targeted; typically to steal high value intellectual property for financial gain, or to attack critical infrastructures.

**SCADA attacks**

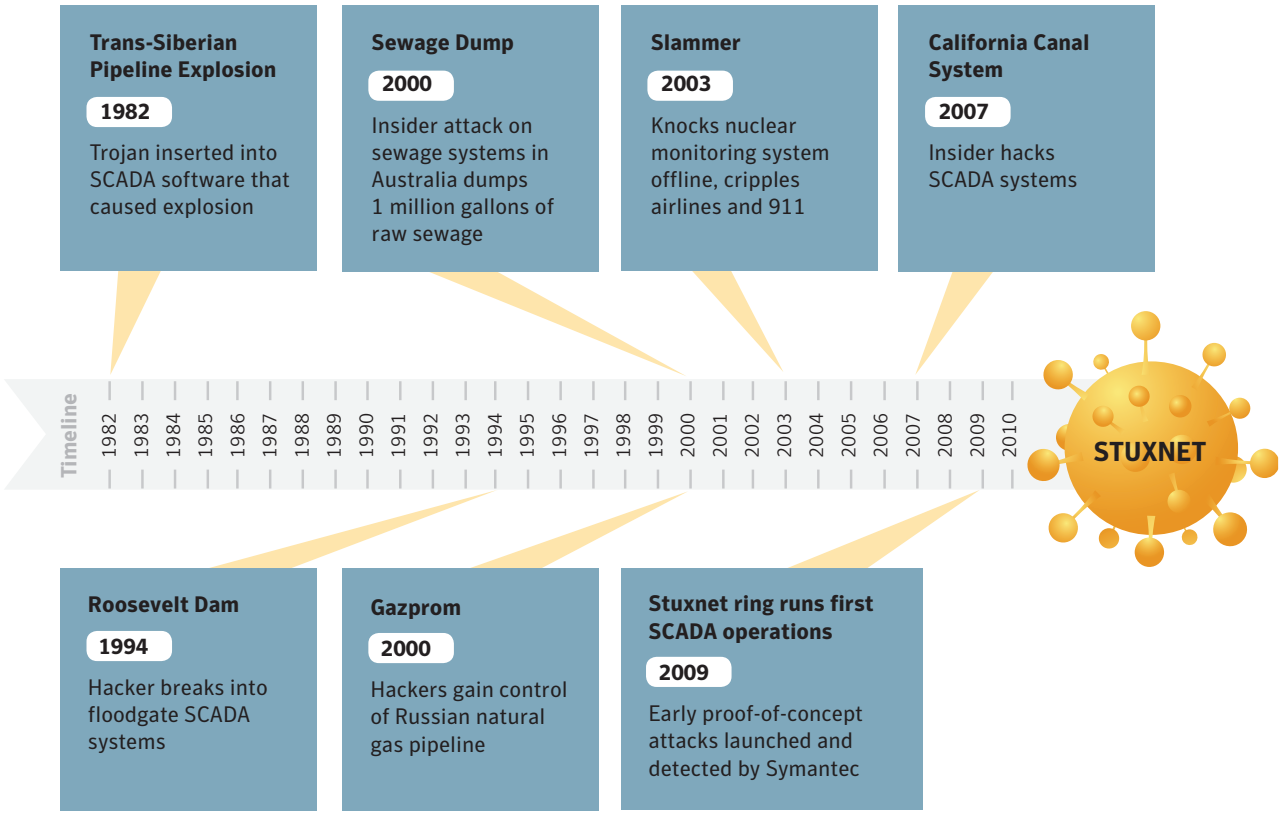



*Figure 3: SCADA attacks prior to the Stuxnet outbreak*

**The danger of political attacks**

The 2010 Symantec Critical Infrastructure Protection study confirmed that not only are cyber attacks on the increase, but that the threat of attacks with a specific political goal in mind is real and these are becoming increasingly frequent and costly[8].

Symantec found that over half (53 percent) of all firms said they suspected or were pretty sure they had experienced an attack waged with a specific political goal in mind. In fact, of those affected, the typical company reported being hit 10 times in the past five years. One IT director from a mid-sized energy company remarked, "We've had people attempt to break in and retrieve documentation, especially the shared material between the oil companies in our library. We had to take some dramatic actions to be able to cut them off."[9]

Furthermore, the attacks are serious, with respondents estimating that three in five (59 to 61 percent) of attacks ranged from somewhat to extremely effective. In North America, 74 to 77 percent of the companies surveyed reported that the attacks were effective[10].

