Information Security Forum

Exploring the emerging cyber risk landscape in oil and gas

Current and future cyber risk challenges facing organisations in industrial environments

Mark Chaplin
Information Security Forum

About the Information Security Forum (ISF)

We are an international association of over 480 leading global organisations (Fortune 500/Forbes 2000), which...

- addresses key issues in information risk management through research and collaboration
- develops practical tools and guidance
- remains a fully independent, not-for-profit organisation driven by its Members
- promotes networking within its Membership.

Our Members include over 99 international banks and financial institutions

THE LEADING GLOBAL AUTHORITY ON CYBER SECURITY AND INFORMATION RISK MANAGEMENT

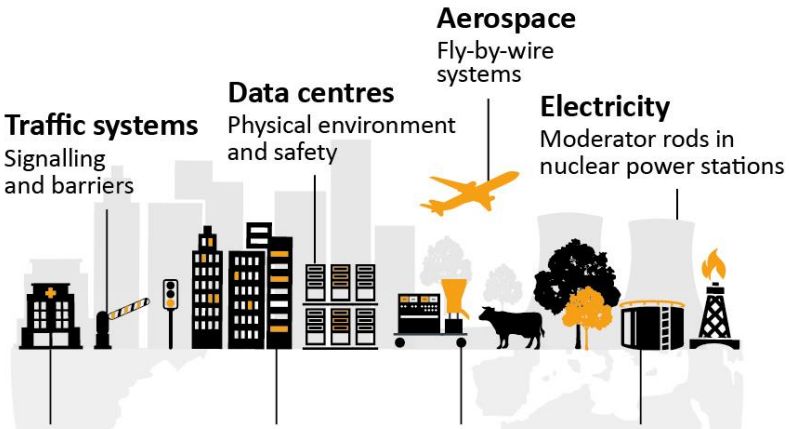
ISF services help business leaders and information security practitioners to address business issues across the enterprise

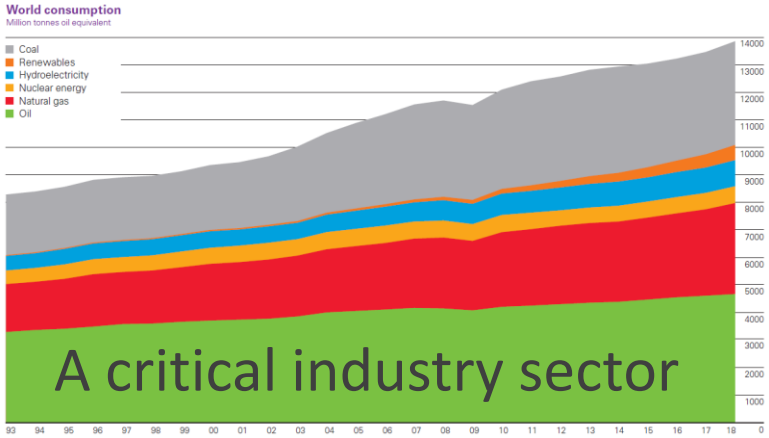
What are the issues faced by:

- Board Members
- Chief Information Security Officers
- Information Security Managers
- Business Managers
- IT Managers and Technical Staff
- Internal and External Auditors
- IT Service Providers
- Procurement and Vendor Management Teams

- Understanding cyber risk as a key component of the business strategy
- Mounting volumes of critical and sensitive information
- Increasing economic, legal and regulatory pressures
- Greater focus on privacy and data protection
- Increased dependency on the supply chain
- Need to be agile and competitive
- Changing culture of end users
- Increased use of diverse technology
- Business impact of incidents
- Emerging and changing threats
- Globalisation and cyber security

The oil and gas industry





BP Statistical Review of World Energy 2019

ISF Industrial Control Systems: Securing the systems that control physical environments

Operations

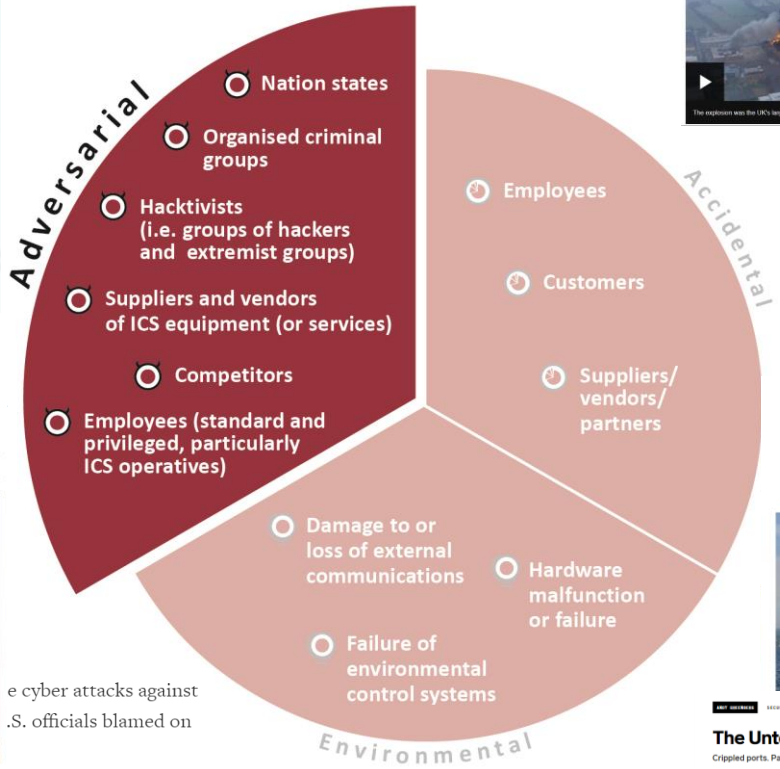
Operating in hostile environments

EXCLUSIVE

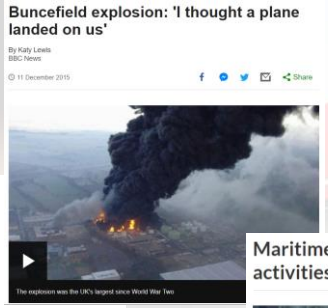
Cyberattack Targets Safety System at Saudi Aramco

One report points to Iran, but the evidence is far from conclusive.

