New Power

Is the UK's energy industry waking up to the threats to cybersecurity?

Cyber attacks and cyber crime are on the increase and the energy sector is an important target. How vulnerable is it? Sian Crampsie looked at the scale of the problem and UK and European attempts to tackle it

In October the European Union Agency for Network and Information Security (Enisa) led a day-long simulation designed to test the region's readiness to counter cyber attacks. Billed as the largest ever cybersecurity exercise in Europe, the complex operation involved over 200 organisations from the public and private sectors from 29 countries, generated more than 2000 separate cyber incidents and tested resilience and procedures at a company, national and international level.

The scale of the exercise indicates the growing awareness of the importance of cyber security to protect businesses, assets and critical infrastructure. Enisa reported in 2013 that global web-based attacks had increased by almost one-quarter and the total number of data breaches was 61 per cent higher than in 2012. It also highlighted in its *2013 Threat Landscape Report* that critical infrastructure such as power networks "are still considered as main potential targets of highly capable threat agent groups" but are hard to protect because of their complex nature.

The financial impact of security breaches is also rising; Enisa believes that global losses resulting from cyber crime and espionage amounted to between $300 billion and $1 trillion in 2013.

In the UK, PWC says that the cost of security breaches has nearly doubled since 2013, with the average cost to a large business of its worst security breach of the year now standing at between £600,000 and £1.15 million.

The type of attack and threat agent varies considerably, says Enisa, from inadvertent security breaches by employees to targeted phishing attacks, code injection and botnets by nation states, cyber terrorists and hacktivists intent on causing some level of disruption, accessing data or espionage. Countering such threats is a huge challenge, and the extent and effectiveness of organisations' cybersecurity strategies varies considerably.

"There's a huge range of maturity amongst differ-

ent organisations in terms of their awareness and their response and similarly there's a huge range of motivations and types and severity of attack," says Andrew Rogoyski, UK vice president and head of cybersecurity services at CGI.

Concern in the energy sector Rogoyski believes that so far the energy sector has not attracted targeted attacks by some of the cyber criminal fraternity that other market sectors have. However energy companies – especially those involved in more contentious forms of energy such as shale gas or nuclear – are becoming increasingly concerned about security breaches and their potential impact.

"Energy companies inadvertently installed malware when downloading software updates on computers running industrial control equipment, giving Dragonfly a route into organisations' networks as well as the means to mount sabotage operations"

Security firm Symantec observed an average of 74 targeted cyber attacks per day globally between July 2012 and June 2013, and says that the energy sector accounted for 16 per cent of attacks.

The vulnerability of the energy sector was illustrated earlier this year when a group of attackers known as Dragonfly managed to compromise a number of oil, gas and electricity firms in the USA and Europe by infecting the software of a number of industrial control system (ICS) equipment providers. Energy companies inadvertently installed the malware when downloading software updates on computers running ICS equipment, giving Dragonfly a route into organisations' networks as well as the means to mount sabotage operations.

The attack followed in the footsteps of Stuxnet, the first known major campaign that targeted industrial control systems. While Stuxnet was targeted at the Iranian nuclear programme, and it had sabotage as its primary goal, Dragonfly had a much broader focus, says Symantec. Dragonfly had espionage and persistent access as its main objective.

According to CGI, the ability of cyber attackers such as Dragonfly to interfere with ICS equipment has become a major concern in the energy sector. The equipment is prevalent throughout the value chain in power plants, networks and distribution systems and is used to monitor and control remote equipment.

"There is quite a lot of concern about how vulnerable industrial control systems are because essentially they are relatively simple systems that have been there for years and years," says Rogoyski. "They become vulnerable when they are connected to an internet point that allows them to be controlled remotely."

Manufacturers of ICS equipment are now starting to improve the security of new devices. A legacy problem exists in the industry because it is not cost-effective to upgrade control systems already in place, and at the same time there is a continuing need for utilities to connect ICS such as Scada (supervisory control and data acquisition) systems to the internet to make them easier to control remotely, even if there is no built-in security.

"As you move down into the distribution networks it is only now that we are starting to see greater degrees of connectivity... and that's opening up potential new attack channels," says Richard Hampshire, principal consultant at CGI.