The survey also found that only one-third of respondents (28 to 33 percent) felt "extremely prepared" against the attacks, while 36 to 41 percent said they felt "somewhat prepared," and 31 percent (across all types of attack) felt less than somewhat prepared[11].

**Targeted attacks trend showing average number of attacks identified each month, 2011**

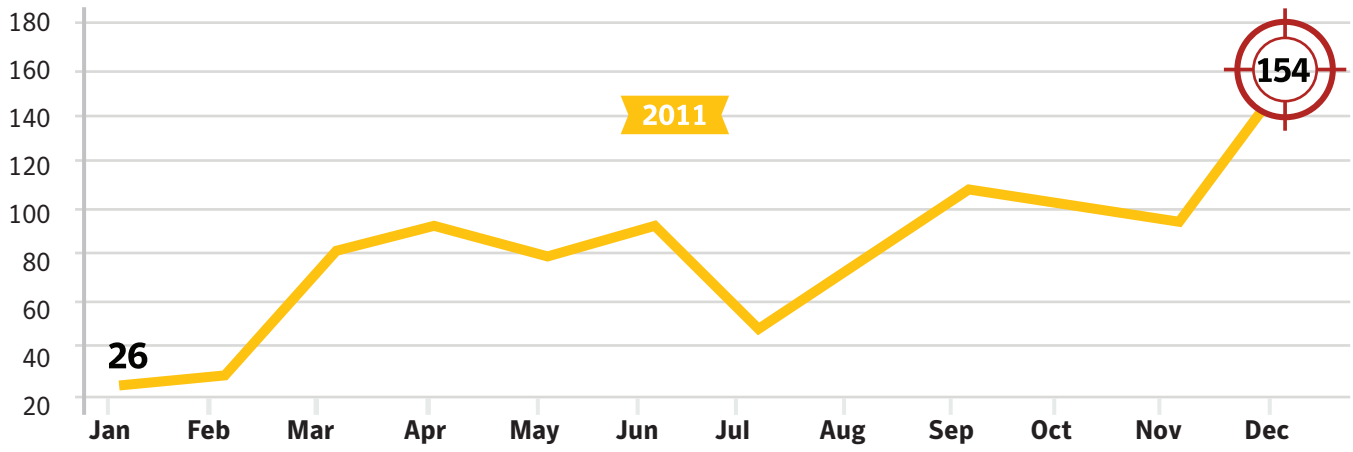



*Figure 4: Symantec Internet Security Threat Report 17 – April 2012 (Source: Symantec.cloud)*

### Cyber attacks used for espionage

Advanced persistent threats (APT) such as Stuxnet, Night Dragon, Nitro, Duqu and Flamer, use targeted attacks as part of a longer-term campaign of espionage and sabotage, typically targeting high value information in government, finance, oil and gas, chemical industries and ICS in general.

**Night Dragon** attacked oil, gas and petrochemical companies. When detected in February 2011, it appeared that the malware had been stealing sensitive information as well as data from SCADA systems for at least two years[12].

### Attack frequency

**In general, how is the frequency of each of the following types of attacks changing? (Only asked of those who at least suspect each type of attack)**

