

# IT SECURITY

SPECIAL 5-PAGE REPORT

## Online security for the masses

An alarming rise in malware threats is creating serious risks for Irish businesses, writes **Dermot Corrigan**

**T**he number of viruses and malware threatening Irish businesses is growing at an alarming rate, according to Dermot Hayden, Sophos' sales manager for Ireland. Hayden said these threats were a serious risk to the IT infrastructure and applications on which many businesses relied.

"There has been a huge increase in threats over the last few years. Sophos' labs are now seeing 150,000 new pieces of malware every day, which is one unique new malware file every 0.9 seconds each day of the year. There has been alarming growth from 50,000 per day in 2009 and 95,000 per day in 2010."

Hayden said many of these threats could be picked up while browsing websites that appeared to be perfectly safe. "A large proportion of the threats are web-based and most are spread through legitimate websites, so you do not need to go to disreputable sites to get infected," he said.

"The trends are towards large increases in the use of so-

cial engineering and social media, fake anti-virus products and internet marketing techniques. E-mail hosted threats, although not new, are still a major threat vector."

### Solutions

With these threats evolving so quickly, vendors had recently decided to take a more proactive approach to neutralising them, said Hayden.

"In the past security vendors were able to issue updates which dealt with threats they had already seen," he said. "Clearly, when you are getting 150,000 new threats a day it is impossible to be reactive. You have to be proactive and be prepared in advance."

Hayden said this had led to the development of 'heuristic' intelligent systems such as Sophos' Host Intrusion Prevention System [HIPS].

"Instead of looking for a piece of malware which has been found previously and a solution to it developed, HIPS looks for traits in any software code it comes across to see if it bears any resemblance to

something it has seen before," he said.

"It might have the fingerprints of a particular malware code writer, or it might ask the machine to do something unusual such as connecting to a server in Nigeria. You need a system in place to detect that sort of activity."

These intelligent systems tended to be made up of a number of different complementary elements, said Hayden.

"Web scanning in endpoint security keeps users safe while not on the secure corporate network, and the tie-up between web and endpoint will develop further," he said.

"Network Access Control [NAC] has always been necessary, but was often overlooked by companies that might have felt it was too complex or difficult to implement. It is now becoming a mandatory requirement to create a secure environment."

Data loss prevention technologies are also now a mandatory requirement in any endpoint security solution."

With mobile internet use so widespread now in many Ir-



Dermot Hayden, Sophos' sales manager for Ireland

SUSAN JEFFERIES

### About Sophos

Established in 1985, Sophos employs 1,800 staff globally and is headquartered in Boston, US and Oxford, Britain. More than 100 million users in 150 countries use Sophos solutions as protection against complex threats and data loss.

The company had been serving Irish-based organisations for over 20 years in cooperation with local distribution

partner Renaissance and a network of resellers on the ground, Hayden said.

"We have over 50 reseller partners in the Republic and sell to all industry sectors. Our 'sweet spot' is the ten to 5,000 user segment, as our products are ideally suited to companies without large and expensive standalone IT security teams," he said.

Customers could choose the support relationship which best suited their own company

requirements, said Hayden. "Customers would purchase a solution from the reseller partner and we supply the solution. The customer then can decide whether to contact the reseller, Renaissance or our 24/7 service for ongoing support," he said.

Hayden said that, unlike some IT applications which moved forward through periodic new releases, security products needed to be updated constantly. "Unlike other IT

solutions which will only ever change slightly over time, such as Microsoft software for example, the dynamic nature of security threats means that our products are being updated daily to keep our customers protected," he said.

"This means we need to be close to our customers ever-evolving needs – customers are looking for more intelligent, integrated, simple to use security solutions across endpoint, mobile and gateway."

www.pwc.com/ie

### The bad guys

The image of the computer hacker as a rebellious teenager looking for attention is out of date, according to Dermot Hayden.

"In the past malware or viruses came from clever but ill-advised adolescents who wanted notoriety," said Hayden.

"You knew then you had a virus as the cursor moved across your screen deleting your words and then your files disappeared."

"That is long gone; it is now about very highly organised criminal gangs, largely South American, Russian or Chinese, stealing data for financial gain. The other difference is they do it

in a way which you do not know."

Hayden said that, these days, malware was designed with the express purposes of stealing valuable and sensitive information on companies and individuals.

"It is really data that these people are after. That might be information on an individual to enable them to get into their bank account and steal money from them," he said.

"It might also be intellectual property from a company which the criminals can use for financial gain. They are always looking to get new types of data and thinking of how they can use that to turn a profit."

Hayden said these gangs could find ways to make use of even information which at first glance might not seem valuable to them.

"We saw an example recently where a criminal gang managed to access a hospital's data systems and extract a list of terminally ill patients," he said.

"That data was passed to another group who put together a written letter campaign to each person on the list advising them of a particular cure being developed and saying they could be involved in the early testing. The criminals managed to extract a lot of money that way."

