SPE Digital Security in Oil & Gas

London, December 2005

Those, like ourselves, who thought that security was a 'horizontal,' generic IT issue, were in for a surprise at the Society of Petroleum Engineering's Conference on Digital Security in Oil and Gas. Information sharing across joint ventures, complex data types and a 'nomadic' population make for rather special security requirements. And the field of SCADA[1] and Process Control Systems (PCS) as deployed in productions facilities, pipelines and refineries has its specific security issues, even though these are shared with other industries like manufacturing and utilities.

The extreme sensitivity of many oil and gas installations means that their protection is a national issue. Oil and gas security initiatives roll in government organizations such as the US Department of Homeland Security (DHS), and academic institutions. Oil company presentations included Chevron's work on a pipeline security test with the DHS, BP's approach to SCADA security, Shell on smart cards for access control and Oxy's frank presentation of the harsh reality of a true (near) disaster (Hurricane Rita).

Over the last couple of decades, the process control industry has been caught up in a massive migration to WinTel-based systems. Old timers (especially from the former PCS incumbents) regret the move to COTS, and the increased connectivity, which is considered responsible for many security issues. Both PCS and corporate IT systems are also moving from a 'China Wall' kind of security with an 'impenetrable' exterior and a 'soft inside' to 'security in depth.' The idea is that security at a very detailed level of granularity is what is required for modern systems – especially if they are to connect and share entitled data with other organizations. This 'trend' is known as 'deperimeterization'. Of course many companies are reticent to breach their Chinese Walls. One subtext here is the degree of access that will be afforded to vendors and contractors who may be pushing harder for deperimeterization than some CIOs.

Enterprise security is about firewalls, patches and anti virus software. With deperimeterization, the same issues are appearing on the plant floor. Various techniques that can be used to probe and test the security of a desktop or server may put peoples' lives in danger if applied to a plant. Patching and updating software in a live plant requires a different approach.

We'd like to take this opportunity to thank the SPE for inviting us to this informative conference and in return, offer Technology Watch readers a small plug for what will likely be another worthwhile event – the SPE Intelligent Energy 2006 Conference to be held in Amsterdam next April – more from www.ie2006.com.

Highlights

Open API for Oil & Gas security (Schlumberger)

SCADA security (BP)

Testing process control security (BCIT)

Pipeline security testing (Chevron)

Disaster recovery (Oxy)

Securing joint ventures (Chevron)

Smart card ID Management (Shell)

---

[1] *Supervisory Control and Data Acquisition – a widely used protocol to control utilities, manufacturing plants and other infrastructure.*

Contents

0528_1   Keynote Address – Philippe Chalon, CIO Total E&P

According to Chalon, although 'we all hate to speak about our own security,' there is a lot to be gained by this kind of exchange of views. Security is a concern for all of us. Total has been working on a global security plan this year involving a change of direction for its security strategy. 'China Wall' peripheral security can make life hard for joint venture partners, service providers and Total's 'nomadic' staff. Total deploys a heterogeneous IT environment with various tools including a company-provided desktop, home PCs, mobile PDAs etc. All of which are operating in a world that is getting 'more and more challenging with hackers, viruses etc.' Total has opted for a three component security architecture as follows:

1) Secure data centers with four security levels and information classified and stored according to its security level in 'vaults', 'lockers' or on 'shelf'. It has proved a major challenge to classify all data and document, which requires agreement with businesses.

2) Secure desktop, 'self secured'.

3) Encrypted data flows from store to desk.

Today there is no longer any difference (except for performance) between the internet and the secure company intranet. A user may be inside or outside the company or on a mobile device. Access is granted according to a user profile and the trust level of the device. For instance, you can't get at reserve data from the public internet in an airport!

0528_2   Securing core E&P processes – Olivier Le Peuch, president SIS[2]

LePeuch agreed with Chalon, 'putting firewall around every component is not a solution.' You need to secure processes, not components. Technology providers are there to develop a reference architecture. Last January's SPE Digital Security in Oil & Gas Conference came to three conclusions. There was a strong recommendation to create an industry security body sponsored by the SPE or another organization. This has not happened yet. Le Peuch hopes that before the next SPE Security Conference we will have begun something.

