cybersecuritylaw&practice

STRATEGIC ANALYSIS BY DATAGUIDANCE
VOLUME 01 ISSUE 07 OCTOBER 2015 WWW.E-COMLAW.COM

Report identifies nuclear facilities major challenges

Nuclear facilities around the globe are facing major industry-wide, cultural and technical challenges to effective cyber security, think tank Chatham House has identified in its report on 'Cyber Security at Civil Nuclear Facilities: Understanding the Risks' published on 5 October.

"Stuxnet demonstrated that air gapped facilities are no longer immune to attack and with the increasing concern over insider threats, it was time for nuclear facilities to be examined with a fresh perspective," said Steve Durbin, Managing Director of the Information Security Forum.

The report identifies 'major challenges' including insufficient spending on cyber security; and reactive rather than proactive approaches to cyber security, and puts forward recommendations, which include establishing an international cyber security risk management strategy.

Dr. Jonathan Cobb, Senior Communication Manager at the World Nuclear Association stresses that cyber security "is an absolute priority," but that the report's comments on current practice do not reflect progress made over recent years.

IN THIS ISSUE

Standard & Poor's issues rating warning about banks' cyber risk

US financial services company Standard & Poor's ('S&P') published on 28 September a note, 'Credit FAQ: How Ready Are Banks For The Rapidly Rising Threat Of Cyberattack?' in which the agency noted that a bank's 'weak cyber security' is a risk that could lead to a bank having its credit rating downgraded by the agency.

S&P describes cyber crime as an 'emerging risk,' and, although the agency notes that cyber breaches have yet to impact ratings on global banks, S&P states that should it assess a bank to not be adequately prepared for a cyber attack, a ratings downgrade could be made without an actual attack taking place, while the negative issues resulting from an actual breach could also lead to S&P downgrading a bank's rating, if the 'significant reputational issues [...] could result in a major loss of customers or if the monetary or legal losses significantly hurts capital.'

"If customer data is stolen in bulk the ramifications can be enormous and can lead to extremely large fines from a regulator and class action law suits brought against the banks from disgruntled customers," said Mike Pullen, Partner at Stephenson Harwood LLP. "Given the risk that banks are now facing, both financial and reputational, any bank that does not take adequate steps to put in place sufficient security measures to prevent a cyber attack is clearly not doing enough to look after its own interests and those of its customers," said Rhymal Persad, Managing Associate at Mishcon de Reya LLP. "Agencies such as S&P would appear entirely justified in adjusting a bank's rating accordingly to reflect the increased risk that a bank is taking."

S&P also outlines in its note how, if a number of cyber breaches affect the banking industry, the result could be an impact on S&P's banking industry country risk assessments.

S&P further describes some of the questions currently being raised with bank management teams in relation to cyber risk, with topics including a bank's monitoring procedures, both internal and external, the institution's safeguards against phishing attempts made against its staff, and its cyber security insurance. "Given the increasing threat posed by cyber crime there is every possibility that other agencies are likely to follow suit in the future," believes Persad. "S&P and the other ratings agencies if they follow S&P's lead may also insist on seeing details of independent external cyber audits," adds Pullen.

NIST releases draft document to address vulnerabilities in email

The US National Institute of Standards and Technology ('NIST') released on 6 October a draft document, 'Trustworthy Email,' which seeks to enhance trust in email, whilst the National Cybersecurity Center of Excellence ('NCCoE') is working on a Domain Name System ('DNS')-based secured email project, to lead to a publicly available NIST Cybersecurity Practice Guide.

"Past data security breaches have shown that email exchanges are one of the major attack points for criminals," explains Alex Lakatos, Partner at Mayer Brown LLP.

Trustworthy Email suggests solutions to address all common exploits; for confidential email, NIST suggests that organisations encrypt email between sender and receiver or secure the transmission between email servers. "Email is vulnerable to more sophisticated attacks," said Lakatos. "Businesses should therefore focus on employee training and be on top of developments in technology and security protocols that make email more secure."

The NCCoE's project will see technology vendors collaborating to develop a platform that provides 'trustworthy' email exchanges across organisations. "The NCCoE points out that adoption and implementation of DNS-based secured email solutions has been slow," said Lakatos. "Demand will probably increase as a result of NCCoE. Also, data security, including email exchange security, is a growing concern for business and also for regulators."