## The Integrity to expand in tough times

By Linda Daly

**S**ecurity specialist Integrity Solutions is expanding with the creation of five new positions at its Dublin office. The company also expects staff numbers at its London office to rise from three to ten in the coming year.

Eoin Goulding, Integrity's managing director, said the company had undergone steady growth since launching in 2005. Its revenues for 2009 rose by 65 per cent to top €7.5 million and Goulding said he expected turnover for 2010 to come in at about €8 million.

Established in 2005, Integrity Solutions provides a range of security services, including analysis, policy design and integration, IT security audits, authentication, regulatory compliance and full-managed security services.

Its workforce has grown from three to 35 in the past six years. Its approach is to evaluate clients' existing infrastructure and systems, identify gaps and weaknesses in their security systems and then find ways

to help them reduce risks and meet compliance requirements.

Integrity's managed security service is scalable. This means it can be extended to new staff, divisions and activities as and when it is needed. The service includes a 24-hour monitoring, reporting service, which is available seven days a week.

The company uses the IT search and analysis engine Splunk, which allows it to index, search and report on IT data as it happens or historically.

"We mitigate the risks and threats, and provide real-time reports. This allows businesses to free up their resources," said Goulding, adding that this approach reduced the amount of time it took to resolve problems. It feeds us real-time information where we can make changes to the network if needs be, so we basically become the eyes and ears of clients," he said.

Goulding recommended that cash-strapped companies take a proactive approach to protecting themselves against potentially damaging and disruptive IT risks.

"Often times, companies have the solutions there, but



Eoin Goulding

cards. On the other hand, they can accidentally put a virus on the system from their home computer or mobile device such as a USB key," he said.

Data breaches are becoming increasingly common as more firms use mobile devices. "Something as simple as losing a device can lead to huge costs," he said.

Goulding warned companies to ensure the necessary security measures were in place before buying into 'cloud' packages that delivered software as a paid-for service over the web. By not doing so, he said unsuspecting companies could face massive IT security risks.

By implementing a managed security, Goulding said companies could benefit from reduced capital expenditure and the cost of paying out for their own IT infrastructure in-house. They could also free up resources by outsourcing and using the services of full-time security experts.

"By outsourcing repetitive security monitoring and protection functions, businesses can have their internal resources focus on the more critical business initiatives," he said.

### Contact:

Kieran Mongan  
Tel: 01 792 8632  
kieran.mongan@ie.pwc.com

Ciarán Kelly  
Tel: 01 792 6408  
ciaran.kelly@ie.pwc.com

Bob Semple  
Tel: 01 792 6434  
bob.semple@ie.pwc.com

**pwc**

## Secure your business

From strategy to delivery, PwC can help you minimise your IT risks and protect you against emerging risks in cybercrime, mobile devices, social media and cloud computing as well as web-related technologies.

## IT SECURITY

## Smart solutions for data protection

A clever strategy can help companies avoid the costly threat of data loss, writes **Linda Daly**

**M**any organisations continue to adopt tactical and costly IT solutions instead of establishing an effective security strategy that can deliver significant cost-savings, a new report from PricewaterhouseCooper (PwC) has found. The firm's CIO and CSO 2012 Global State of Information Security survey reports that just 43 per cent of firms worldwide are implementing effective IT security strategies. Kieran Mongan, leader of information security advisory services at PwC Ireland, said firms must start to protect their IT systems and take IT security seriously.

"There's a large disconnect between IT security and business. A lot of business stakeholders are so focused on the economic downturn and in maintaining their business that they're not providing the necessary support to make security effective," Mongan said.

With companies holding information relating to personal, financial and corporate data and trade secrets, they have a vested interest in keeping information secure.

Nearly 80 per cent of firms

report losing some form of data through IT security breaches. Yet funding of IT security has been at risk in the current environment, with evidence suggesting that certain areas are showing signs of degradation.

For example, the survey of 9,600 senior executives in 138 countries found that expenditure on identity management and business continuity/disaster recovery were down 5 per cent in organisations over the past 12 months. "There is reluctance among management to commit to security funds even at the risk of degrading security further where there isn't a cohesive strategy," said Mongan.

### Data breaches

Typically, data loss could cost anywhere in the region of €10,000 for small firms to €1 million-plus for large corporates, said Mongan. While firms faced regulatory fines if data breaches occurred, typically in Ireland regulators weren't as aggressive in fining organisations as in other parts of the globe, he said.

However, there are non-tangible costs such as the erosion of public confidence in compa-



Kieran Mongan, leader of information security advisory services at PwC Ireland

TONY O'SHEA

nies, the operational costs in managing a security incident and the time it takes to recover systems. Mongan said that firms should allocate 15 to 20 per cent of their IT budget to security.

They can then evaluate their return on investment by defining the key performance indicators, and looking at the number of security incidents prior to adopting security measures.

### Customer demands

While many companies lack a defined security strategy, those that do say customers

are driving the agenda. Fifty per cent of respondents said that client requirements was the top reason for implementing information security systems.

Just 45 per cent listed 'legal and regulatory environment' as the top priority.

"Organisations are recognising they have a new relationship with their customers and many perceive that customers now drive information security," said Mongan.

