Cyber risks for critical infrastructures

MAJOR CHALLENGE FACING THE OIL INDUSTRY

Networked communications for oil platforms and pipelines allow processes to be better monitored, key functions to be automated and costs in general to be cut. On the downside, the oil industry becomes dependent on reliable and secure IT infrastructure and has to ensure appropriately comprehensive IT and communication security.

by Urs Kürzi, Customer Segment Manager

When tensions involving oil arise, they hardly bode well. Shortages have a direct impact on the price of heating oil and petrol and darken the economic prospects of entire economies. Individual waterways that tankers take to oil terminals are bottlenecks and become geostrategically significant as a result. The most minor disruption and deviation from the normal course of events quickly has massive ramifications for the global market because oil is such a systemically relevant factor. All efforts to secure the oil supply help to keep today's economic and social systems running smoothly.

Oil producers are subject to attacks from cyberspace every single day because of IT networking. The attacks could come from territorial claims from neighbouring countries or competing oil producers or be launched by frustrated employees*. Cyber risks pose big challenges to oil producers today because cyber tools lend themselves to easy scaling and targeted uses. They have a major advantage over physical attacks with genuine weapons. For instance, when pipeline or rig systems are paralysed in a virtual sense, it costs no more for the attacker to attack a large number of oil platforms in cyberspace from

Secure satellite communication is essential when prospecting for oil and gas deposits.

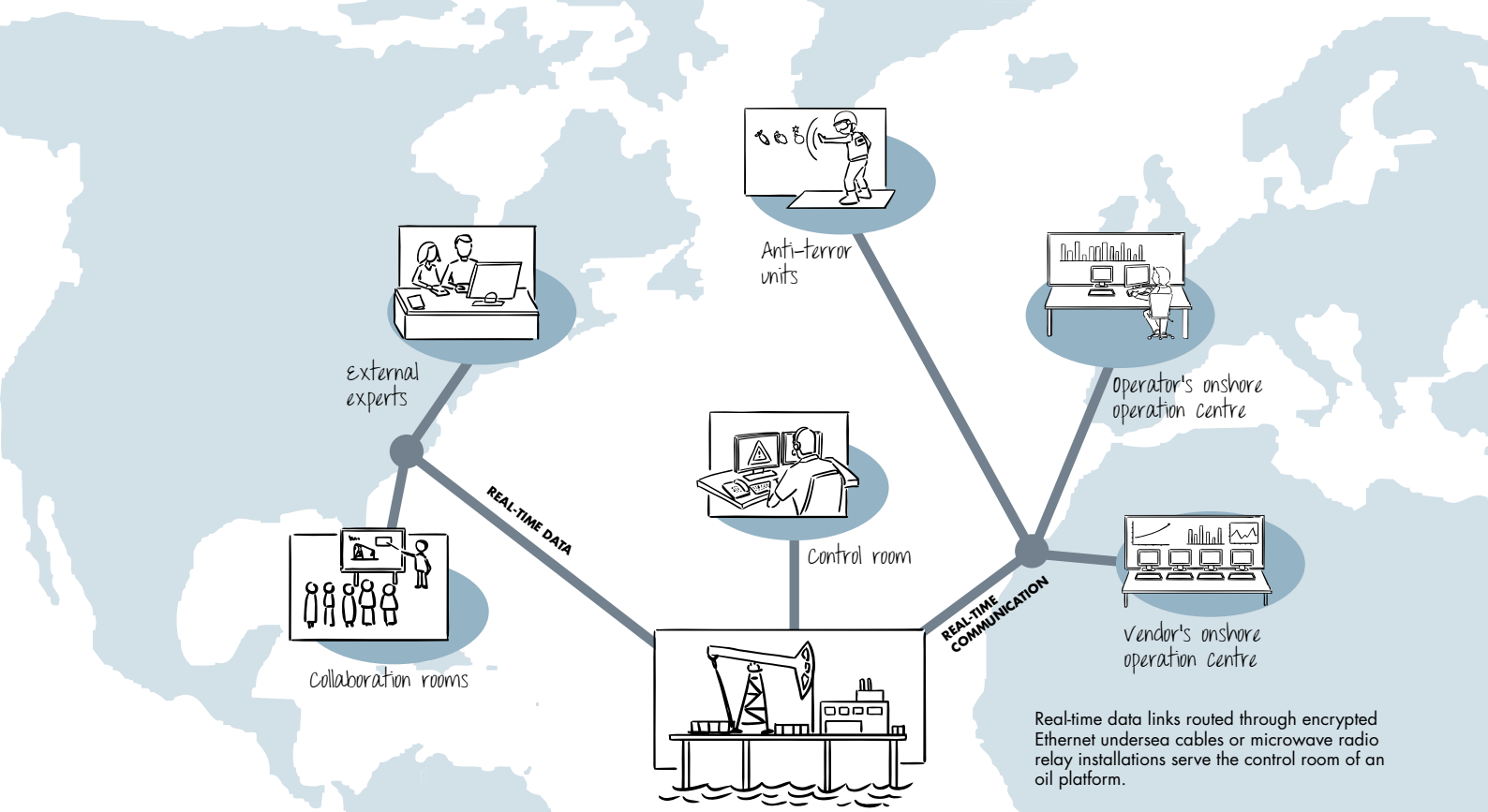
the outset. With genuine weapons, each bomb costs extra and collateral damage is enormous. Moreover, with cyber-attacks, one can usually only guess who the perpetrators are. Consequently, a "digital arms build-up" is financially advantageous for an attacker and quite efficient considering the low risk of being identified.

