Some 175 attended the American Petroleum Institute's (API) 4th annual oil and gas IT security conference. Last time we reported on this topic, from the 2005 SPE IT Security Conference[1], ([TW 0528]) there was talk of 'de-perimeterization.' a move to open up the isolated (and secure) SCADA and DCS systems and connect them to business networks. This was to enable more direct access to real time data in ERP and management systems. Five years on, now that 'de-perimeterization' has to a degree happened, some are having second thoughts as to the wisdom of opening up what can be sensitive processes and networks to access by a wider community. Boardwalk Pipeline is moving to 're-perimeterize' (*our term*[2]), isolating its SCADA system from the business network. A similar move is envisaged by Colonial Pipeline.

'A study' found that less than 1% of successful attacks resulting in actual data loss came from outside the organization. 19% were perpetrated by disgruntled employees and 80% were accidental. Such findings have lead companies to move from reactive to proactive threat assessment, incident response and risk management. Realistic drills are considered key elements in security. Server virtualization and cloud computing are suggested as a route to enhanced security, providing suitable attention has been given to roles and responsibilities. Traveling employees make for a particular risk – and there are moves to lock down devices and encrypt traffic. Still, mobile devices can mean 'really rough' gaps in security. The situation is worse when top management flaunts the rules and uses the latest, unsecured electronic gadget! Management involvement in security appears to be work in progress – there is a need to move from an 'authorizing' culture to 'mandating' security initiatives. Finally, several US government agencies have issued roadmaps and other documentation on securing SCADA systems.

Highlights

The security 'nightmare scenario'

Segregating SCADA and business systems (re-perimeterization)

Emerging threats

Securing the mobile workforce

Table of Contents

This Technology Watch report was produced by The Data Room.
For more information and sample reports please visit
www.oilit.com/tech **or email** tw@oilit.com**.**

---

[1] *Full text available on http://www.oilit.com/1_tw/2005_contents/0528_SPEDigitalSecurity_2005.pdf.*

[2] *The term 'reperimeterization' also appears in the context of Network Access Control – see for instance http://www.opus1.com/nac/index.html.*

0928_1   Keynote – Harry Raduege, Deloitte and Touche

Lt. General (retired) Harry Raduege's keynote traced the history of cyber-security from the first hacker attacks in 1979 to the findings of the Center for Strategic International Studies (CSIS) Cybersecurity Commission. These include the necessity of securing Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition (SCADA) systems for industries like upstream oil and gas and refining. While the specifics of the report are classified, it is understood that recommendations include background checks on personnel working on pipeline SCADA systems. The theft of laptops from executives traveling overseas is now 'a matter of national security.' Raduege warned, 'if your DBA is driving a Ferrari, check your network security' and concluded that the prevalence of consortia and universities in the oil and gas industry, 'makes the probability of data leaks even higher.'

0928_2   A security 'nightmare scenario' – Michael DuBois, Colonial Pipeline

DuBois described a hypothetical 'nightmare scenario' plan involving an attack and ransom demand on a major US Pipeline perpetrated by an 'insider.' Pipelines used to be secured through 'isolation and obscurity.' But today, adding Microsoft Active Directory to SCADA systems or even just running an operating system patch can open security holes. Industry needs the government to provide more specifics on threats. A study found that less than 1% of successful attacks resulting in actual data loss came from outside the organization, 19% were perpetrated by disgruntled employees and 80% were accidental. Funding of pipeline security remains a priority despite market downsizing. DuBois advocates vetting of personnel, partnerships with labs and 'at least' yearly simulations and drills. He closed by wondering if the best strategy was not to go back to isolation.

0928_3   Segregation of SCADA and business systems – Brian Gore, Boardwalk Pipeline Partners

Boardwalk participated in a 12-hour drill that included a 'mind numbing constant attack.' The specifics of the exercise are secret, but Gore revealed that one team was given a 30 minute head start to implement security by running Nmap, Wireshark, TCPDump, and OpenVAS to baseline the network traffic and then develop a list of firewall rules, ports to lock down and routes to change. The drill included corporate 'resistance' to the shutting-down of business systems and corporate ignorance of the danger level. As a result of the exercise, Boardwalk is now engaged in a plan to completely segregate its SCADA system from the business network, with the ability to deploy security and lock down the pipeline system and then open connections as needed. The drill underlined the importance of communicating with management, the need for baseline data to identify anomalous events and a plan to 'attack yourself' continuously and 'think outside the box.' It takes CPU power to analyze network traffic and understand 'confusing' protocols. Gore now advocates monthly simulated attacks and redundant ways to communicate and operate. Management should be 'requiring,' not authorizing security. He concluded by emphasizing the importance of SCADA compared to business systems observing that 'if a report doesn't go out, no one is going to die, but are we OK with blowing up a town?'