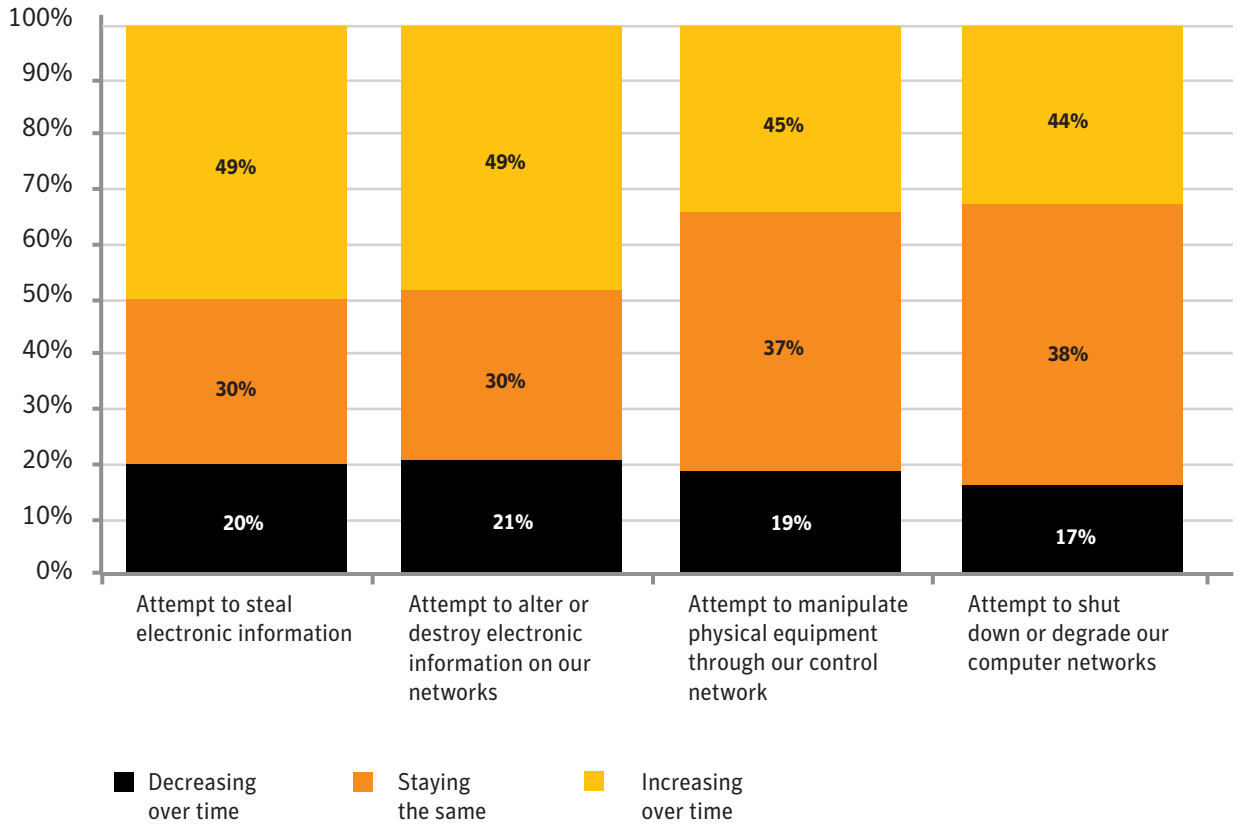



*Figure 5: Symantec Critical Infrastructure Protection Study Data, November 2010*

**Nitro** attack waves, focusing mainly on the chemical industry, started in late July 2011 and continued into mid-September 2011. The purpose of the attacks appeared to be industrial espionage: collecting intellectual property for competitive advantage[13].

In October 2011, **Duqu**[14] came to light followed by **Flamer**[15], a highly sophisticated and discreet threat targeting the Middle East in Spring 2012. Neither caused any cyber-sabotage but both were used for extensive espionage and data exfiltration.

The August 2012 virus outbreak against the oil and gas industry in the Middle East, also known as **Shamoon**, was first detected by Symantec on August 16, 2012[16]. This information-stealing malware incorporated a highly destructive 'wiper' module. Shamoon renders infected systems useless by overwriting essential blocks on disk. Infected organisations can experience huge operational impacts including loss of intellectual property and disruption of critical systems[17].

Ongoing investigations by Symantec[18] show that not only are companies within the oil or gas industries at high risk of APTs, but also those companies manufacturing industrial sensors, meters, pumps and valves. These are a target as attackers try to gain confidential information about critical components and embedded systems in SCADA and other ICS systems. They can provide information and illegal access, which would allow hackers to manipulate processing within various industries. This could lead to serious outages, loss of revenue and reputation, not to mention potentially causing disasters that could have an impact on the health and safety of industry employees, the public and the environment.

The Symantec Security Response Dossier on **'The Elderwood Project'**[19], published in September 2012, supported these observations. This group attacks supply chain manufacturers who service special target industries for wholesale gathering of intelligence and intellectual property. The target sectors of the attackers include oil and gas companies.

## Meeting the challenges of regulation and compliance

Cyber security for the critical energy infrastructure is a national, if not a multi-national, security issue exacerbated by potential insider risks and a magnified attack surface. Security officers within the oil and gas industries are seeing increased pressure from authorities to implement security standards and comply with new regulations and directives.

The Forrester survey ranked 'Meet regulatory and environmental compliance' among the top three oil and gas industry priorities[20].

The disasters on the oil platforms Alpha Piper (1988) and Deepwater Horizon (2010), as well the Buncefield Oil Refinery fire in the UK (2005), resulted in greater impetus within the industry to safely secure systems by implementing standards, optimising process workflows under both normal and emergency conditions, and guaranteeing ongoing intensive training and education of the workforce.

To further mitigate risks, security vendors and governments have started joint programmes to improve how industry control systems like SCADA environments are monitored in depth. Their objectives are to detect intrusions, analyse successful attacks and improve the security of systems.