From SIS' perspective, the reserves management process crosses three departments. We need a security-centric architecture, integrated standardized workflows, identity (ID) and access management. One significant SIS initiative is a security-enabled workflow based on an infrastructure of identity mapping, a public key infrastructure (PKI), directory services and role designation. A layered approach supplies applications and data to a user's portal. Hosting this kind of environment is a 'best practice'.

What is changing? Security remains a top IT spend priority (Goldman Sachs CIO Survey Nov 2005). Upstream operations are 'accelerating'. There is increased attention on oil and gas from both regulators and investors. All of which means we need to increase productivity by workflow optimization – and we need to

---

[2] *Schlumberger Information Solutions.*

enhance application and collaboration security. The oil and gas risk profile is unusual. The biggest challenge is the joint venture (JV). JVs require a flexible IT architecture. Historically this has been addressed with 'one-off' solutions – one on one, VPN, infrastructure duplication etc.

But the emerging paradigm of 'federated identity management' (FIM) is a possible solution here. FIM can be viewed as a layer of shared ID and access management, leveraging existing credentials and defining secure channels between users and entitled resources. The idea is to create secure, streamlined collaboration and to eliminate risky third party ID management. The FIM timeline sees SAML 1.x and Liberty ID-FF (now) moving to SAML 2.0 2006. As to the way forward, 'we need to form a body to standardize and certify security across the industry'. Le Peuch suggests a technical working body to design and vet an industry-wide solution for collaboration security.

Petrotechnical application security currently means that for three applications, there will be three security systems! We do recognize the need for a multi-application environment. To enable security for this we suggest a move to an application access platform for authentication according to policy management, operating system authentication and applications hanging off the security platform. We want to publish and share this security API with industry. We plan to publish this as open source and provide sample applications.

0528_3   Government and industry cyber security partnerships – Don Paul, Chevron.

Paul described the increasing 'digital intensity' of the industry. A refinery produces 1TB/day of raw data from perhaps 30,000 I/O points and 75,000 model coefficients. A large offshore field produces 10 GB/day. A subsurface project portfolio is contained in around 1,000 TB. In Chevron, active storage amounts to over 2,000 TB in 2005 (it was 5 times less 10 years ago). Chevron totals some 4 million transaction and 2 million emails per day. Corporate data storage is growing at 2 TB/day – and this is 'not nearly enough.'

Historically, enterprise, engineering & ops and R&D/technology were three different systems. But today users and data flows cross all three domains. Everything is connected. Everyone, CIO, CFO, CTO and the business needs to get along to make security work. If you are a 'threat generator', everyone is exposed. This is not a battle to be fought and won, it is a continuous engagement. Doing nothing is not an option, 'staying the same means declining security and increasing risk.'

Government and industry partnerships are important. Government R&D can help because government faces the same problems as industry. Industry needs to dialog with the US Department of Defense (DoD). Because of the global nature of the industry, we share National Security problems.

The Institute for Information Infrastructure Protection (I3P) is a two-year-old grouping of ten institutions that performs R&D on SCADA security in oil and gas. Linking the oil and gas industry (LOGI^{2}C) is a US Department of Homeland Security (DHS) Science & Technology Unit sponsored project to improve security and reduce vulnerabilities of pipelines etc. Members include Chevron, BP, Sandia National Laboratories and SRI International. The LOGIC2C correlation engine has analyzed abnormal events over a 12 month period on a 10,000 mile Chevron Pipeline SCADA network. This has 1200 devices, 500 points of entry, is 95% unmanned and under central network control. The project used multi dimensional data analysis and a 'best of breed' LOGIC2C correlation engine. The project investigated a possible multi pronged cyber attack over a period of time with feints etc. The technique is applicable to digital oil fields now and later to complex SCADA systems that interface with the outside world as deployed in refineries and marketing. See also http://www.nipc.gov/.