"Customers have the ability

to be heard around the globe on social networking sites, and can have a significant impact on large institutions in an instant. The rise of client requirement demonstrates the continuing strategic importance and integration of the security department to the business."

### Increased risks

The increase in cyber crime, which Mongan attributed to the economic downturn, is also driving security strategies. "Cyber threats tend to increase during contractions in business cycles. They tend to be more adaptive and more pervasive. When they come they tend to stay with you a lot longer, and have much more intelligence," he said.

As organisations open up their networks to partners and suppliers to allow exchange of information, they are faced with another security threat.

"Their partners and suppliers may not have the cohesive strategy that you may have. You need to be aware of all of the interfaces that you have. You need to understand your information flows."

"You need to understand the type of information that's travelling across your network or that's being stored," said Mongan.

In this instance, service level agreements (SLAs) must be studied and contracts put in place with robust penalty clauses for those who don't have sufficient IT security measures.

"You need to define your security requirements. You need to monitor and scrutinise your third party suppliers and clients. It's important for the external parties to have the same level of monitoring and audit-

ing of activities that you would have internally," said Mongan.

### Emerging technologies

In addition, there are emerging risks associated with the cloud, mobile devices, social media and web-enabled technologies. Strategies that are in place must include emerging technologies and threats, according to Mongan.

In the PwC survey, a dichotomy of views was found when it came to cloud computing. Some 54 per cent of respondents felt their security had improved because they'd made the transition to the cloud whereas 23 per cent said that it had disimproved. "There are key problems with the cloud from a security perspective. Cloud vendors often satisfy themselves as to what security is best for them, rather than their customers," said Mongan.

"Customers need to be more dogmatic and negotiate more," Mongan advised firms again to negotiate and develop proper SLAs that defined clearly from the beginning what the IT security requirements were. "You can outsource the responsibility for control but you cannot outsource accountability," he said.

The proliferation of mobile devices such as smartphones is also increasing risks for firms, as many employees use them without a clear internal policy and end-user agreement.

Forty-three per cent of respondents in the PwC survey have a security strategy for employees' use of personal devices, 37 per cent have a security strategy for mobile devices and 32 per cent have a security strategy for social media.

free from  
security worries



Rits is the premier independent provider of Information Security consulting and professional services in Ireland. Our vendor independence, superior levels of technical excellence and our 'security only' focus differentiate us from other providers.

We provide our clients with unparalleled peace of mind that their systems, business operations and reputational risks are evaluated and minimised by a team of industry leading security professionals.

Our team of specialists can deliver a range of market leading services:

#### Assurance Services:

- Penetration Testing
- Application Security Testing
- Vulnerability Assessment
- Systems Hardening
- PBX Reviews
- Wireless Assessments
- Network Security Reviews
- Database Security Reviews
- Anti Virus Health Checks
- Firewall Rules Review

#### Computer Forensics

#### Consulting:

- Policy & Standards
- ISO27001
- Outsourced Information Security Advisor
- Strategic Planning
- System Design
- PCI Compliance & Audit
- Implementation Management
- Training & Staff Awareness

#### SafetyNet Program

- Subscription based vulnerability assessment service

By Gareth Naughton

**A**s businesses become more dependent on technology for their day-to-day operations, the challenge to make their systems secure continues to grow.

More and more firms are equipping their employees with portable devices such as laptops and smartphones to enable flexible working. Businesses are also utilising consumer technologies such as social networking sites to further their business ends, and empowering their employees to make use of these tools.

These developments have brought with them new threats to their IT security. "We're seeing a huge increase at the moment in hand-held portable devices such as smartphones and laptops," said Robert Lanigan, security software sales, IBM.

"While previously you could draw a circle around the organisation and keep everything inside, with people now walking around with hand-held devices which have got huge stores of information, managing those is becoming an increasing challenge."

Lanigan said a lot of laptops were controlled and managed adequately once they were within the company network. However, in today's working climate, he said they often left the network. You have to make sure the next time they come back on the network the companies' policies and procedures are being enforced," Lanigan said.

Having clear usage policies and procedures for employees was as vital as having the right security technology, he said. With the increasing prevalence of social networking in business, this is true now more than ever.

"Through the use of these social networking technologies – Twitter, for example – information can be very quickly dis-



Robert Lanigan, security software sales, IBM

## Flexible working putting firms at risk

seminated outside an organisation that shouldn't be. Organisations need to have specific policies and procedures in place around how they manage those social networking capabilities."

Lanigan categorised three types of threats to an organisation's IT security: external, internal and reputational. The external threat comprises attacks like phishing and hacking, which have shown an increase in the last couple of years with some high-profile casualties such as Sony.

The internal threat comes from employees accessing systems they shouldn't have access to and getting hands on information they shouldn't be in possession of. The third threat is the one to a company's reputation, which can be impacted negatively by even a small security breach.

### Intrusion prevention

One basic level of security every organisation should have to counter external threats was to ensure they were using firewalls and intrusion prevention and detection software, said Lanigan.