As part of the seventh EU framework programme, the project CRISALIS (CRitical Infrastructure Security AnaLysIS), for which Symantec is a project partner and coordinator, was launched in June 2012 with the goal of improving the security of critical infrastructures[21].

Special security standards focusing on ICS are also being defined as SCADA networks become increasingly open. These include API 1164 (American Petroleum Institute 1164), AGA 12 (American Gas Association: Cryptographic Protection of SCADA communications), the ISA SP99 standardisation series (Industrial Automation and Control Systems Security), and others. These complement international security standards like ISO 27001/27002 or ISO 27005 for Risk Management and better meet the special cyber security needs of the industry.

However, the successful demonstration of compliance based on different regulations can be a very time consuming and costly process if it is not supported by automated software tools.

## Managing operational complexity

Strategic IT trends like virtualisation, cloud and mobile, are cornerstones of operational effectiveness and efficiency. As a result, they are becoming widely adopted in the oil and gas industry:

- Business critical IT applications are increasingly running on virtualised servers.
- Cloud services are expanding into core exploration and production processes.
- Mobile technologies improve the collaboration of users and the connectivity of smart devices across widely distributed infrastructure assets.

However, with all these benefits comes risk if proper management is not in place. Security is the number one concern of cloud computing, as external cloud service providers often don't provide visibility and transparency into their security architecture and processes[22]. Mobile malware is rising fast[23] and the diversity of mobile operating systems, combined with bring your own device (BYOD) strategies, does not make it simple for IT departments to manage and secure enterprise mobility. Business critical applications should only run on virtualised servers if strong security and availability measures can guarantee the integrity and reliability of the applications and information.

The convergence between enterprise IT and OT brings various generations of technologies together, resulting in substantial organisational and cultural changes. Traditionally, security risk in OT has been managed completely separately from enterprise IT risk. Now there is a necessity to unify the conflicting cultures and fragmented ownership risk in order to achieve the best possible end-to-end security approach.

## Protecting critical infrastructure and information

Achieving a secure IT and OT infrastructure is not an easy task due to the multiple challenges the industry faces. Robust and provable security does not start with deploying point products to fill holes. To begin with, vulnerabilities must be identified and analysed using a risk management process supported by a framework that directly relates to business risk.

The European Network and Information Security Agency (ENISA) confirmed that 'processes' are seen as the most important pillar to secure critical infrastructures and ICS – much more important than technology and people[24].

Governance, risk management, and compliance (GRC) helps security leaders in energy companies to communicate IT risk in business-related terms, prioritise remediation efforts based on a composite view of risk, and automate assessment processes to improve overall security and compliance posture. Based on best practices and guidelines for protecting IT information and ICS, the framework should support various steps from identifying critical assets through to continuous audit processes.

Security in SCADA systems will also change the priority of critical characteristics. Until now, availability in ICS was the main criterion: more important than confidentiality and integrity which are often the top priorities for IT. Stuxnet has opened the eyes of OT managers so that the integrity of ICS processes and related information is now at least as important as availability of control systems.

Focusing solely on IT data centers and operation control centres is not enough. As the supply chain and technical infrastructure domains are highly complex, a comprehensive end-to-end approach is necessary. Each part of the industry value chain needs to be analysed, assessed and secured – but not in an isolated way. Security officers should consider the following disciplines as part of their GRC framework and security strategy:

- Securing operations
- Combining security with data
- Managing smart endpoints and embedded systems
- Protecting the data explosion