0928_4   National SCADA Testbed – Gary Finco, Idaho National Lab

The Idaho National Lab houses the National SCADA Test Bed (NSTB) run by the DoE's Office of Electricity Delivery. This facility does joint installs with vendors two to three times a year, publishes procurement guides for security products, and includes cyber, wireless, and SCADA critical infrastructure protection test beds. A recent assessment of twenty systems, 13 in their lab and 7 on-site, identified vulnerabilities in communications, applications, systems, web interfaces, account management, and information disclosure.

0928_5   The Consensus Audit Guide for SCADA – Al Rivero, Telvent

Many core SCADA servers are still UNIX-based and associated systems need physical protection when these computers fail. There are three levels of threats, hackers working for notoriety, disgruntled employees seeking profit, and nation-states 'intent on disruption.' Rivero stopped short of advocating prescriptive regulation, advising instead the adoption of a 20-step Consensus Audit Guide for SCADA systems[3].

[3]*Government Computer News - www.gcn.com/Articles/2009/02/23/Baseline-IT-security-guides.aspx*

0928_6 Virtualization's role in security – Ivan Skeri, Baker Hughes

There is a good business case for server virtualization. Advantages include cost and complexity reduction and 'resource isolation' that brings improved reliability and security, better services levels, automated server provisioning, better hardware and energy utilization. Storage, network and application virtualization plays a role in security, especially for containment and quarantine during attacks. Virtualization can help isolate a problem and limit its impact by creating Internet access and network monitoring partitions. A 'honeypot' can be implemented to trap attempted attacks and for 'self-testing' exploits in a contained environment.

0928_7 CIO Panel

The CIO panel included Zhanna Golodryga, CIO of Global Petroleum at BHP Billiton, Jim Green (Chevron), Kevin Campbell (Hunt Oil), Mike Perroni (Halliburton) and Don Worley (Marathon downstream). Moderators were Dan Chisum (ConocoPhillips) and Paul Huttenhoff (Chevron).

What are the CIO's biggest challenges?

Marathon – Keeping their assets running and maintaining visibility of security issues up to Board level.

Halliburton – Customer data security especially since most security issues were related to manual processes.

Chevron – Sustainable compliance procedures, not just reactions to events.

Chevron – How to make every user aware of their security environment.

Hunt – The security aspects of 'social engineering.'

How can CIOs educate the CEO?

BHP – By explaining the balance of risk and trust against the ability to work.

Marathon – By making regular security reports to the Board and presentations to C-Level managers – especially regarding the take-up of social networking applications.

How are companies dealing with social networking?

BHP – We have policies for mitigating the risk, but are also looking at the advantages.

Hunt – We currently block Facebook and Twitter although we do have a pilot program running with 25 college interns.

Chevron – We are still asking where the value is!

Halliburton – We block all social networking sites for productivity reasons.

What security metrics are deployed?

Hunt – We look at security metrics the same way as we view insurance, by measuring incidents and exposure.

Halliburton – We have good metrics for the percentage of transactions that are blocked.

How do you rate insider vs. outsider risks?

Hunt – We rate the insider threat below that of keyloggers and malware.

BHP – We proactively monitor unusual activity.

Chevron – Our effort focuses on third party employees and joint ventures.

What are the risks of cloud computing and software as a service (SaaS)?

Chevron – We are bullish on cloud computing although we are still assessing the risks.

BHP- We have concerns about providers' liability – and are looking at internal provision first.

Marathon – We do use SaaS but only with a formal risk assessment cover

0928_8 Emerging threats - Sujeet Shenoi, University of Texas

Attacks have been made on ATM machines and voting machines. These are basic SCADA devices that, although protected by volunteers, can be attacked by a wireless or PCMCI port. Today telecom attacks can be floods of valid messages, or spoofed 'transfer prohibited' messages that force re-routing. Working with Williams Pipeline Natural Gas, U Texas has analyzed MODBUS on TCP traffic to show that 22 of 29

possible attacks are at 'severe' risk level. Using the DNP3 protocol for electrical systems, the number of possible attacks goes to 91, and the arrival of 'smart grid' devices will make the curve 'exponential.' Companies at risk can isolate, encrypt, authorize, and secure their SCADA services (reactive policies), or they can be proactive and use threat assessments and situational awareness for anomaly and intrusion detection, incident response and risk management. Some security threats can have massive costs, such as the 'tromboning' of call packets to lengthen telecommunications into higher rates. Future proactive measures must include multi-layer defense in depth strategies, leveraging the trend of SCADA systems to store historian data to make forensics easier, and using the fact that SCADA data streams 'tend to have less random packets than TCP/IP.'