Internally, all the different user endpoints in a company, such as desktops, laptops and

mobile devices, need to have security capabilities like anti-virus and anti-malware software installed. Security patches are a particular problem for organisations at the moment.

"When Microsoft, for example, discovers a vulnerability in its operating system that is being exploited, it needs to get a security patch out to the end user as quickly as possible. You have to do it almost instantaneously. That's a big challenge and a lot of organisations are struggling at the moment with it."

IBM has a team called X-Force, which distributes virtual patches to companies to keep them ahead of anticipated hacking threats. "Our team will create a virtual patch to deal with the vulnerability until Microsoft or whoever releases its security patch."

Of utmost importance is to have clearly demarcated roles and responsibilities for employees in relation to accessing and using IT systems. "You would be quite amazed at the number of organisations that allow people access private information they shouldn't have access to."

Lanigan said making your IT secure needn't be an expensive investment and typically made business processes more efficient.

Rits

Information Security Centre  
2052 Citywest Business Campus  
Co. Dublin

Tel: +353 (0) 1 6420500  
Fax: +353 (0) 1 4660468  
Email: info@ritsgroup.com

# IT SECURITY

## Unified solutions make real sense

Irish IT firm Renaissance has developed security systems to ensure firms are kept safe in cyber space, writes Dermot Corrigan

Last May, Irish IT security solutions and services distributor Renaissance entered a new distribution agreement with Cyberoam, a leading global unified threat management (UTM) vendor.

Such UTM products offer one easy to implement and manage replacement for customers who might previously have had a tangle of different internet security products, according to Michael Conway, director of Renaissance. "Cyberoam is one box which provides people with email filtering, web filtering, VPN [virtual private network] access and also acts as a firewall," said Conway.

"That fits well within organisations which may have an old-style firewall from a few years back, a different email filtering system and so on. Delivering all these functions from one piece of technology brings down the total cost of ownership and meets organisations' security needs much better." Such new generation unified solutions were increasingly popular due to the increasingly sophisticated nature of the IT security challenge facing Irish organisations, said Conway. "Eighty per cent of malware attacks now come through web-browsing. A few years back people were concerned about certain dodgy sites, or a dangerous email attachment," he said.

"Now, commercial or other normal legitimate sites can be susceptible to malware attacks and when you are browsing you can be attacked without realising. Things like key-loggers and trojans can be downloaded automatically. These log the information you type in, such as credit card information, and pass that on to someone else."

**Intelligent solutions**

By implementing newer unified solutions, Conway said companies could phase out older systems that were not geared today's IT security threats.

"A lot of organisations first put in web-filtering solutions some years ago. A lot of these were based on simple categorisation, with good types of sites and bad types of sites. They were more productivity filters than security filters. Those older-style solutions do not offer much protection against malware and newer type threats which are evolving all the time," he said.

The latest security systems are more intelligent and responsive. "Newer web-filtering solutions look at the actual web address you are visiting. They use reputation filtering, so they know whether each URL is good or bad," said Conway.

"As well as identifying categories of sites such as gambling or adult content, it can look within sites it allows and recognise whether these apparently good sites have been affected with viruses or malware."

These solutions use the mountains of IT security data collated daily by the larger security vendors. "The latest IT security products are dynamic, picking up threats on an on-

going basis. They make use of what are called honey traps, which constantly pick up information all over the internet," said Conway.

"These communicate automatically with your own systems so the updates do not require any staff effort from the client's side. Clients effectively now have access to a database of threats, which is updated in real time."

### Market evolution

Established as Renaissance Contingency Services by Conway and Dennis Woods in 1987, the company was the first anti-virus solution provider in Ireland. It employs 11 staff at offices in Dun Laoghaire.

Renaissance acts as a central distributor, providing IT re-sellers around the country with security solutions in areas including email scanning, authentication, port protection and encryption technologies.

It also offers support for the development and implementation of business continuity and IT continuity solutions for clients. Vendors with whom Renaissance has distribution agreements in Ireland include Sophos, M86, Cryoserver, Beyond Encryption, MX Sweep and Celestix.

Conway said Renaissance's re-seller partners had adapted their own offerings to deal with the realities of the wider economic climate. "There is now very little margin in just selling laptops or similar; they must provide useful value-added services and make sure they keep their clients comfortable and safe. We help them provide full total cost of ownership solutions which are relatively inexpensive and are profitable for the resellers to implement," he said. Advances in the delivery of security solutions – such as new, emerging cloud-based monitoring and management systems – allowed Renaissance's partners to offer clients value for money solutions, said Conway.

"There is a lot more management of people's environments using cloud-based technology going on now. For instance, a reseller might have 20 customers using Cyberoam, and these can all be managed and remotely monitored from one control panel," he said.

"We have also deployed some other cloud-based technologies, such as archiving and mail-filtering, which also allow our resellers deliver services to their clients in a very cost-effective way."

### Advice

IT security could be a big concern for companies forced to cut back on their IT team during the downturn, Conway said.