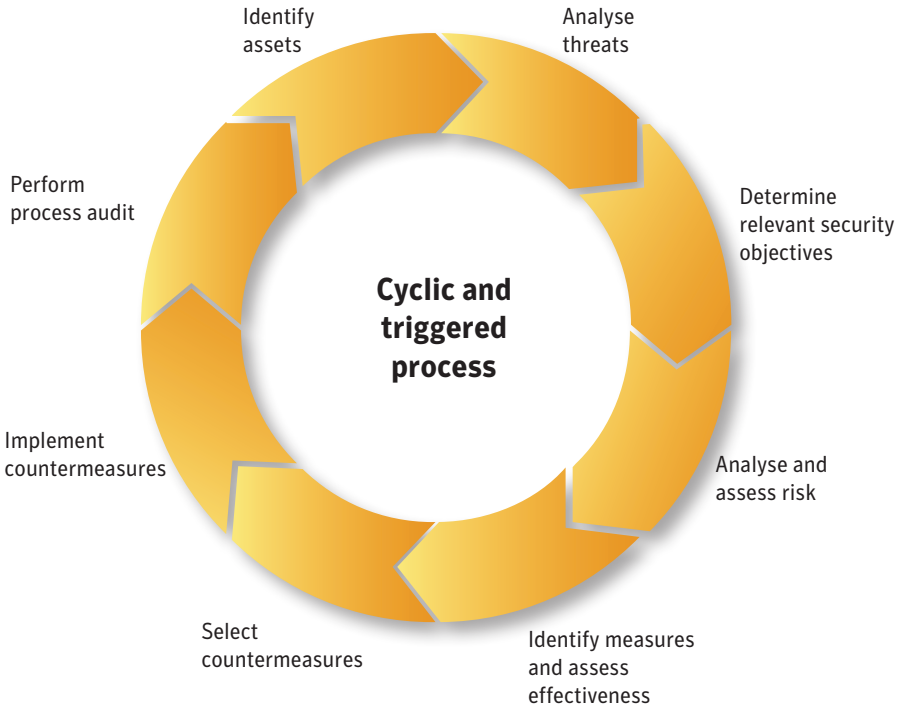



*Figure 6: A cyclic GRC process as the foundation for ICS security (Source: VDI, VDE 2182)*

**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 |

*Figure 7: Top 10 most critical SCADA vulnerabilities (Source: Idaho National Laboratory)*

**Securing operations**

Operation control centres are at the heart of managing operational processes and the recent attacks on SCADA-based critical infrastructures demonstrate the need to make security a top priority.

The 10 most significant SCADA vulnerabilities were analysed by the US Department of Energy's Idaho National Laboratory (INL) between 2003 and 2011[25]. SCADA vendors and energy companies should use the table below to assess their control systems for these common vulnerabilities and mitigate with appropriate countermeasures.

Unsurprisingly, 'unpatched published vulnerabilities' was identified during the analysis as the most likely access vector. Software that is not using the newest patch version and is therefore vulnerable is often spread over many SCADA systems. In some instances, SCADA owners are not allowed to patch their control systems as they would risk losing the certification and integrity of their control systems. Availability and operational effectiveness must therefore be preserved and a different security approach is required for energy delivery control systems that will not impede operations.

SCADA systems can profit greatly from the deployment of advanced security solutions that harden the environment, detect anomalies and respond to threats, while continuously monitoring the interaction with field devices and the Internet. The use of sophisticated heuristic and whitelisting techniques provides protection against zero-day attacks. In the example of the Stuxnet worm, many of the zero-day vulnerabilities could have been protected by the setting of policies to allow only certain system applications to run.

Among the top SCADA vulnerabilities identified by INL were improper authorisation and authentication, standard protocols with clear text authentication and unprotected transport of SCADA credentials. Identity and access management solutions must have higher priority, especially in consideration of the accelerating interconnection with enterprise IT systems, and the adoption of cloud, mobile and remote management functionalities.

**Unpatched software integrated into SCADA**

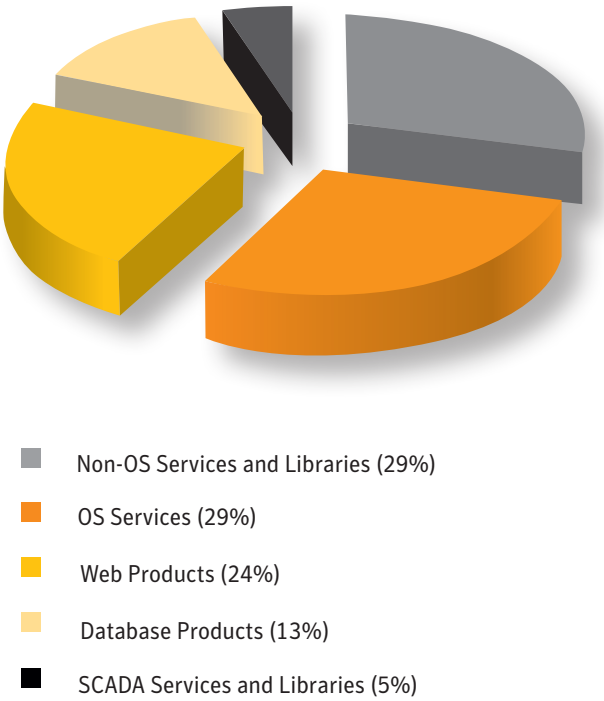



*Figure 8: Unpatched Software Integration Statistics (Source: Idaho National Laboratory)*

**Combining security with data**

Security has changed radically from protecting the perimeter to protecting information, so the most obvious approach is to embed security with data. Multiple technologies already exist and can be combined to achieve confidentiality, integrity and authentication.