0928_9   Security and cloud computing – Jim Reavis, Cloud Security

Some of the hype around cloud computing is real, as evidenced by 'the acceptance of computing as a utility in oil and gas.' Governance challenges include the possibility of the provider going out of business, failure to achieve SLAs, or poor business continuity planning. There are also questions of financial stability, data centers in countries with unfriendly laws, proprietary lock-ins with technology or data formats and the fact that mistakes made by the cloud provider's internal IT security can be orders of magnitude more serious. It is analogous to the comparative risk and exposure of a car crash vs. a plane crash. Cloud computing threats include unvetted 'innovations,' publicly-known cloud architectures and the fact that the load management itself can be used as an attack. Cloud computing also opens up new avenues for attacks such as poisoned AMI images. The Cloud Security Alliance was set up to facilitate the adoption of security standards (at a time when most of the industry is not talking to each other) and to provide pragmatic guidance in 15 different domains around governing and operating in the cloud. Principles include secure location of data, the right to audit on demand and the need for retention policies to meet e-discovery standards. The cloud can open up vulnerabilities and there is a need to 'compartmentalize' during incident response – data encryption keys should not be available to cloud providers. The concept of federation must be standardized – 'common sense is not optional.'

0928_10   Securing the mobile workforce – Fabio Ottolini, Schlumberger

The biggest challenges to security are external storage and multiple connectivity routes. Supporting different device models, features, network coverages and roaming charges can be problematical. The answer is user awareness of costs, expectations and policies, supported by documentation, quick guides, testing and change management. A standard operating system is desirable, but pressure from the C-Suite for the latest device can sometimes drive purchase decisions. The best bet is to involve local procurement specialists and set user expectations for support, since device management is never global or complete. Schlumberger uses data encryption, expiring PIN's, remote wiping and self-destruct technologies. Other considerations are backups and certificates, with the knowledge that for attackers, mobile devices may be the path of least resistance.

0928_11   Securing the mobile workforce – Jim Heaton, Baker Hughes

Mobile devices mean 'really rough' gaps in security. Baker Hughes approaches the problem by addressing the human factor with onboarding and offboarding procedures, mandatory training and scorecards. The company also uses external audits and a 'poison pill' that disables devices after a couple of days of without connectivity. Network security zoning is used for untethered PC protection and can shut down USB ports in the field. A mobile security Market Based Reference Model is used to evaluate vendors. But it is recognized that application and session control may not be as mature as other capabilities. In preparation for next-generation technologies, they are evaluating Bluetooth security, geo-fencing for access based on location, and cloud backup technologies.

0928_12   Exhibitor - Alert Enterprise

Alert Enterprise provides security software combining IT and physical security to monitor and respond to cross-enterprise threats in compliance with the Chemical Facility Anti-Terrorism Standards (CFATS). Their system can enhance monitoring in targeted areas based on HR system activity like employee actions or reviews. More from www.alertenterprise.com.

0928_13 Other resources

0928_13.1 DoE[4] Roadmap to Secure Control Systems in the Energy Sector (2006)

http://www.oe.energy.gov/DocumentsandMedia/Roadmap_to_Secure_Control_Systems_in_the_Energy_Sector.pdf.

0928_13.2 DHS[5] Roadmap to Secure Control Systems in the Chemical Sector

http://www.us-cert.gov/control_systems/pdf/ChemSec_Roadmap.pdf

0928_13.3 DoE INL NSTB Report on Common Control System Security Vulnerabilities

http://www.oe.energy.gov/DocumentsandMedia/31-2008_INL_Common_Vulnerabilities_Report.pdf.

0928_13.4 API Conference Website and Presentations

www.oilit.com/links/1001_9.

0928_14 The Data Room – Technology Watch

© February 2010

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

Technology Watch Home Page   info@oilit.com

---

[4] *Department of Energy.*

[5] *Department of Homeland Security.*