"IT security is more important now in some organisations because people are now very tight on resources. If a staff member leaves an organisation, you might not have the level of expertise or flexibility in-house that you had previously. Everything is so tight now that nobody can afford any glitches. They need to be a bit more proactive now in terms of how they protect themselves."

Conway warned managers not to just assume that because they had once bought an IT security solution – perhaps something which came bundled with the hardware originally – they were therefore completely safe.

"If someone buys a security solution and plugs it in and just leaves it there, with no maintenance or updating, you are very exposed. You are living with a false sense of security – it's a bit like someone saying, 'I got my house insured years ago, but I never renewed or updated the policy'. Tens of thousands of new threats are coming through the vendors' integrated threat laboratories each day," he said.

The increasing role of IT systems as the vital backbone of all operations within the organisation meant even short losses of access to information or applications could have very

serious business consequences, said Conway. "IT infrastructure is now absolutely a key part of many companies' key business. The level of interruption they can survive is getting shorter and shorter. Organisations need to have their email systems up, their applications running and full access to the internet," he said.

Conway advised companies to make sure they sought professional help should their systems go down unexpectedly. "If you have a failure due to some kind of attack, such as malware or virus, you cannot just restore it as it was, you

must sort it out before you can bring everything back up, so the ability to react quickly, and deal with customers' problems, is key." IT security concerns would continue to be important into the future, particularly as staff became more and more mobile, said Conway.

"You can now bring your internal corporate security systems and policies into a mobile environment. When a laptop or smartphone uses a public wi-fi network everything is referred back through a proxy in your own organisation to make sure you are protected."



Michael Conway, director of Renaissance: 'Older-style solutions do not offer much protection against malware'

SUSAN JEFFERIES

## SOPHOS

simple + secure

# FREE Mobile Security Toolkit

Tablets, iPads and smartphones are great for productivity resulting in more and more organisations using these devices. But with 67% of people not using passcodes, they are also a potential data loss disaster.

Education is the key. Tell people how to keep their smartphones – and the information on them – secure.

The **Mobile Security Toolkit** gives you:

- ▶ Presentation on mobile security threats
- ▶ Video on why you should always lock your phone
- ▶ Tips for creating a safe passcode
- ▶ Plus much more . . .

Download your mobile security toolkit at:  
[www.sophos.com/mobiletoolkit](http://www.sophos.com/mobiletoolkit)

And to find out how Sophos can help you secure your IT infrastructure and data, call us on +44 1235 544138.



## IT SECURITY

## The changing face of IT hacking

By Niall Byrne

The image of the IT hacker as a geeky teen no longer holds true, according to Tim Quan, enterprise security manager, Unity Technology Solutions. Quan said the hacking community had evolved to include clever white-collar criminals facing little threat of ever being caught.

Popular cyber-criminal tactics include the harvesting of credit card numbers. This can be done using rogue fixed and wireless devices, which are classified under a target company's name and attached to legitimate networks.

Spam blasting to hundreds of thousands of harvested email addresses is also popular. This required just a small percentage of recipients to make the crime pay and the cost to the instigator was low, Quan said.

"Typically, they will blast a share and generate a run on it while having bought low and sold high, and the company owners will frequently know little or nothing about it, and are pretty powerless to counter it," he said.

"It is a safe criminal activity but a good spam handling appliance or service will look at this type of activity and reference it correctly as spam, and will drop the inbound mail connection attempt, thus nullifying the profitability."

SMEs also run the risk of having their PCs or servers



Tim Quan, enterprise security manager, Unity Technology Solutions. Right: Colm Lennon, security service manager, Unity Technology Solutions



SUSAN JEFFERIES

used as drones or zombies by criminal who secretly access and use them to launch an undetectable distributed attack on a target.

"These malware code strings can be prevented from 'calling home' by use of a detection service which spots and blocks their intentions, effectively nullifying the intended objective," said Quan.

He said few SMEs had these services in place, relying in-

stead on low-cost firewalls and basic – sometimes free – anti-virus software, which was often the source of the bad code in the first place.

Apart from external threats from dedicated cyber-criminals, bad company practice is another major challenge for businesses. Combating this requires a holistic awareness to security.

"The single biggest threat to an organisation is the insider

threat, which is a trusted user within an organisation circumventing established security controls," said Colm Lennon, security service manager, Unity Technology Solutions.

Lennon cited an example of a hospital employee accessing the admission records of a neighbour they recognised in the waiting room.

"This information can be passed on verbally to an unauthorised person with no mal-

icious intent.

However, the effects are that the hospital security controls have been circumvented and the privacy of the patient breached," he said.

There is also the risk that sensitive company information will be emailed to an unsecured web account or copied to a USB drive.

In many cases, this is not malicious activity, but simply a need for the user to copy infor-

mation to an external source so it can be accessed from outside the office.

However, without effective security controls, the sensitive information left the organisation where the risk of unauthorised access increased, Lennon said.

The organisation cannot guarantee the information is adequately protected once it has left the environment and this can lead to data projection

breaches which can have both reputational and financial implication for an organisation.