> **Q&A**
>
> *What are the security risks in these environments?*
>
> Cyber threats are likely to be multi dimensional – they could involve someone altering data tables in a refinery, with potentially catastrophic consequences.
>
> *[Shell] What standards are needed for security? We don't want to make security too easy!*
>
> This is a tradeoff. You can't rip out all your heterogeneous control systems like you may do with components of a desktop computer. You need to introduce security components into an environment with multi-generational systems. There is a key need to be able to address multi-generation devices. And we need standards for validating devices. Standards are crucial.

0528_4   Implementing Process Control Security – Justin Lowe, PA Consulting[3] and Ian Henderson, BP

Improving the security state of process control SCADA systems 'is not a diet but a change of lifestyle.' In old days, process control systems (PCS) were clunky but resilient, and there was no chance of hacking them. Today, DCS and SCADA are all implemented on Wintel and increasingly on internet protocol (IP) standards and share the security risks of such systems. Except that fewer security measures exist for this specialist hardware. Even an emergency shutdown system may have an IP interface. Wireless systems may offer remote access (for maintenance). All with concomitant security risks. After the Nimbda worm, BP now has a Chief Information Security Officer (CISO) responsible for digital security. Lowe asks 'are DCS systems at risk today?' In the past there was a separation between IT and PCS. In fact the engineers didn't always get on (there was even outright hostility) with the IT department. The problem confronting Paul Dorey (Chief Information Security Officer BP) was the 400 PCS sites. These are heterogeneous, from small to huge, and were resistant to IT 'interference' in control systems. A group center of excellence was established with individual business-owned initiatives. BP has 'built security into PCS engineers' day jobs.' Security tools and cookbook have been developed along with online training.

Risk assessment involved measuring the impact of 'generic scenarios' such as the loss of all Microsoft machines, all Unix, all IP or all Ethernet (subsequent to attack by worms and viruses). This helped evaluate the strength of solutions and established a scale of 'from zero to five padlocks.' This scale 'allows the security posture to be articulated.' During the pilot, Lowe met with Ian Henderson, a PCS engineer who became a convert to the cause and moved to his current position of Advisor, PC Digital Security, for BP. Ian Henderson met with the PA Consulting specialists one morning. By lunchtime he was 'pulling out modems!' BP buys all its control systems so we need to engage with vendors to have security built in. We also have ties with Microsoft and Symantec who advise on threats to IT and process control systems. Current threats are communicated by email and telephone auto diallers. Action may involve disconnecting the PCS from IT systems. The PCS still operates, oil pumps, and refineries refine. In 2004, BP initiated vendor accreditation for antivirus, security patches and secure, remote access methods. Patches used to take 6-9 months to implement. This is now better but still variable across vendors. A related issue is the fact that it takes from 10 days to nearly a year for a security patch to be accredited. But there was a big improvement in 2005 and now anti-virus accreditation is widely accepted and standard on some systems. Patches now take days instead of weeks. Some patch in under a day. It used to be said that you can't patch SCADA. Actually you can, maybe faster than IT systems.

BP contributes to standards like ISA SP99 and API. BP also works with government organizations like the UK NISCC, the European Commission and the US Department of Homeland Security. BP is also working with BCIT on security testing (see below) especially on the Java 'Achilles' vulnerability test platform.

After security testing, what to do if you find a vulnerable system? You should contact the vendor and give them time to fix it, then apply the patch. But it is harder to patch a PLC[4] than a Windows desktop. You may find that flashing the EPROM causes the device to stop working! You can't expose vulnerabilities to the public. Penetration Testing/Red Team testing of control systems is not permissible on a plant because of the potential danger of successful penetration. 'This is not email outage or system downtime.' BP's approach is to test a PCS in the vendor's facilities, at the end of FAT[5] before a system is shipped.

BP performs security 'health checks,' site audits, presenting the results as a spider plot. This allows refineries to be compared with each other. What's next? More firewalls, more IT in PCS etc.