"Many ICS devices in place in the energy sector were installed long before cybersecurity was a concern and until now companies have relied on the existence of an "air gap" isolating them from other IT networks to protect them from infection."

Many ICS devices in place in the energy sector were installed long before cybersecurity was a concern and until now companies have relied on the existence of an "air gap" isolating them from other IT networks to protect them from infection.

However the increasing use of the internet to control equipment remotely is diminishing the air gap, and even when protocols still exist to isolate Scada and distributed control systems, there is a risk of "cross-contamination" from back office functions.

The danger of 'cross contamination' This highlights the dangers of other types of attack such as phishing and spam, some of which can be targeted at specific employees by masquerading as communications from the human resource department, for example. An en- >

Sian Crampsie is a freelance journalist

gineer may unknowingly contaminate the company's IT network and then access the Scada system, which then becomes infected.

But as Rogoyski points out, hackers can cause just as much disruption to an organisation by interfering with its email or back office systems as they can by infecting operational assets such as networks or generators. "There are many ways of disrupting an organisation these days," he notes. "It gives [companies] a broader range of things to cover."

It also means that suppliers and other business partners need to employ the same security standards to prevent infection. Hackers will often use small businesses as a means of entry to larger enterprises through the supply chain, according to Symantec

One factor that the energy sector does have in its favour is that the physical assets are designed to fail safe. "Operational systems tend to be less accessible on line for historical reasons and there are a lot of safety overlays that tend to protect them from a security point of view," says Hampshire.

"Hackers can cause just as much disruption to an organisation by interfering with its email or back office systems as it can by infecting operational assets such as networks or generators."

This means that the risk of a widespread blackout caused by a cyber attack is low, although CGI believes >

Cybersecurity and the smart grid

The emergence of smart grid technology represents a major shift change for the electricity sector, digitising traditionally isolated energy network control systems and connecting operational networks and IT systems, with benefits for both utilities and consumers alike.

Millions of smart meters are being installed around the world alongside other IT-based components designed to generate, process and communicate data across the grid. Their presence will help utility companies to measure energy consumption more accurately, offer customers new products, and improve the operation and efficiency of their networks.

However with these benefits come new challenges. Enisa says that key vulnerabilities of the smart grid include issues of customer security, physical security, implicit trust between components, teams with different skills and competencies and the involvement of multiple stakeholders.

In addition, through the use of wireless communications, components might be vulnerable to specific targeted threats. For example, AMI (advanced metering infrastructure) components could be manipulated by users in order to perform fraud.

According to Symantec, utilities must also be prepared to address privacy concerns surrounding personally identifiable information, as well as be able to securely store the vastly increased amounts of data generated by smart devices. There will also be a need for cultural change, as security risk in operational technologies such as Scada is traditionally managed very differently from that in enterprise IT. With smart grids, these two systems will increasingly merge and the fragmented ownership risk across the internal organization will need unification.

Enisa notes in a December 2013 report on smart grid cyber security that the development of both smart grid infrastructure and smart grid security are at an early stage of maturity. Because smart grids infrastructures have generally not been operational for a very long time, experience with security issues has not been widely gained nor analysed. In addition, security issues and assessments are managed confidentially and have not been shared industry-wide.

Publicly-available information on smart grid security issues therefore originates mainly from research and generic assumptions, and the standardization activities that are important for security are based on this work.

Global security standards for smart grid components such as AMI are still in their infancy, according to Symantec. Germany has taken a lead with the definition of mandatory security profiles for smart meter gateways to restrict the electronic metering and transmission of personally identifiable information to service providers in the smart grid 'ecosystem'. This initiative is likely to have an impact on other countries in the EU, where regulators are closely watching developments.

Cabinet Office summit presses companies to share information

The UK goverment hosted a cybersecurity summit on 5 November for a dozen insurers aimed at improving and extending the insurance available to cover cybersecurity.

Also on the agenda was initiatives that would see more data about cyberattacks shared, because at the moment security concerns have meant little information about the extent and natire of attacks is shared. "The key issue here is data," Mark Weil, chief executive, UK and Ireland, at insurance brokers Marsh told the Financial Times. "By pooling data we can start to at least see what's going on. Right now I don't think we can even see, holistically, how bad it is."