Common controls to reduce the risk of insider security breaches include:

- the establishment of a comprehensive security policy;
- an awareness program that reinforces the consequences of non-business access;
- a monitoring tool to analysis activity on an ongoing basis;
- an investigative function to

resolve suspect activity; and ■ a disciplinary component to hold violators accountable.

For external threats, good access control policy and efficient network mapping will help companies to detect rogue devices, having first locked down all legitimate devices.

Good fixed network and wireless network intrusion prevention services will offer greater assurances of data integrity and retention.

## You shouldn't notice great security

It should be perfectly natural, just there when you need it. Reliable, fast and a part of you, you don't even notice.

Like world-class IT security from Renaissance, protection for your business that can cover:

- Anti-virus
- Web
- Email
- Email archiving
- Encryption

To get the protection that suits you, call Renaissance today to find a dealer near you..

Cyberoam

M86 SECURITY

safend  
Securing Your Endpoints

SOPHOS

Renaissance®



## Have some cloud control

By Gareth Naughton

Companies need to reinvent the way that they approach IT security as they move into the cloud or run the risk of exposing their business to unnecessary danger.

Anthony O'Mara, senior vice president of cloud security firm, Trend Micro, said that while cloud computing was an exciting development with huge potential, it should be approached with due caution.

"Cloud computing is a very positive, disruptive influence in the way we can do business today. However, as with anything disruptive it can also create opportunities for the less savoury elements in our society.

"So, to make sure that we can take advantage of the full benefits cloud computing can offer it is necessary that we are not just as diligent but more sensitive to the security threat than we have been for earlier computing platforms," he said.

Trend Micro has been at the forefront of cloud security since its inception, developing products in the space well before its competitors and is now the world's leading cloud security provider.

The company employs more than 220 people at its EMEA operations in Cork with plans to rapidly expand the workforce over the next year.

Rik Ferguson, director of security research and communication with Trend Micro EMEA, believes the industry as a whole needs to see the expansion of the cloud as an opportunity to develop new and innovative products.

"We are working in a completely new architecture right now and we, as the security industry, have to be willing to take a step back, look at what we have done historically and say: 'okay that was then, this is now and we may need to re-engineer something from the ground up in order to make it not just compatible but more effective'.

"It is about looking for the opportunities that technological advancement offers us instead of looking for the quickest way to make money out of it," said Ferguson.

The normal approach to server security is no longer applicable in a world where companies are storing and accessing information and soft-



Anthony O'Mara, senior vice president, Trend Micro

ware on virtual servers which may not even be housed in their own premises.

"Traditionally, we have always designed security from the outside in. We have always imagined an attacker on the outside, so, we build a strong perimeter with Firewalls; maybe some intrusion prevention stuff; content scanners and then some security technology on the servers and security technology on the end point," said Ferguson.

"It has always been built in layers from the outside toward the centre. But in a virtualised world, and definitely in the public cloud scenario, we need to design security from the inside out."

The first step is to secure the data itself by ensuring that everything sensitive is encrypted and that only you have the keys to that data, especially in a shared storage scenario on a public cloud.

"That is right at the centre of your model and, then, we need to make sure that we secure the perimeter of each individual virtual server because they are going to be in a shared environment whether inside your business or in a public cloud with other businesses.

"The only perimeter over which you have any control is the perimeter of your own machine," he said.

"It is about installing effective firewalling and intrusion prevention technology at virtual machine level and making sure that the perimeter of your virtual machine is as secure as it can possibly be. Only that virtual machine should be able to access your encrypted data – you can't even share those keys with your cloud provider be-

cause they shouldn't have access to your data."

While the positives of public and private cloud computing – the ability to house all your servers on one machine cutting down on costs, being more environmentally efficient and allowing staff to access virtual servers from anywhere in the world – companies need to be aware that it presents a new security challenge.

"It is the same threat, but differently applied. In the past, one compromised server may

have been used to launch attacks against other networks – to bury deeper into the network, but traditional technology was designed to cope with that," said Ferguson.

"When you move into a virtualised scenario, traditional technology falls down. If one of your virtual servers is compromised either as a result of an external intrusion, malware or whatever it may be, it could be used to launch attacks against other virtual servers hosted on the same machine."

unity.

Ingenuity,  
Applied.

www.unity.ie

Voice  
Security  
Infrastructure  
Call Recording  
& Analytics  
Managed  
Services

Ireland's leading  
independent provider  
of ICT managed services

Call us now on  
+353 (0)1 247 7400  
visit [www.unity.ie](http://www.unity.ie)  
or email [info@unity.ie](mailto:info@unity.ie)

The Mews, 15 Adelaide St, Dun Laoghaire, Co. Dublin

W: [www.renaissance.ie](http://www.renaissance.ie) E: [info@renaissance.ie](mailto:info@renaissance.ie) T: 01 280 9410

# IT SECURITY

## For security, get your cards in order

Credit card data security is becoming an increasingly important consideration for businesses in all sectors, writes **Dermot Corrigan**

All Irish businesses must be aware of their obligations under the recently introduced Payment Card Industry (PCI) data security standards, according to Angela Madden, managing director, Rits Information Security Specialists.