0528_5   Testing PCS security – Eric Byres, British Columbia Institute for Technology.

Byres asks, 'what is the likelihood and what happens if someone hacks a PCS?' A PA (REFERENCE) white paper sorts out the facts from the urban myths. ISID is an industrial security incident database with contributions on 103 incidents from 17 companies in oil & gas, power etc. Incident reporting started getting busy in 2001 and grew though 2003 (the worst year). Initially, most incidents related to internal causes (accidental). But in 2005, they are now mostly 'external', coming in over the WAN/business networks 'straight though the firewall,' or as direct IP connections, VPN, dial up etc. Many, perhaps most, firewalls

---

[3] *Joint presentation with Ian Henderson, BP.*

[4] *Programmable Logic Controller.*

[5] *Factory Acceptance Testing.*

are incorrectly configured. According to a study by Avishai Wool[6], 80% of corporate firewalls had gross configuration errors. Even a well configured firewall is not enough. The Slammer worm got into a nuclear plant through its T1 line. Routes to SCADA systems include VPN, laptops and HMI controllers (via dialup modem). Now the hacking community is starting to get interested in SCADA, with presentations at the Toorcon 2005 hacking conference. In particular, the Goose protocol of the power industry was the subject of a presentation on 'SCADA Exposed' by Mark Grimes of SAIC. The bottom line is you can't just install a PCN[7] firewall and forget about security. Perimeter defense is not enough. Plants need hardening with defense in depth.

The probing for vulnerabilities approach doesn't work in a plant. One operator scanned a robot and the arm started swinging around. An ISS scan performed on a food manufacturer's network caused PLCs to crash and lost $1 million of product. In a gas utility a consultant locked the SCADA network, shutting down the facility for several hours.

SCADA systems are beginning to interest hackers. There is market pressure to make everything talk to everything MODBUS, TCO, HTTP, some 20/30 protocols. While these are tested from a compliance standpoint, it is less clear how such systems would react to a denial of service attack. In fact products are shipped and deployed with serious flaws such as inherent protocol vulnerabilities.

Quality Assurance (Byres' specialty) is about finding vulnerabilities before control devices are deployed. Byres advocates a multi-pronged approach, profiling for vulnerable services, known flaw testing, resource starvation (DOS attacks). Following a DOS, devices may stop and never start again. Other tests include buffer overflows and 'fuzz testing,' sending mangled packets. In 2001 BCIT tried to do this for a major oil company, a task that required 30-40 different command line tools to test a device. So BCIT developed its 'Achilles Protocol Vulnerability Test Platform' (for BP and the US Government). This embeds test tools like NMAP which become plug-ins for Achilles. Six health check 'watch dog' projects have been completed. The limited testing to date has identified 10 critical vulnerabilities. Operators need a minimum security assurance level for individual devices. The 'crunchy on outside, soft'n' chewy on the inside' model is not good enough.

Q&A

The move from isolated, dedicated systems to Windows-based internet connected systems appears to have brought a lot of problems. It sounds as though IT has a lot to answer for. Do the benefits outweigh the risks of connection to the public internet?

When BP's systems are unplugged from the internet they still run.

This needs to be looked at connection by connection (BCIT).

In the past, vendors have been involved in security. But after a couple of years, nobody wanted certified devices. You can do the right thing, but it is hard to get everyone to cooperate. We need a 'common criteria' based system like the military.

The Achilles is 'common criteria'-like. Perhaps we need a TUV-like official standard (as used for safety). BP is building security into its procurement process and will only buy systems that have passed the Achilles test.

0528_6   Secure Joint Ventures – Mike Reddy, CIO Chevron International E&P.

