

CASE STUDY

At Missing People no virus gets missed

Missing People is the UK's only charity that works with young runaways, missing and unidentified people, their families and others who care for them.

As part of its activities, the charity regularly publishes a number of e-mail addresses in public domains such as their websites. This initially resulted in an estimated 100,000 e-mails received every day, of which the vast majority are unsolicited commercial e-mail or spam. Missing People realised that adequate protection was therefore essential to mitigate the risks posed to IT systems by all varieties of malicious code, and to minimise staff's exposure to unpleasant content.

According to Tim Beaman, Head of Information and Communication Technology at Missing People, a high proportion of incoming e-mail used to be spam or potentially contained viruses. Since the charity implemented Trend Micro ScanMail's, Tim Beaman noticed that 99% of unwanted messages were being blocked. "The advanced heuristic scanning embedded in Trend Micro's ScanMail's software, its spam blacklisting and enterprise content filtering facilities, make the software invaluable to our organisation."

Trend Micro's solutions also protect a total of five servers and up to 125 computers in the charity. "We have also kept our Servers virus free with Trend Micro's Server Protect, enabling us to protect files, scan incoming and outgoing mail to user PCs that are protected against malware."

"Without Trend Micro's software Missing People would lack the essential tools to fight these threats and our mission of staying virus-free and operating as professionally as we do today, would be impossible to achieve," comments Tim Beaman.

www.missingpeople.org.uk



Playing with fire

Companies are increasingly focused on risk management, but often fail to take on board the need to rehearse the very crisis they are preparing for. Dominic Cockram, CEO, Steelhenge Consulting Ltd, explains

In a world increasingly obsessed with eliminating risk to individuals, businesses and public organisations today face a widening range of threats; are they really prepared for them?

Planning, training and exercising are the three parts of an organisation's resilience strategy that are now, from a risk-management perspective, absolutely non-negotiable.

The rising risk environment is well documented, and 'risk assessments' are now the prerequisite of every activity. But their very ubiquity obscures, and even exacerbates, the real problem for organisations. Assessing risk may absolve you from theoretical or legal responsibility when things go wrong; it doesn't do anything to ensure you can put them right. Consequently in recent years and largely driven by the flaky reliability of IT-driven systems, the concept of 'business continuity' has developed into a

detailed planning process, with a degree of committed corporate focus. However, as with risk assessment, business continuity planning is still often seen as a 'tick in the box', rather than a genuine guarantee of future corporate health.

Integration is the first casualty. As soon as business continuity is hived off as a separate responsibility, rather than becoming part of every manager's role, it is already 'planning to fail'.

The second challenge to an organisation's resilience is a lack of trained capability. Training is often either woefully inadequate or entirely absent from the risk-management environment.

Plans are devised that require a lot of people responding precisely, with appropriate skills and knowledge, at the right time, to handle a crisis and guarantee the future of the organisation. Yet the attitude to training is often akin to sending a football team into an

FA Cup Final after having just sat them in a room for an hour and drawn some set-piece moves on a blackboard. The development of staff capabilities in crisis needs serious attention.

Training makes skills, only practice makes perfect. For every individual that's a truism; for a team, under pressure, it's fundamental. You have to exercise to complete the circle. Yet design and delivery of effective exercises is an art and rarely a core organisational management skill.

There are now specialists, like Steelhenge, who are able to deliver the whole three-part programme, or – if planning and training resources are in place – deliver the all-important 'practical'. Effective testing of plans through well designed and executed exercises is essential.

To really protect your business, systems, people, reputation and data you need to be rehearsed. ▶

Software engineering at the University of Oxford

Not just a city of dreaming spires, Oxford is now the place to go for software nous

The Software Engineering Programme at the University of Oxford is a programme of advanced education and applied research, offering access to the combined expertise and resources of the Oxford University Computing Laboratory and the Department for Continuing Education. The Programme has been supported by the Engineering and Physical Sciences Research Council since 1992.

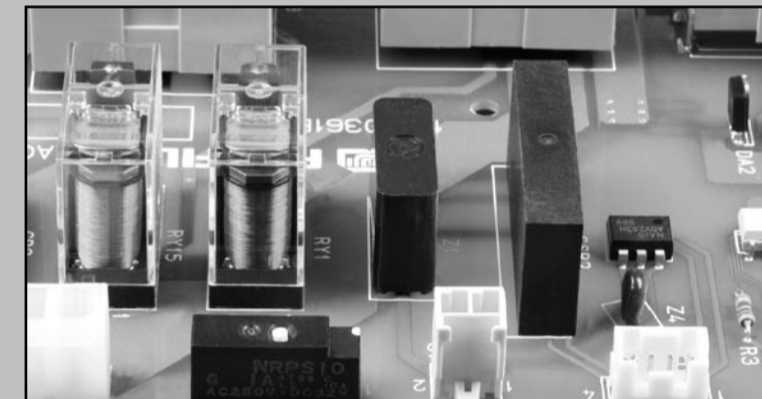
The Programme offers opportunities for part-time study, with courses in key areas such as object technology, software architecture, computer security, precise modelling, and development processes. There is also the possibility to take some of the courses from the Oxford Bioinformatics Programme, in areas such as algorithm design, data mining and systems biology.