PCI is an industry standard introduced in 2006 to harmonise security standards for credit card data across all industry players, including financial institutions and individual merchants. No Irish company handling credit card transactions could afford to ignore these regulations, Madden said.

"Anybody who stores, processes or transmits credit card information must comply with these PCI data security standards. Depending on the volume of trade you are involved in or the services you provide, there are various levels to comply with. Vodafone would be a level one given the volume of credit card transactions it does, whereas a local flower shop would be a level four," she said.

Madden said that a number of steps were involved in becoming fully PCI compliant. "Companies have to complete

a quarterly vulnerability scan on the IT infrastructure used to either process or transmit their credit card transactions. They also have to complete a self-assessment questionnaire. If these obligations are not fulfilled, the banks impose hefty fines," she said.

The banks that enforce these standards were increasingly ensuring that smaller companies followed the correct procedure, said Madden.

"Previously, many of the major banks have been focusing on level one and level two merchants, but now we have seen a bigger move towards getting the level threes and four merchants compliant. Until now there was not much awareness of what was involved among these type of businesses," she said.

### Support

Madden said only PCI-approved consultants such as Rits could ensure businesses were compliant with the regulations. "We are one of a handful of QSAs [Quality Security Assessors] who are certified by the PCI council to help people do their audits and become compliant. We are getting more and more people asking us to



Angela Madden, managing director, Rits Information Security Specialists

help them through the process," she said.

The preparation involved depended on the size of company and complexity of the client's IT systems, said Madden. "For the largest organisations it could be a year-long process, until all the necessary controls are put in place. We would sit down with them and do a gap analysis, looking at where they are and what they need to do to become compliant. Your receptionist might never see a

credit card, but the PC on his desk must be appropriately secured," she said.

"We might come in for a few days and do a project plan, which they could then implement internally using their own people and we would come back later and ensure all had been done correctly."

"With SMEs it can usually be done in a day. For small shops who just have the little terminal on their counter it is much easier – we just help

them fill out the self-assessment questionnaire and put it into plain English for them."

### Flirting with disaster

Companies skimping on their IT security spend were flirting with disaster, said Sean Reynolds, founder and chief executive of Rits. "Some people see IT security as a discretionary spend and are backing away from it," said Reynolds.

"They are reducing the protection they have, or taking a chance and not having it at all. However, just because you have not been compromised or your systems have not melted down yet does not mean it will not happen in the future. The more you can do to minimise that sort of exposure, the better."

Reynolds said that the downturn meant that companies were even more at risk of IT security breaches – and subsequent business failures – than they were during the boom times.

"Problems have come with the downturn which are unique to this particular economic environment. You see people, including both employees and management, taking risks which they would not have done in the past. This can lead to some very serious security breaches," he said.

Larger organisations in particular must protect themselves from potential data losses when disgruntled employees left the company, said Reynolds.

"Some people being made redundant are taking the opportunity to steal information which they feel they are entitled to, although they are not. We have worked on a case where a client was blackmailed by former employees who had taken information with them that they should not have. Staff would typically never have considered doing this in a more normal situation," he said.

### Two-pronged approach

Dealing with this new environment required a mixture of strong policies and smart technologies, said Reynolds. "At a minimum you must have a set of rules which everyone knows. Thereafter you need a set of technologies which compartmentalise the data, so that nobody can easily steal your organisation's business critical information," he said.

Reynolds said that there could be some initial pushback from individual staff as these measures were introduced, but in the long run most saw the importance of keeping security as tight as possible.

"The first time they encounter a security partner such as ourselves there is a steep learning curve. Invariably there is resistance initially as they have their own set way of doing things. However, once you show them the issues involved, they are converted and thereafter always write secure code," he said.

### Relationships

Established in 1990 by Reynolds, Rits provides high level IT security consultancy ser-

vices across a broad range of specialist areas such as computer forensics, vulnerability testing and the development of IT security policy and strategy.

Its clients include government departments, semi-state bodies and enterprises across the utilities, financial services, healthcare, pharmaceuticals and IT sectors. "With our larger enterprise and government clients it is always a relationship-based arrangement. That is how we operate – we provide a service where they can call us at 2am in the morning if there is a problem."

"With our clients it is a partnership; we are an independent adviser, and do not push a particular vendor or product line."

### Future plans

The company employs 14 people, with the majority based

at its headquarters in Citywest Business Campus on the outskirts of Dublin.

"We are hoping to add to the team in the coming months; at the junior level and also on our senior consulting team. We are looking to bolster our strength in areas such as PCI standards, forensics and other strategic IT security areas," Reynolds said.

Reynolds said the company was also currently evolving its service offering to customers. "We are modifying the way we operate and looking for economies of scale in our own business. We have cut away some of the commodity-type operations to concentrate more on the service end of the market and ensure we provide a Rolls-Royce premium standard offering. "Over the next six months we will be adding new web-based services, particularly targeted at the SME sec-

tor," he said.