There is increasing demand for accessing Chevron IT resources by Joint Venture partners and other third parties. Current security methods are labor intensive and provide only 'course grained' security. Reddy described a Federated Identity Management Technology proof of concept test undertaken this year by Chevron, Schlumberger, Sun, Microsoft and others. Federated identity is a standards-based means of sharing an identity and entitlements across different domains – as between JV partners and their contractors. The test was performed across 30 servers with heterogeneous federation technologies. The test ran with Chevron's web-based 'Operational Excellence' application and Schlumberger's Petrel. The demonstrator showed that seismic interpretation could be performed across the firewall using Citrix thin clients. Standard Microsoft Office and web-based applications can be shared securely today – although more support is forthcoming with Microsoft's Longhorn/Vista server. Computer Associates' eTrust SiteMinder 6.0 also ran. Reddy concluded that while federation services can help, they will not solve everything.

---

[6] *IEEE Computer Magazine June 2004.*

[7] *Process Control Network.*

0528_7   Security and disaster planning – Don Moore, CIO Occidental Oil & Gas

What keeps me Don Moore awake at night? Security and disaster recovery planning. There has been a lot of focus around this in the past year, with a brainstorming session to identify potential security problems. These might include a tornado on Tulsa, geological issues (Ecuador-volcanic activity, west coast earthquakes), geopolitics (guerilla activity) and terrorist threats (a dirty bomb in LA) etc. 'We operate in dangerous places.' Disaster planning is now a full-time job in IT.

Hurricane Rita put Oxy's planning to the test. Houston is Oxy's largest office. With Rita, Oxy learned a lot about shut down, business recovery etc. Houston-based employees were concerned for their personal safety following what happened in New Orleans. Employees started disappearing, shutting systems down in the middle of moving data. Three million people tried to leave Houston at the same time. It was taking 27 hours to cover the 220 miles to Dallas. In general, while Oxy's disaster plans worked, business continuation 'did not work well at all.' Business continuation is directed at protecting corporate IP, most of which is digital these days.

> **Q&A**
>
> *What are you doing to fix these problems?*
>
> We are tightening up on security, audits etc.
>
> *When have you done enough?*
>
> We thought we had before Rita. But things didn't go according to plan. We have gotten help from outside. Consultants have done a great job managing firewalls etc. But we will never be through.
>
> Shell also uses outside people.

0528_8   Security in the automated company – Ibrahim Lari, Dolphin Energy

Dolphin Energy is a UAE-based JV between Oxy, Total, ADCO and operates Qatar's North Field. Dolphin has combined IT & DCS over the field, linking plant automation with its ERP systems. Plant automation applications are integrated for production accounting, mass balance etc., easing decision making. But security is an issue with 200 plus switches in the plant. It was different with old style DCS that were hard to penetrate. Dolphin is undertaking a risk assessment of DCS penetration etc. These are 'serious challenges to the automated company.'

0528_9   Global identity management – Edmund Yee, Chevron

Chevron is deploying a common image for its Windows desktops with automatic update and an enterprise security architecture. This involves all users – employees, contractors, 3rd parties, JV partners all have managed identities as users and administrators. Devices and services (applications) also have IDs. All business processes use IDs (line of business, SAP, Oracle, network logon, applications etc.) The idea is to 'unify and simplify physical and logical access with a single corporate ID card.' This provides a single common process for authentication. The first result is a reduction in Helpdesk costs where the N° 1 issue was password management with about 3000 password resets per month globally (at $20-40 a time). The project is also designed to ease merger and acquisition activity. It also offer ESSO[8] and Web ESSO single sign on where needed. Shell's identity model has a Meta Directory and HR system at its core. This is surrounded by directory services along with a 'provisioning workflow.' Outside everything is the Active Directory. Authentication plug-ins have been developed for specialist applications such as G&G.

A desktop enforcement tool (Windows only) is in trial and an emergency access tool for lost authentication. The plan is to get rid of passwords next year as critical components become available. Role-based access control (RBAC) is defined in the Directory. Biometrics authentication is available for special groups. The project was difficult because of multiple stakeholders – HR, IT facility, Company. Shell has built identical test/production structures and data content. Security is about process and it is important for an outside audit company to check for security flaws. The proof of concept on immature technology was a challenge. Many competing vendors wanted to be 'right behind' the Windows GINA[9].

---

[8] *Enterprise single sign on.*

[9] *Windows 'Graphical Identification and Authentication' technology.*

Q&A

How do you do emergency access?