Transferring critical control information over unsecure lines to external service providers or cloud storage locations requires data encryption. User authentication leveraging strong two-factor authentication and one time password entry, allows only trusted personnel to gain access to critical data and control systems. Digital certificates can also be used for authentication, signing and encryption.

Energy providers should only select third-party providers who are committed to fulfilling these requirements. Where cloud deployments are part of the operational efficiency programme, cloud service providers must commit to support the security guidelines developed by the Cloud Security Alliance (CSA).

Furthermore, it is important to automate the controls on critical information and only allow transfer using predefined policies based on the structure and type of data content. Technologies such as data loss prevention can automate the generation of policies controlling the flow, storage and access of critical information.

**Managing smart endpoints and embedded systems**

Oil and gas companies need to manage the increasing number of smart devices that play a dominant role in their digitally intensified world. In addition to mobile technology, which will increasingly be deployed to improve operational efficiency, the proper management and protection of embedded systems within control processes will become an essential part of security architecture. Security in embedded systems is about managing and securing data, identity and services across the entire supply chain, to avoid these devices being compromised and opening an additional threat vector.

Currently, few regulations exist on implementing security for embedded systems. This poses major risks for cyber attacks, particularly as many smart devices have a lifetime of 15 years or more and are not easy to access and replace.

Due to scalability requirements on one hand and non-standard hardware and proprietary firmware in embedded systems (such as meters and pumps) on the other, standard computer security software often can't be deployed. Therefore, device certificates and public key infrastructure (PKI) architectures are seen as the best security practice.

By implementing PKI into embedded systems, important parts of the OT can be secured at the communication layer, creating a system that identifies connected devices as authentic and verifies configuration and integrity. PKIs are ideal for large-scale security deployments that require a high level of security with minimal impact on performance. In a PKI environment, it is essential that private keys and certificates are guarded by a reliable management solution that protects against ever-evolving data threats. As only a few oil and gas companies can afford to build and run such a highly scalable certificate authority (CA) for device authentication, managed PKI service providers with a strong focus on this business provide a good alternative to internal management.

**Protecting information in the data explosion**

Exploration of new energy resources, that generate large quantities of seismic and geospatial data, is extremely cost-intensive. The digitisation of the oil and gas industry generates huge volumes of data. This includes real-time information on control processes which, according to some countries' regulations, must be archived for several years.

This digital intensity requires an intelligent and scalable information management approach to storing, protecting, backing up, archiving and retrieving data whenever needed. Acquired data is a highly valuable intellectual property with the potential to offer ongoing competitive advantage against competitors. Therefore, special consideration is needed to protect sensitive information against illegal access and data exfiltration.

Cost-efficient and secure information management builds on several layers of solutions. Data must be categorised, archived and processed in a manner that enables organisations to demonstrate regulatory compliance, provide evidence of accurate operational processes, and respond to potential legal actions. Efficient backup technology, using the latest data deduplication technologies, protects large data volumes while saving storage resources.

Storage lifecycle management ensures that only critical data is stored on fast storage, and automatically moves less critical data to less expensive disk arrays and even tape.

Access to confidential geospatial data created by exploration activities must be strongly secured. Security officers should implement:

- Measures to secure the storage platforms and server hardware.
- Strong access control with authentication and authorisation.
- Monitoring of the access patterns of authorised users. Unusual data transactions or attempts to store or move large volumes of data to storage devices outside of the policy could be detected by a warning system. Such protection against malicious insiders would have prevented the US Army from losing large amounts of highly confidential information to Wikileaks.

## Impact on business priorities

There are four key areas to consider when aligning increased digitisation with the needs of the business:

**Secure the critical infrastructure**

Cyber attacks against critical infrastructures and ICS have made headlines. Governments are leaning on energy providers to implement appropriate security measures to avoid any disruption of the oil and gas supply chain.

Oil and gas firms risk their reputations, losing revenue and huge fines if they cause a major environmental incident. Politically motivated cyber attacks, which are not detected and stopped early enough, can increase the likelihood of environmental disasters and put the health and safety of the population at risk.

**Protect company value**

A recent disaster demonstrated the effect this type of incident can have on the market capitalisation of an organisation: in this instance a drop of more than 50 percent in value[26]. On average, just the announcement of a corporate security breach has a negative impact of about 1 percent of the market value of the firm during the days surrounding the event[27].

**Comply within a regulated industry**

Regulatory bodies provide standards and guidelines that are evolving with stricter penalties for non-compliance. Again, GRC helps to define policies in order to achieve compliance with external regulations and best practice frameworks. These policies map to controls for multiple mandates to avoid redundant efforts and drive costs down through automation.