"We are hoping to add to the team in the coming months; at the junior level and also on our senior consulting team. We are looking to bolster our strength in areas such as PCI standards, forensics and other strategic IT security areas," Reynolds said.

Reynolds said the company was also currently evolving its service offering to customers. "We are modifying the way we operate and looking for economies of scale in our own business. We have cut away some of the commodity-type operations to concentrate more on the service end of the market and ensure we provide a Rolls-Royce premium standard offering. "Over the next six months we will be adding new web-based services, particularly targeted at the SME sector," he said.

### Commercial Profile: Trend Micro

## Protecting your network from the threat inside

How to turn risk into productivity



Thanks to mobile devices, such as Blackberries, iPhones and iPads, your employees are able to work anywhere, anytime, and ensure productivity levels while away from the physical office. However, a myriad of new threats to the business network have been created by those "on the inside", as a result of this process of "consumerisation."

As employees connect their own devices to the network enterprises must consider the impact on their IT security. At its core, consumerisation describes how innovation in information technology now emerges primarily in the home and how it is adopted (some would say invades) in the world of work.

Recent technological innovations haven't just shifted the goalposts; they have changed the game plan entirely. Data costs both for broadband and for 3G access have tumbled; unlimited use packages are now the norm.

The advent of the iPhone turned device selection into a consumer-driven choice and the success of Android has amplified that. The success of the iPad has meant that the laptop is being relegated to the status of the desktop. Cloud services such as Twitter, Facebook, Google Apps, Amazon Web Services, and Apple's iCloud have pushed the collaboration and communication platforms outside the corporate perimeter and into the hands of the user.

Employees increasingly expect our work environment to be available on-demand and visible from wherever we are, whatever the hardware we choose to use; in fact this is one of the key defining characteristics of cloud. File-sharing services, virtual server availability, social networks, blogs, wikis, instant messaging public hotspots, low cost mobile internet, high-performance hardware, collaboration environments these all mean that external is the new internal. It is entirely possible, with a combination of these consumer services, for an employee to

sit in your head office, never once connect to the corporate network and still have access to everything they need to do their job effectively.

### Is your enterprise blind?

So when employees access their corporate email from a 3G tablet using a web interface and use a public file sharing service to synchronise their files; when those employees laptops are left chained to their desks and their work life is mobile; when they use public social networks for professional networking and never connect to the VPN; does your enterprise just go blind? And is that employee sitting in your head office inadvertently creating a technology threat that your business just won't see coming?

### A strategy that differentiates

The answer on both counts is no – as long as your organisation has a robust consumerisation strategy. This means the ability to manage any device that connects to corporate assets over public networks such as 3G. To focus on connection to the enterprise network is no longer sufficient. Your consumerisation strategy needs, for example, to be able to remotely differentiate the corporate from the personal content on user-owned devices (consumerisation is about so much more than the device your employees choose to use.)

Access to information and services both internally and externally needs to be re-examined in the face of this crumbling perimeter. Your business needs to acknowledge the reality that is already upon it. As was pointed out in a study by the Economist Intelligence Unit back in 2009 "much education, training and organisational experimentation is needed to ensure that greater technology freedom does not sap productivity or cause damage to the company. The sooner that firms begin to tackle this, the sooner the

benefits of technology democracy will start to flow".

### Where can I learn more about consumerisation and how it affects my business?

Trend Micro has a comprehensive range of solutions to help ensure that consumerisation becomes a byword for productivity – rather than shorthand for a security risk – in your business.

These include:

- Mobile Device Management and Mobile Device Security. Available for almost any mobile operating system, Trend Micro Mobile Security manages and secures smart phones and tablets, including those based on Android, BlackBerryOS, and Apple iOS.

- Light & Lean Endpoint Security protects PC and Mac with the industry's lightest, yet fastest and most effective threat protection suite.

- Data protection. Trend Micro provides end-to-end protection for data, whether it's at rest, in motion or in use.
- Enterprise applications on the Web and in the cloud. Trend takes customers through the virtualization journey from server virtualization, through desktop virtualization to cloud computing, securing users, protecting applications and maintaining privacy and integrity of corporate information.

- Threat Discovery and Threat Information Management. Trend Micro's non-intrusive, out-of-band network over-watch technology identifies rogue devices and pinpoints the sources of dangerous or malicious traffic, so administrators can take charge.

To learn more about how Trend Micro can work with your enterprise to protect and manage your IT security with innovative solutions and products, please visit [www.trendmicro.ie](http://www.trendmicro.ie) or contact us on 021-7303000



# Check Point 3D SECURITY

Check Point 3D Security combines policy, people and enforcement for unbeatable protection

**POLICY**  
POLICY that supports user needs and transform security into a business process

**PEOPLE**  
Security that educates and engages PEOPLE in policy definition, education and incident remediation

**ENFORCEMENT**  
Visibility and control of all layers of security—network, application and data

[www.integritysolutions.ie](http://www.integritysolutions.ie)  
[info@integritysolutions.ie](mailto:info@integritysolutions.ie)  
+353-1-2934027