Today an emergency card can be activated through a phone call. We are working with Microsoft and RSA to develop a long term solution.

Can you quantify benefits as to cost, or a reduction in security incidents?

The main benefit is in card issuance – employees look at the card as their corporate ID. It is taken more seriously and lost less. Password resets are down.

What is special about this to the oil industry?

Nothing.

0528_10 Large scale smart card deployment – Ken Mann, Shell

Shell's IT Infrastructure Refresh Project began in 1999 and involves 120,000 users in 135 countries at 1200 sites. It has reduced the cost of delivering a desktop by 50%. It is based around Windows 2000 and Active Directory. Email is encrypted on the fly depending on its confidentiality level. A Smart Card-based solution 'gives preference' to Microsoft-based products. The original goal was to build an out-of-the-box infrastructure 'without engineering.' But it 'didn't quite work like this although much was already in the operating system. Like others, Shell is moving from the 'hard perimeter, soft interior' security model, moving security down. Any device trying to connect will have to pass a number of tests. It may be restricted to guest internet access or full access if all its patches and anti virus are up to date. Schlumberger Information Solutions is to take this smart card management system (SCMS) to market. Microsoft is 'pushing smart cards hard.' Both Shell and Schlumberger are early adopters.

0528_11 SCADA risks & vulnerabilities – Mark Logsdon, UK NISCC

COTS[10] hardware and software has let hackers into water and electricity supply systems – notably with a denial of service (DOS) attack on Israel Electric Corp. In general, terrorism-related incidents are 'probably under-reported.' There are risks from hackers and politically motivated individuals. Today, PCS/SCADA vulnerabilities are 'widely understood.' NISCC has set up a number of information exchanges, with regular discussions of threats and vulnerabilities. Vendors, including US firms allow NISCC to manage vulnerabilities in their software and to share the information with members. NISCC, along with PA Consulting has published a good practice guide – see links below. Threat investigation is also a large part of NISCC's work, studying the *modus operandi* of hackers and other groups. Companies should ask 'would you recognize an attack/intrusion?' The answer is probably not. Logsdon opined that eventually, PCS will 'merge and be subsumed into the IT department.'

Links

NISCC SCADA Portal

SCADA & PCS firewall best practices

SCADA security policy best practices

NISCC Warning Advice Reporting Point toolkit - WARP

Q&A

How sure are you that there will be/has been an attack on a PCS?

There are examples in the UK and elsewhere of PCS attacks. These were discussed at a recent Birmingham hacking conference, coming from criminals using 'hacking tools for hire such as a botnet for DOS. It may be hard to know it is happening. This is unlikely to result in a system crash, more likely the aim would be to steal data, IPR issues or spy on M&A activity etc.

Is your own Portal secure?

Yes.

0528_12 The developing laws of cyber security – Jeffrey Ritter, Kirkpatrick & Lockhart Nicholsen Graham

Company portals 'store evidence of failure' and may represent 'summary judgment evidence against the company.' Many rules and regulations govern a business and all represent potential points of failure.

---

[10] *Common off-the-shelf.*

Lawyers may even perpetuate business inefficiency. Ritter proposes a new 'systems law,' bringing the communities of law and technology/security together. In addition to 'legal' rules, systems law includes 'technology' rules. These are 'the rules by which systems are designed, constructed and operated at all levels of their architecture.' There is a hierarchy of technology rules, from company business rules and computer codes, to the infrastructure stack (comparable to the telecom stack in fact). Standards are essential to achieving trusted information exchange across communities at all levels of complexity. Standards are 'the language of shared knowledge.' Ritter advocates replacing the ambiguity of 'legal law' with well-defined 'systems law'.

Q&A

Is it possible to have zero risk?

No, but you should manage toward this...

Please give some examples of applicable standards.

HTTPS – this is never specified in legal agreements

NISCC is in the game of ensuring that standards are secure. IP stack, next generation networks.