Anarchy as a possible outcome of being without power

It is in the interest of every country to protect its seaways for tankers, pipelines and oil platforms with their industrial installations, information and communication systems. Available technology increasingly allows oil producing installations to be run with a minimum of personnel and vital operations to be conducted by remote control from the mainland. Operators based on the mainland use real-time data links to check, measure, analyse and record drilling rig processes. The control room on an oil platform is also in constant contact with different suppliers on the mainland. The oil producers' communication network covers service, maintenance and supply organisations, emergency services and the helicopter base for evacuation missions, the operations centre and the anti-terrorist units that physically protect the production installations.

Exploration of oil and natural gas deposits

A country does well to take a strategic position on its supply of oil and natural gas. The resources for doing so include partnerships for capital and technology to develop newly found deposits; the strategic aspects of these resources have to be planned. Sovereignty in energy policy is based on huge quantities of measurements from chemical analyses of the character of the soil, assessments of territories with a big potential for oil and gas deposits, and licenses to produce in prospective regions. Finally, the deployment of new drilling rigs has to be well prepared. Sovereignty in energy policy entails a myriad of sensitive basic information that needs to be treated confidentially so a country can benefit fully from the resulting competitive advantages.



Real-time data links routed through encrypted Ethernet undersea cables or microwave radio relay installations serve the control room of an oil platform.

A confidential communication infrastructure is a particularly important factor in prospective searches for oil and gas deposits. Tapping, loss of authenticity and unauthorised examination of data are especially big risks where billions are invested in advance. Searches are typically conducted on the high seas or in remote areas. Satellite communication is indispensable. For outdoor missions, Crypto AG has a satellite communication case with the function of a secure mobile office: encrypted phone calls, e-mails, files, video conferences and secure remote access to the home network.

ICT security is a major challenge with today's networking. Experts have to implement a holistic ICT protection plan in actual practice, a plan that starts with risk identification and is summarised in a vulnerability analysis. International relations with OPEC, among others, help greatly in preparing ways of coping with extraordinary situations. Continuity management and crisis management also play a role, as do the relevant underlying laws. Information and communication infrastructures can be afforded the highest level of protection building on ICT security architecture from Crypto AG.

* Author Greg Grant reported on the attack on a computer-controlled drilling rig on 25 August 2009. A worker who was not hired full time hacked into the network from the mainland and simulated an oil leak. Fortunately, nothing happened except for virtual damage.

Source:
NZZ, 26 July 2012 Thomas Speckmann, "Der Wurm im Computer"
(The Worm in the Computer)
SINTEF report including basis for the graphics, 2007, Incident Response Management in the Oil and Gas Industry

CRITICAL INFRASTRUCTURES

Pipelines, oil production facilities, electricity companies, traffic networks, hospitals and banks are among the critical infrastructures a country has. The protection of critical infrastructures goes beyond just the national borders in each case, as is obvious from the recent attacks that have become public. Stuxnet, the cyber-attack conducted against an Iranian nuclear facility in the summer of 2010, showed vividly the new and sophisticated techniques being employed. The conclusion from this attack is that a dedicated team must have worked for years on the plan and its professional execution. Mark Bowden, journalist and author of the book "Worm", goes a step further, calling the launch of the computer worm "Conflicker" in 2008 the first digital world war. This worm attacked millions of computers worldwide in no time at all. Cyber wars are the threats we presently face. Let us protect ourselves from them so our flow of power is not shut off.