



First Pharmas, now Farmers Targeted by Animal Rights Extremists

Animal rights extremists are targeting farmers at a rate of one incident every nine days, according to the Sunday Telegraph, raising fears that they are widening their scope.

The number of incidents could be higher, it is thought, as not all are reported to police.

The development comes after police success in curbing attacks on animal research companies, such as Huntingdon Life Sciences, Europe's largest contract medical testing centre, and companies involved in the construction of a £20 million research centre at Oxford University.

In one incident, extremists caused £250,000 of damage to lorries in a firebomb attack on a farming business in Oxfordshire.

The Animal Liberation Front claimed it had used sophisticated electronic devices to detonate the bombs remotely and dedicated the attack to the memory of Barry Horne, the activist who died in jail in 2001 after a hunger strike.

Other incidents have involved white powder being sent to farmers, break-ins to farms, and threatening phone calls and emails.

The farm attacks warning has come from the National Extremism Tactical Coordination Unit (NETCU), a police unit set up to combat animal rights activists.

Supt Steve Pearl, the head of NETCU, said those attacked have been predominantly involved in intensive poultry farming.

"You will always have people who object

to the use of animals in farming and take direct action. People do fear they are going to be targeted and we are trying to reassure them," he said.

More than two thirds of the unit's work relates to attacks on animal testing companies, but 18 per cent now concerns the farming industry, including businesses selling foie gras, as well as other companies, including circuses that keep captive animals.

The National Farmers' Union has urged members to report incidents to police. Matt Davies, from the union, said: "Mostly, it is intimidation tactics and harassment by telephone. Lives have been affected by this extremism.

"It is regrettable that individuals see fit to terrify people in their own homes. Farmers do a humane job to the best of their abilities."

Farms run by Bernard Matthews, the turkey farmer at the centre of a bird flu outbreak earlier this year, have also been targeted.

At the height of the scare, in February, at least two letters containing a powder were sent to one of his properties. An employee had to have medical attention when her hands started swelling after she touched one letter.

A full report on the recent NETCU 2007 National Stakeholders Meeting will appear in the next issue of Security Now.

For further information on the above or for any other security issues contact Agenda on 08456 44 55 46 or info@agenda-security.co.uk

IN THIS ISSUE

First Pharmas, now Farmers Targeted by Animal Rights Extremists

The Fraud Act 2006

Agenda Achieves CTP Accolade

Is your Wireless Internet Connection safe from Hackers?

Are You Playing With Fire

Lazy about Laptop Security

Countdown to Destruction

Concerned about Animal Rights Extremism?

Letter to the Editor ...

If you have any areas of interest or a particular subject you would like to read about in future issues of Security Now, please e-mail details to

info@agenda-security.co.uk

Countdown to Destruction



We're all familiar with scare stories of worms, virus attacks, Trojans and the like. We need look no further than the 'I Love You' worm, 'Code Red' or 'Slammer' to see the massive impact these malicious pieces of software can have on a global scale.

They are made possible by security flaws in software products, often associated with Microsoft Windows. These flaws are commonly due to mistakes by programmers who fail to consider the security implications of the code they write. This is often out of consideration of the user's experience rather than the user's security. Hackers have ways of discovering these programming errors and writing software of their own, known as exploits, which can take advantage of the software vulnerabilities and give them the ability to take control over computer systems.

In the past, you will have read articles that give advice on applying

the latest software patches which are issued to fix the programming mistakes that lead to security vulnerabilities. The old mantra is as important now as it was last year. Keep your security up to date or else a hacker is going to design an exploit that can be used against a vulnerability in your system.

However, the playing field has been evolving over the years and the way in which exploits are created has changed dramatically. In the past, there used to be a time delay between details of a vulnerability being announced and hackers creating exploits to take advantage of it. Nowadays, there is an increasing trend towards the precise opposite situation. Exploits are being found in the wild, sometimes on compromised systems, that nobody knew about. In other words, hackers are creating exploits for vulnerabilities that nobody else knew existed. These exploits are known as 'zero days' (or 'Odays'), so called because there are 0 days between a vulnerability being announced and an exploit being released.