BY ELIAS GROLL | DECEMBER 21, 2017, 6:08 PM



e cyber attacks against
.S. officials blamed on



Maritime crime threatens Nigeria's petroleum activities offshore

Cyberattack on Sau
U.S.

The New York Times - by NICOLE PERLRO

In Cyberattack on Sau Firing Back

OCT. 23, 2012

PHOTO: VesselFinder

The Telegraph

Iran oil tanker at centre of diplomatic row with UK 'goes dark' off Syria after being released by Gibraltar

The Untold Story of NotPetya, the Most Devastating Cyberattack in History

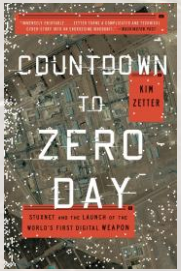
Crippled ports. Paralyzed corporations. Frozen government agencies. How a single piece of code crashed the world.

New York Times, Wired Magazine, Reuters, Foreignpolicy.com, BBC, The Independent, The Telegraph, The Washington Post, The Huffington Post, The Guardian Nigeria, Arab News, Energy Voice

Stuxnet: A case study

- Sophisticated digital weapon targeting an industrial facility
- Political landscape, international concern and UN inspections
- Years to develop and undetected for a long time
- Six month investigation
- Discovered or disclosed?
- Followed (or preceded) by Duqu, Flame, Gauss and Mini-Flame

- Rootkit & zero-day vulnerabilities
- Encrypted and nested libraries
- Command and control/peer-to-peer
- Magic markers and inoculation values
- Compromise of operations, safety and security capabilities
- Backdoors and AV evasion
- Intelligence gathering
- Decision making
- Evidence removal



Countdown to Zero Day by Kim Zetter

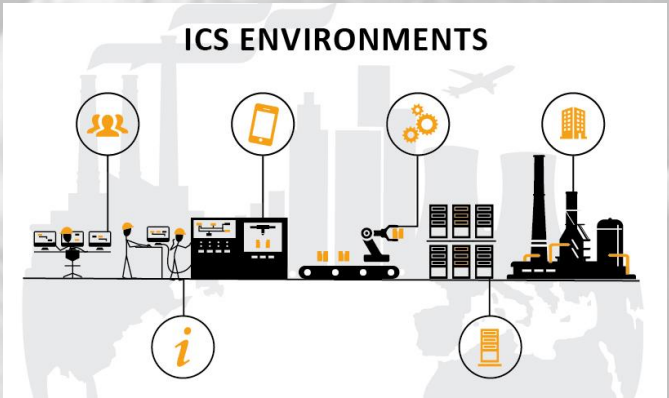
Security challenges in operational environments

Unclear level of risk

- Inherent design weaknesses
- Many technical security vulnerabilities
- Larger attack surface
- Targeting by sophisticated attackers

Uncertainty about security

- Unknown extent of security weaknesses
- Inconsistent regulatory landscape
- Heavy reliance on suppliers



Protection constraints

- Lack of ownership for protection
- Differing safety and security requirements
- Differences in terminology
- Inadequate knowledge of operational security controls

Improving cyber security in operational environments

1. Technical security architecture
2. Security configuration and monitoring
3. Security management and assurance

C.1 Build technical ICS security architecture

- 1.1 ICS security architecture design
- 1.2 Network segmentation
- 1.3 Demilitarised zones (DMZ)
- 1.4 Data communication mechanisms
- 1.5 Network devices

C.2 Perform ICS security configuration and monitoring

- 2.1 Technical and physical resilience
- 2.2 Hardware and software management
- 2.3 Patch management
- 2.4 Access control
- 2.5 Malware protection
- 2.6 Intrusion detection
- 2.7 Integrity checking

C.3 Provide ICS security management and assurance

- 3.1 People management
- 3.2 Technical security vulnerability management
- 3.3 Change management
- 3.4 Security event management
- 3.5 Security incident management
- 3.6 Business continuity and disaster recovery
- 3.7 External supplier management
- 3.8 Security assurance

ISO®

ICS › 35 › 35.030

ISO/IEC 27019:2017

Information technology — Security techniques — Information security controls for the energy utility industry

New ISA/IEC 62443 standard specifies security capabilities for control system components

ISA

The International Society of Automation

Cyber Security for Industrial Automation and Control Systems (IACS) EDITION 2

Open Government status

Open

HSE Health & Safety Executive

Operational Guide 86

Cyber protection for oil and gas operations

1. Test and update incident management and crisis management capabilities
2. Acknowledge uncertainty associated cyber risk
3. Improve cyber protection while maintaining safety, reliability and availability
4. Identify operational technology and monitor continuously
5. Provide continuous assurance of cyber risk mitigation

Information Security Forum

Thank you

isflive.org

securityforum.org