**Gain competitive advantage**

Security is a business enabler and a competitive differentiator. The main objective of the oil and gas industry is the seamless transition to a higher operational efficiency. However, due to the risks, this can only be achieved with a strong focus on information protection and security. As a result, security as an integral part of IT and OT becomes an important business tool. Without a proper security and compliance architecture and framework, the risk would become unpredictable and uncontrollable. Companies would not be able to move fast enough during the transition process and any increase in production capacity could be impacted.

## Recommendations for the secure transition to the digital oilfield

It is important to implement the correct processes and best practices to create a seamless transition to higher operational efficiency:

**Start with a risk management process**, such as ISO 27005, to enforce IT policies and automate compliance. Use GRC for prioritising risks and defining policies that span all segments of the enterprise IT and OT/SCADA environments. Oil and gas companies can enforce policies through built-in automation and workflow to not only identify threats, but also remediate incidents as they occur or anticipate them before they happen.

**Align the two separate worlds of OT and IT** as the transition towards higher operational efficiency will force both areas to merge. The risk management process to achieve the necessary end-to-end security must encompass both worlds.

**Protect information proactively** by taking an information-centric approach. Embedding security within data and taking a content-aware approach to protecting information is vital for identifying ownership, where sensitive details reside and who has access to it. Classify data and utilise encryption to secure sensitive information and prohibit access by unauthorised individuals.

**Authenticate users and embedded systems in ICS** by leveraging solutions that allow businesses to ensure that only authorised personnel have access to systems. Strong authentication also enables organisations to protect public-facing assets by ensuring the true identity of a smart device, system, or application. This prevents individuals from accidentally disclosing credentials to an attack site and from attaching unauthorised devices to the infrastructure.

**Manage systems** by implementing secure operating environments, distributing and enforcing patch levels, automating processes to streamline efficiency, and monitoring and reporting on system status.

**Protect the infrastructure** by securing endpoints, messaging and web environments. In addition, defending critical internal servers and implementing the backup and recovery of data should be priorities. Organisations also need visibility and security intelligence to respond to threats rapidly.

**Ensure 24x7 availability of the critical infrastructure** by implementing non-disruptive testing methods and reduce complexity by automating failover. Virtual environments should be treated identically to physical environments, with organisations adopting more cross-platform and cross-environment tools, or standardising on fewer platforms.

**Develop an information management strategy** that includes an information retention plan and policies. Organisations need to stop using backup for archiving and legal retention, implement deduplication everywhere to free up resources, use a full-featured archive and eDiscovery system and deploy data loss prevention technologies.

**Cooperate with a security and information protection partner** with worldwide visibility of attacks trends who is able to address the complete range of security challenges the oil and gas industry is facing.

## Conclusion

Oil and gas companies will be in the strongest position to maximise the opportunities offered by the digital oilfield if they are prepared for the security challenges this transition will bring. Developing an end-to-end architecture designed to manage critical infrastructures, promote compliance, and protect information will be key to creating a competitive advantage.

## The right partner for infrastructure and information protection

Symantec protects the world's information, and is the global leader in security, backup and availability solutions. Our innovative products and services protect people and information in any environment – from the smallest mobile device, to the enterprise data center, to cloud-based systems. Our industry-leading expertise in protecting data, identities and interactions gives our customers confidence in a connected world.

The company supports the oil and gas industry and their suppliers in their transition to increased operational efficiency by delivering end-to-end security and promoting an information management approach. Symantec works closely with governments around the world and is coordinating the EU research project CRISALIS[28] on the detection and remediation of vulnerabilities and attacks in critical infrastructures.

Symantec operates the largest and most comprehensive PKI solutions for enterprises and service providers available on the market today, and has been doing so since 1995. The overall system architecture is designed to support the issuance and management of over 100 million certificates per year[29].