Do you have 'shining examples' elsewhere that we should be emulating? Of intrinsic rules in hardware enabling trusted communities.

E-payment is a good example of an industry driven commitment to security. Zero day settlements are a possibility. Also the American Chemical Society has developed ISO standards as condition of membership. Members commit to the ISO 17799 standard in auditable framework. The US Government gives favorable treatment to members of ACS.

[Herb Yuan] I hear some dissonance in this industry which is not known for its adherence to standards – or for change in general. I'm chairman of POSC and responsible for standards in Shell. What force and in what time frame do you see us moving to this aspired state?

A Japanese study demonstrated the relationships between rules of network and rules of law. With the passage of time, communities form and grow, building on the rules. There is 'spontaneous generation' of competing standards to fill gaps. Standards can be seen as conveying a competitive advantage. The global information society will not prevail without standards and rules. The question is, 'who will write the rules.' If companies don't, government will. Today, a lack of information quality is impacting network use.

0528_13 Sarbanes-Oxley – Chris Wright, KPMG

Following the major capital scandals of Enron and the like, people could no longer rely on balance sheets. Paul Sarbanes and Michael Oxley's act was designed to restore faith in company accounting. Even if you don't work for a company with US shareholders, the reporting standards are spreading. Sarbanes-Oxley (SOX) aka section 404 is specific to a company's controls over its financial reporting (and only this – not all internal controls). SOX only addresses the financial reporting of COSO Framework. Three IT areas are impacted: 1) Trust CIO, IT strategy, 2) IT controls, a new scope was mandated by PCAOB and 3) Process controls, with three-way matching of invoices. Some companies thought that if accounting was outsourced, it was 'nothing to do with us,' but companies cannot delegate responsibility for control. Note that SOX stipulates that IT shouldn't have access to live financial data. So some companies have put monitoring in place and then had nasty surprises as to who could see their financial information. Change management is also an issue. Business continuity management is specifically excluded from SOX because SOX is not concerned about the future value of assets. 'SOX is about the 31st of December.' It does cover a company's ability to backup and restore financial data, to ensure that a transaction has completed, been properly recorded and authorized. Note that nine companies in the energy and utilities sector failed SOX. Some was 'Creative accounting,' but for IT, the problem was mostly access and control. Useful resources include 'The IT Executive's Best Practice Guide to SOX,' a Gartner White Paper[11]. See also www.itgi.org and COBIT's good papers on SOX deployment. This incidentally 'has put an end to the way many people use spreadsheets.'

Q&A

[OXY] We have spent a lot of time on the outside and are now looking at the interior, access control etc.

---

[11] *See also the SOX Toolkit.*

Yes one company had 2,000 users who had left but who were still on the system – a big potential threat. SOX has changed awareness of this.

But a lot of time is wasted on systems that don't refer to SOX. How do you ring fence SOX?

SOX is not HSE. It is about systems that are used to produce financial information, especially around reserves. You need a top-down approach to see what impacts financial numbers.

How do you manage access for database and system administrators?

With a two-part password and two people responsible for sensitive parts of the system – and by logging what was done by whom.

0528_14 Compressor health monitoring – Nick Bleech, Rolls Royce

Rolls Royce (RR) compressors are widely used in oil and gas. Unit Health Monitoring (UHM) of these massive units transmits real time information back to RR for predictive & preventative maintenance. 60 UHM-capable units have been delivered to date. Information goes over the internet – so a secure solution was required. The UHM server must be able to shut down without affecting operations. IPSec (IP security) has been added to the UHM network. This uses 2-factor authentication. All part of 'deperimeterization' – the term came from the Open Group 2002 Jerico Forum - defining a set of standards for secure use of the internet. This kind of application needs standards, common policies. There is also the 'trend' of the semantic web, described by Bleech as 'a move to a genuinely useful way of sharing and discovering information.' ISO 27000 series also ran. UHM 'illustrates the inevitability of deperimeterization.' See www.jerichoforum.org for more on shared trust forums.

Q&A

[ConocoPhillips] Deperimeterization could conflict with the customer's view. What if they say 'no'?