Each course is delivered by an expert in the subject, and includes an intense teaching week of classes, practicals, and group work; class sizes are kept small

to facilitate interaction and to promote learning. Courses are usually taught in Oxford, but can be delivered in-house by arrangement.

These courses may be used as credit towards postgraduate qualifications — at Certificate, Diploma and Masters' level — from the University of Oxford. These qualifications are open to those with an appropriate combination of academic and industrial experience; a first degree in computer science or software engineering is welcome, but not necessary.

The Programme is also a centre for research activity; a 50-strong research group in software engineering is involved in a number of national and international projects in areas such as digital mammography, cancer clinical trials informatics, distributed computing for climate prediction, languages and tools for object model transformation, virtual research environments, and model-driven software engineering. ▶



How to stay safe online

The internet and email offer wonderful opportunities for business, but they can also be a potential source of problems. Here is how to get protection

For a considerable slice of humanity, the Internet has revolutionised the way we work, play, communicate and generally interact with each other. Just in the world of business, companies great and small can now find customers, suppliers and partners in countries where they may have no physical presence, just on the strength of their website.

Australian IT security developer Tier-3 is a case in point. Founded in 1999, it got its first international customer on the other side of the world, in the UK security sector, thanks to someone coming across its website and contacting the company, recalls co-founder and chief technology officer Geoff Sweeney. "We launched our first product in 2001, and shortly afterwards we got our first customer in the UK government via an Internet search," he recalls.

Yet the other side of the coin is that, where there is opportunity, there is also risk. Both the Internet and email are potential sources of problems, from viruses in emails, through websites that stealthily plant software on a computer to use it for their own purposes, unbeknown to the user, to others that may distract employees from their work or even, in the case of inappropriate content, cause them distress and potentially lead to litigation, if they were viewed in the course of a work-related search.

To address these issues, there is a range of products in the market for filtering traffic coming onto a company's network from the Internet. Because email uses a different protocol, i.e. a different set of rules for how information is formatted for communication, from regular Internet traffic, there are dedicated products that sit at the point where a company's network joins the public Internet (often referred to as the gateway). Companies like Secure Computing and IronPort (which has just been acquired by the networking giant Cisco) offer filtering devices for enterprises, while in the small and medium-sized business arena there are others such as Barracuda.



However, that is only the email side of the problem. There is also a need to filter Web content, and in that context, there are a number of companies in the market, with the two biggest, Websense from the US and Surfcontrol from the UK, about to become one, since Websense is buying Surfcontrol.

These companies look at the Web addresses of sites, known as URLs, that employees are requesting access to and compare them with so-called real-time blacklists. They can then block those sites and/or advise network administrators that someone was trying to access them.

Sites get on the blacklists because they have been found to be the source of malicious content such as Trojans, i.e. the software that downloads surreptitiously and is used either to launch attacks from the unwitting user's computer, or to gather information about the user's surfing habits.

The URLs of known pornographic sites or others that might cause offence are also on these lists.

Some companies offer filtering not as a piece of soft- or hardware that a customer has to buy, but as a service. Trend Micro, one of the largest developers of anti-virus software for scanning email traffic, argues that the rate at which malicious software, or malware for short, alters its profile to evade detection is too fast.

"Baseline security techniques like pattern matching, and even heuristics, can't keep up," says Raimund Genes, its CTO of anti-malware, and for this reason Trend has just launched Total Web Threat Protection, which is just such a service.

It works by picking up a request to access a URL, then puts in a parallel request to a server farm operated by Trend, which replies with information about that address. "We can block known malicious sites, suspicious sites and the addresses of known bots, or we can block only the known malicious, which would be the 'Low' security setting," said Genes. "We can warn the user and the admin when a site is suspicious, then block access to it if that is the customer's policy." ▶

Transparent Full Hard Disk Encryption

Strong Pre-Boot Authentication

Policy-Based Port Management

Comprehensive Management of All PCs and Mobile Devices

Complete data security made easy with Pointsec products from Check Point

All laptops, handhelds and removable media devices should be encrypted, helping you feel confident that you have done everything you can to stop security breaches on mobile devices. Pointsec products from Check Point provide easy-to-manage and flexible solutions where it really matters – from full disk and removable media encryption to inbound and outbound data protection.

For more information please go to www.checkpoint.com/products/

Check Point
SOFTWARE TECHNOLOGIES LTD.

—puresecurity™—