## References


1 International Energy Agency: World Energy Outlook 2011 by Dr. Fatih Birol
Parliament House Canberra, pp. 3-4, 12th December 2011

2 Forrester, The IT-driven Energy Revolution incl. the Forrsights Budget and Industry Priority Tracker Survey, p. 3, Q4 2011

3 Symantec Security Response: W32.Stuxnet Dossier, February 2011
http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf

4 Siberian Pipeline Sabotage: Hacking the industrial SCADA network, Pipeline & Gas Journal, Nov. 2009, Vol. 236, No. 11, by Frank Dickman
http://pipelineandgasjournal.com/hacking-industrial-scada-network

5 Hacking SCADA/SAS Systems, seminar presentation by NESEC at Petroleum Safety Authority Norway, p. 8, 2006

6 Symantec Internet Security Threat Report ISTR 17, p. 41, April 2012
http://www.symantec.com/threatreport/?inid=us_sr_flyout_publications_istr

7 Symantec Internet Security Threat Report ISTR 17, p. 14, April 2012

8 Symantec Critical Infrastructure Protection Study, p. 5, November 2010
http://www.symantec.com/content/en/us/about/presskits/Symantec_2010_CIP_Study_Global_Data.pdf?om_ext_cid=biz_socmed_twitter_facebook_marketwire_linkedin_2010Oct_worldwide_vision_cip

9 Symantec Critical Infrastructure Protection Study, p. 5, November 2010

10 Symantec Critical Infrastructure Protection Study, p. 5, November 2010

11 Symantec Critical Infrastructure Protection Study, p. 7, November 2010

12 Symantec: The Night Dragon Myth
http://www.symantec.com/connect/articles/nightdragon-myth

13 Symantec Security Response Dossier: The Nitro Attacks
http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the_nitro_attacks.pdf

14 Symantec Security Response: W32.Duqu – the processor to Stuxnet, November 2011
http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_duqu_the_precursor_to_the_next_stuxnet.pdf

15 Symantec Security Response Update on Flamer 'Analysis of Flamer C&C Server' http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_flamer_newsforyou.pdf
16 ICS-CERT (Industrial Control Systems – Cyber Emergency Response Team; JSAR-12-241-01— Shamoon/DistTrack Malware, 29th August 2012 https://www.us-cert.gov/control_systems/pdf/JSAR-12-241-01.pdf
17 Symantec Security Response about Shamoon http://www.symantec.com/connect/blogs/shamoon-attacks-continue
18 Martin Lee, Symantec EMEA; Industry Risk factor for targeted attacks, September 2012
19 Symantec Security Response about 'The Elderwood Project' http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the-elderwood-project.pdf
20 Forrester, The IT-driven Energy Revolution incl. the Forrsights Budget and Industry Priority Tracker Survey, p. 3, Q4 2011
21 CRISALIS - CRitical Infrastructure Security AnaLysIS, an EU funded project for Critical Infrastructure Protection http://www.crisalis-project.eu/
22 Security Guidance for Critical Areas of Cloud Computing; Cloud Security Alliance www.cloudsecurityalliance.org
23 Symantec Internet Security Threat Report ISTR 17, pp. 25-26, April 2012
24 ENISA Smart Grid Security Recommendations; Annex III – Survey and Interview Analysis www.enisa.europa.eu
25 Idaho National Laboratory, Vulnerability Analysis of Energy Delivery Control Systems, September 2011
26 The BP Oil disaster: Stock and Option Market Reaction http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1631970
27 "Estimating the market impact of security breach announcements on firm values", Goel, S., Shawky, H.A., Information & Management v.46 p. 404 (2009)
28 CRISALIS - CRitical Infrastructure Security AnaLysIS, an EU funded project for Critical Infrastructure Protection
29 Symantec Managed PKI service http://www.symantec.com/content/en/us/enterprise/fact_sheets/b-managed_pki_service_DS_21196186.en-us.pdf

**Further reading**

White Paper 'Smart Grid – A view from Symantec' http://www.symantec.com/content/en/us/enterprise/white_papers/b-smart_grid_view_from_symantec_WP_21189389.en-us.pdf

**Glossary**

| | |
|---|---|
| AGA | American Gas Association |
| API | American Petroleum Institute |
| APT | Advanced Persistent Threat |
| BYOD | Bring your own Device |
| CA | Certificate Authority |
| CIP | Critical Infrastructure Protection |
| CSA | Cloud Security Alliance |
| DCS | Distributed Control Systems |
| ENISA | European Network and Information Security Agency |
| GDP | Gross Domestic Product |
| GRC | Governance, Risk and Compliance |
| ICS | Industrial Control Systems |
| ICT | Information and Communication Technology |
| ISO | International Standards Organisation |
| NIST | National Institute of Standards and Technology |
| OT | Operational Technology |
| PKI | Public Key Infrastructure |
| SCADA | Supervisory Control and Data Acquisition |

**Author**

Frank Bunn, Symantec Corporation

Symantec World Headquarters
350 Ellis St.
Mountain View, CA 94043 USA
+1 (650) 527 8000
1 (800) 721 3934
www.symantec.com

Symantec is a global leader in providing security, storage and systems management solutions to help customers secure and manage their information and identities.