A working group will report back to the Cabinet Office in April 2015 on topics including the role of the insurance industry in reducing the impact of cyber attack on critical national infrastructure.

that this might change in the future as there is increased investment in new systems and technologies that are network-enabled and increase connectivity. The World Economic Forum estimates that there is a ten per cent likelihood of a major critical information infrastructure breakdown in the coming decade, and says such a breakdown could cause damages of $250 billion.

The cost of defence While successful cyber attacks rarely result in damage or harm to physical assets such as generators, the costs associated with such breaches are escalating. According to the UK government, 81% of large corporations and 60% of small businesses reported a cyber breach in 2013, while Symantec estimates that cyber crime victims worldwide lose around €290 billion each year.

Costs are incurred through downtime, correcting internal systems, communicating with customers and suppliers, and even legal fees. Firms also have to consider the damage done to their reputation should an attack affect their customers.

"Insurance is likely to cover only data breaches and the cost of investigations, and growing awareness of cybersecurity is forcing firms to seek more comprehensive policies"

In the case of sophisticated attacks such as Dragonfly that are designed to remain undiscovered, companies may need to carry out extensive forensic investigations to track down complex and sophisticated pieces of malware lurking on their systems, something for which specialist help is often required.

The rising costs – together with government interest in tackling cybersecurity issues in key sectors such as energy – is driving a new insurance market.

A survey carried out by PWC for the UK government found that 52% of large organisations have insurance that would cover them in the event of a breach. However, such policies are likely to cover only data breaches and the cost of investigations, and growing awareness of cybersecurity is forcing firms to seek more comprehensive policies.

"Insurance firms were seeing a large increase in demand for cyberattack policies from the energy sector, but they were turning down contracts because firms' security defences are too weak"

The BBC reported earlier this year that insurance firms were seeing a large increase in demand for cyber attack policies from the energy sector, but that they were turning down contracts because firms' security defences are too weak. In October Tom Ridge, the former US homeland security chief, announced plans to partner with five leading Lloyd's syndicates to provide "a new and innovative cyber insurance solution".

Such developments indicate that insurance firms see cybersecurity as a new business opportunity and several are starting to offer new products and write new risk, following in the footsteps of the USA, where the cybersecurity insurance market is more developed because of regulations requiring firms to report breaches.

In addition to insuring against cyber attacks, US insurers are also offering clients services such as digital forensics support and legal advice in the event of a breach, as well as risk assessments to determine the vulnerabilities in their systems. Such products will also become available in Europe over the next few years as the market matures and regulations sur-

rounding breach reporting come into force.

The emergence of insurance has been a good stimulus to improve awareness and response in the energy sector. “It changes the way people think about security,” says Rogoyski. “Instead of just being a technical issue, it starts to cross the desk of the chief financial officer or CEO ... and that increases the awareness and sensitisation of organisations".

Raising awareness of the importance of cybersecurity in sectors such as power, gas and water is also a key objective of governments in Europe.

In the UK, the 2011 National Security Strategy categorised cyberattacks as a tier one threat to national security alongside international terrorism, and the government launched a National Cyber Security Programme to strengthen UK cyber capacity. The initiative includes the creation of a National Cyber Crime Unit, the provision of cyber security advice to businesses, the formation of a Cyber Security Information Sharing Partnership and the creation of a single reporting system for financially motivated cyber crime.

In 2013 the European Commission published a cybersecurity package setting out ways of preventing and responding to disruptions, including a proposed directive on network and information security (NIS). It also opened a new European Cybercrime Centre (EC3) in the Hague.

The NIS directive would require all member states, key internet enablers and critical infrastructure operators, and operators in energy, transport, banking and healthcare services to ensure a secure and trustworthy digital environment. It would also create a cooperation mechanism to share early warnings on risks and incidents and require operators of critical infrastructure to adopt risk management practices and report major security incidents on their core services. NP

Links

European Cybercrime Centre

Enisa

UK National Cybercrime Unit

European resilisence and cybercrime centre

Joint Cabinet Office/insurance industry statement