We bear the hit of building an authenticated link. We do this already for customers without a network.

0528_15 Microsoft security in manufacturing – Ron Sieliski, Microsoft .

There is a tradeoff between usability, security and cost – 'You get to pick two.' Microsoft is working on cost effective solutions to the other two issues. The Manufacturing Automation Protocol (MAP) was 'forced on suppliers by the automotive industry' and is 'exorbitantly costly.' Hence the move to low cost OLE for Process Control (OPC). The other side of the coin is that incidents reported to CERT, such as DOS, damage to systems and loss of data are growing exponentially. In 2004 there were so many incidents that CERT gave up recording them. But 'there is no going back on commodity technology for connectivity.' This gives 'great visibility of the manufacturing process.' According to a Gartner study[12], 'Microsoft will dominate plant floor for the remainder of this decade.' The same goes for pipelines and other energy systems. Operators may still run DOS, Windows 3.1 and 95 which are no longer supported. A straw poll of the audience revealed that some (Baker) still have DOS, Windows 95 running – others 'don't know'. One reason standards bodies (ISA, NIST) have a problem is that 'they abstract so much that they don't address the problem.' Every environment is unique.

On security, Sielinski advocates 'defense in depth' with multiple layers of security. The Windows Security Center 'brings it all together.' AntiSpyware has been the most popular download ever from Microsoft. A new security scanner is available from http://safety.live.com to scan for vulnerabilities. OneCare Live[13] (another download in Beta) that runs 24hr/day and tells you your system is clean. Microsoft Update is being changed to have everything in the same place. Microsoft Baseline Security Analyzer 2.0 for small businesses is a Windows Server update service that helps administrators decide on patch/update policy so that legacy applications can still run. Antigen security is used for messaging. Microsoft identity and access management leverages Alacris smart card[14], Windows Server and Active Directory underpin ID management.

See www.microsoft.com/security/guidance, where there are '16,000 pages for your perusal.' Work is in progress on a 'most secure configuration' for process control with Honeywell Invensys and SciSoft. The aim is to 'put the trust back into computing.'

---

[12] *Possibly a selective quote – see for instance this Managing Automation article.*

[13] *Strangely 'only available in the USA'.*

[14] *Acquired by Microsoft earlier this year.*

Q&A

What patch management tools are used for control systems?

Windows is a commodity technology. It's the same OS and same tools for process control as for others.

Security Resources

Using OPC via DCOM with Windows XP Service Pack 2

NCSP Improving Security Across the Software Development Lifecycle

ISA SP99 Manufacturing and Control Systems Security

CIDX Cybersecurity Initiative

NIST Process Control Security Requirements Forum

ARC Advisory Group CyberSecurity Portal

0528_16 Combined threats – Barry Horne, QinetiQ[15]

Horne described a 'thought experiment' of a 'combined threat' (both physical and cyber) on a fictitious oil company. First the company website was defaced, and then a white powder delivered to reception. All meetings were cancelled. But the board members showed up anyhow. An email virus arrived and caused the mail servers to 'fall over' because of multiple 'reply to all' emails, a 'DOS executed on itself'. E&P databases pirated, a bomb on a train, the cell phone network overloaded. The study showed how a 'nuisance' event may be a cover for a more serious cyber attack. Companies should ask, 'What's going on beneath the noise.' But even if a global email says 'do not reply to all,' people still do.

0528_17 Technology Watch subscription information

This report has been produced as part of The Data Room's Technology Watch reporting service. For more on this subscription-based service please visit the Technology Watch home page or email tw@oilit.com.

© January 2006

The Data Room
7 rue des Verrieres
F-92310 Sevres
France

Tel (USA)	281 968 0752
Tel (UK)	020 7193 1489
Tel (France)	+33 1 4623 9596
Fax	+33 1 4623 0652
	info@oilit.com.

---

[15] *QinetiQ used to be a part of the UK Government Defense Evaluation and Research Agency DERA and is still part-owned by the Ministry of Defense.*