An even more worrying trend is for a vendor, for example Microsoft, to announce a series of security patches and on the same day hackers will be able to discover what problems the patches fix, and then release an exploit for those problems before many administrators have been able to apply the patches.

As you can imagine, such attacks are difficult to defend against. There are best practices that can be followed, security products that can actively monitor for 'Odays' and services such as security reviews that can highlight areas of weakness in corporate IT defences. A combination of these measures can help ensure that your organisation is not the next victim of a 'Oday' attack.

Contact info@agenda-security.co.uk for further information or call us on 08456 44 55 46.

IN BRIEF

Lazy about laptop security

According to data encryption specialist, SafeBoot, 29 million workers in the UK are "walking security hazards".

Their survey found that although half of the respondents had security on their laptop, most had no idea how to use it or had found it so complicated that they hadn't bothered to learn any more about it.

Nearly one-quarter of those asked had lost their laptop or had it stolen and over 25% said they did not see the point of shredding documents.

Did you know?

- On-line banking fraud rose by 44% in 2006 compared with 2005 (source: APACS)
- 10,000 mobile phones are reported stolen every month in the UK alone. (Source: Met Police)
- In 2004 it took 20 minutes for an unprotected computer connected to the Internet to be infected. It now takes 60 seconds! (Source: EMEA)

Don't let it happen to you!

Are You Playing With Fire?



The Regulatory Reform (Fire Safety) Order became law in 2006, but many companies are either not aware of the changes or are choosing not to take the appropriate action required to ensure they comply with the legislation.

Is this due to ignorance of the safety aspects relating to the place of employment and the employees - or is it due to a lack of understanding of the changes?

Either way, ignorance is no excuse. If you haven't acted yet, don't wait until it is too late. You may find yourself answering questions to the local authorities or H&S Inspectors for failure to implement the necessary changes - or worse still, defending your actions in a court of law due to a fire accident. Better to be safe than sorry. Act now! Seek advice or training from stevem@agenda-security.co.uk or contact us on 08456 44 55 46.

Is Your Wireless Internet Connection Safe From Hackers?

They hunch over laptops in their cars on neighbourhood streets, tapping into other people's wireless broadband connections for some free time online, and are fast becoming criminals of the internet age.

Wi-Fi theft leaves no fingerprints and keeps its distance, but thousands are at risk because they don't adequately password protect their wireless accounts.

Using the strong broadband signal of the neighbours may seem relatively harmless but it can now result in a criminal record. In the past month or so, two people have been arrested for using other people's wireless connections without permission in Worcestershire, in what are believed to be among the first cases of their kind. A man was spotted by residents using a laptop while parked in his car outside a house in Redditch. In an unconnected incident, a 29-year-old woman was arrested following a similar incident, also in Redditch, earlier in the month.

They received a caution for dishonestly obtaining electronic communication services with intent to avoid payment.

PC Tony Humphreys, from West Mercia police, said: "Wireless networks don't stop at the walls of your home - without the necessary protection, neighbours or people in the road may be able to connect to your network. This might slow down your service,

or more importantly, your connection could be used for unlawful purposes." Most wireless networks are unsecured when first set up, but can be configured to stop unauthorised users accessing them.

It is advisable to check your connections. Unscrupulous people could be accessing your connection to download obscene material or even steal your identity.



Agenda Achieves CTP Accolade

Agenda is pleased to announce that it has been granted 'Preferred Supplier' status to the Career Transition Partnership (CTP), the MOD tri-service resettlement training provider for armed forces personnel leaving the services and entering civilian employment.

Agenda has gone through a vigorous selection process to assess their suitability for providing training in both SIA licensing areas (Guarding and Door Supervision) and for the training of future security managers to the standards of the Institute of Leadership and Management.

Last year around 7,000 personnel from all three services left to pursue a new career as a security professional. Agenda can draw from a wealth of experience, not only in security training, but also in a variety of fields in the security industry.

The CTP run the ISO 9001 Quality Management system for all personnel entering the resettlement programme and insist on a 'fit for purpose' approach to accrediting companies to Preferred Supplier status. The Agenda team will draw on their own experience of ISO 9001, Safe Contractor and other accreditations to provide not only the training but also the administration and running of the courses.

Measuring the successful outcomes of training is very important to the CTP and Agenda. That is why all courses run by Agenda have a Training Evaluation process in place that is part of the QA process for all our services. This ensures that the trainees receive the appropriate level of training and the delivery is kept to the high standard required by the examining authorities and the CTP.

Agenda is looking forward to working with the CTP and welcoming all students who wish to gain the best training and qualifications to give them the best-possible platform for success in a new career.

For further information speak to Steve on 08456 44 55 46 or email stevem@agenda-security.co.uk

The Fraud Act 2006

New legislation is now in place to combat the rising cost of fraud

A new independent study* into the nature, extent and economic impact of fraud has found that fraud costs the UK economy a minimum of £13.9 billion a year, increasing to £20 billion when estimates for income tax and EU fraud are added.

This amounts to £330 for every man, woman and child in the country! That, of course, includes you and me and we have to foot the bill. In an attempt to stem this escalating crime the Government has brought in new legislation.

The Fraud Act 2006 came into effect on 15 January 2007 and creates a new general offence of fraud in three key areas:

- Fraud by false representation
- Fraud by failing to disclose information, and
- Fraud by abuse of position

It also creates new offences:

- Obtaining services dishonestly
- Possessing, making and supplying articles for use in frauds
- Fraudulent trading applicable to non-corporate traders.

Schedule 1 of the act repeals various offences including:

- Theft Act 1968 section 16 (obtaining pecuniary advantage by deception);

This section was available for use by employers to dismiss an employee who had provided false information (in their CV, qualifications etc) to gain employment or promotion. This area is now covered by Section 2 of the new legislation.

Section 2 makes it an offence to commit fraud by false representation which must be made dishonestly. A clear distinction from previous legislation that now enables the fraud to be committed against a 'machine'.

**The report, commissioned by the Association of Chief Police Officers' Economic Crime Portfolio Group, was compiled by Morgan Harris Burrows LLP in association with Professor Mike Levi of Cardiff University. The full report is available to download from the ACPO website.*

Concerned About Animal Rights Extremism?

The animal rights movement has been dealt several blows in recent times, high profile cases and long sentences appear to have deterred some of the more radical activists. At least on the surface we are seeing a reduction in direct action and particularly with respect to those actions now identified under the SOCA Act such as Home Visits. We must not be complacent though and understand that the animal rights extremist movement leaders will never change their views and activities against research institutions and anybody remotely attached to them will continue.

We have seen an increase in information leaks, in cybercrime and in attacks on research institutions in main land Europe. In the USA there have been new laws implemented (AETA) and heavy sentences imposed on SHAC supporters in particular but there continues to be acts carried out against research facilities, their employees and their suppliers. Agenda Security Services believe that the tighter legal constraints will lead to more infiltrations and in particular short term temporary infiltrations through agencies and suppliers to research institutions.

The Human Resources, Accounts or Archives departments are as vulnerable to infiltration or information being socially engineered out of the company as much as the more sensitive areas are. Creating a security aware culture to reduce the threats and training people to stop employing infiltrators in the first place should be an operational imperative for those involved directly or indirectly in research. Simple processes can be put in place to reduce the possibility of data loss and thwart social engineering attempts.

Agenda Security Services has been training research institutions and suppliers to the industry in just these types of techniques for many years now. In excess of 3500 people have been trained worldwide including recent sessions in the USA, Canada, Germany and of course the UK. The more security aware we are the more secure we all become. Don't be complacent, contact Agenda today to find out how our enjoyable and memorable courses can make you a tougher target!

For more information contact norman@agenda-security.co.uk.

PREFER AN ELECTRONIC COPY OF SECURITY NOW?

We are getting more and more requests to send out an electronic version of Security Now rather than a paper based copy. If you would prefer to receive an electronic version of the newsletter please forward your e-mail address to clarew@agenda-security.co.uk and type "Security Now PDF" in the subject of the e-mail and we will arrange for you to receive future copies electronically.



Offices in Cambridge and Hull
Tel: 08456 445546 Fax: 08456 445547
Int Tel: +44 (0) 1964 671791
E-mail: info@agenda-security.co.uk
Web: www.agenda-security.co.uk



ISO / IEC
27001 : 2005