



**>EVERYTHING YOU NEED TO KNOW  
ABOUT EMAIL AND WEB SECURITY  
(BUT WERE AFRAID TO ASK)**

>A NON-TECHNICAL GUIDE FOR OWNERS AND MANAGERS  
OF SMALL TO MEDIUM SIZED BUSINESSES

## >CONTENTS

INTRODUCTION	>1
'IT CAN'T HAPPEN TO ME.' REALLY?	>1
VIRUSES, SPAM AND PHISHING	>2
INAPPROPRIATE CONTENT, EMPLOYEES BEHAVING BADLY	>3
HOW TO ASSESS YOUR RISKS	>4
WHAT TO DO ABOUT IT	>5
CASE IN POINT: MESSAGELABS HELPS ACORN ASSESSORS	>7

**IT SECURITY  
ISN'T JUST  
GOOD PRACTICE,  
IT'S GOOD  
BUSINESS.**

**>INTRODUCTION**

What you don't know can destroy your business. It's hard to imagine modern business without the internet but in the last few years it has become fraught with danger. Internet crooks are the dotcom entrepreneurs of crime, using the power of computers and the interconnections of the network against innocent businesses to make money.

Make no mistake; viruses, spam and spyware are the products of a global 'business' that is worth as much as \$105bn<sup>1</sup> a year. To put that into context, online crime is bigger than the global drugs trade. With so much money at stake, it's not surprising that the problem is getting worse.

The risks are only part of the story. Internet security is also a competitive advantage. Customers and suppliers want you to care about their privacy and protection. Who will pick up your customers if a computer security incident hits your business? IT security isn't just good practice, it's good business.

**>'IT CAN'T HAPPEN TO ME.' REALLY?**

Many businesses, especially those with little or no IT support, tend to put a low priority on protecting themselves. Ironically, this makes them more attractive targets.

Consider the accounting firm that was infected by a virus because their anti-virus software wasn't up to date. It took them days to clean up their computers, and their reputation suffered because their computers turned into 'zombies' which send out spam email to all and sundry. The repairs cost thousands, but the reputation or brand damage is incalculable.

Imagine a manufacturing business where certain employees downloaded pornography in the office. It sounds like a cringeworthy episode of The Office. But if an employee took the company to an Employment Tribunal for permitting a degrading and offensive environment it could turn into a serious drain on management time, with a substantial fine to make it worse. It can happen. In one recent case, a tribunal found an employer guilty of sex discrimination because employees were looking at pornography in the room where the complainant worked.

IT systems and information security are more important to UK companies than ever before and many small businesses now believe security is as high a priority for them as large business. A recent DTI survey<sup>2</sup> reported that nearly 50% of UK firms reported one or more IT security incidents in the last year. The average serious incident can set you back between £10,000 and £20,000. The good news is that an ounce of prevention is worth a pound of cure.

<sup>1</sup>The Online Shadow Economy – MessageLabs whitepaper  
[http://www.messagelabs.co.uk/white\\_papers/online\\_shadow\\_economy.aspx](http://www.messagelabs.co.uk/white_papers/online_shadow_economy.aspx)  
<sup>2</sup>BERR; 2008 Information Security Breaches Survey

## >VIRUSES, SPAM AND PHISHING

According to MessageLabs Intelligence<sup>3</sup> which is based on analysis of billions of emails and web pages each week - one email in every 143 is malicious. One in 245 is a fraudulent phishing email. Eight in every ten is spam. Over one thousand new malware web sites are discovered each day. Put simply, unless you protect yourself properly, email and web access is always going to give you problems.

But what do these terms mean for business? If 80 percent of email is unwanted spam advertising, it means 80 percent of your email server's capacity and 80 percent of the bandwidth used for email is wasted. Email seems 'free', but you pay for servers and internet connections. Wouldn't it be better to cut off the flow of spam before it reaches your network? That way you keep the bandwidth and server capacity for your business, not the criminal's.

Phishing emails are more dangerous. They are used to trick people into giving away private information on fake (but highly realistic) websites. A common example is to persuade people that they need to log into the online bank account and sort out a bogus transaction.

Criminals use these sites to get bank account numbers, passwords, credit card information and passwords.

Another common trick is to get employees to log into a fake, company website, so that criminals can get user names and passwords to log into your network. The risks of business fraud are obvious. Some of these fake sites are so realistic even experts can tell them apart from the real thing. Wouldn't it be better if these emails never reached your employees?

So what about the threat from malware? Call them viruses, worms, trojans, spyware - they all spell bad news. Malware is an unwanted program written by criminals running on a computer in your business, and that's a never good idea.

What sort of damage could this do? Viruses can give hackers remote access to your data and remote control of your systems. They can also be used to launch criminal attacks on other computers. They can send out thousands of spam email messages. They can infect other computers. Worst of all, they can do all this without any outward sign that something is wrong. Other kinds of viruses display intrusive adverts for pornography and gambling, and even disable security software. If there is a way to make money from your computers, there is a virus that will do it.

Viruses can give hackers remote access to your data and remote control of your systems. Viruses spread in email attachments, when people visit certain websites or simply spreading from computer to computer on the network. The only way to be safe is to keep your network virus-free.

<sup>3</sup>MessageLabs Intelligence; 2008 Annual Security Report  
<http://www.messagelabs.co.uk/intelligence.aspx>

## >INAPPROPRIATE CONTENT, EMPLOYEES BEHAVING BADLY

Then there are pressing legal, productivity and reputation issues:

- Do you want your employees downloading pornography or other inappropriate content on work computers? It could happen – the majority of visits to pornographic sites occur during office hours
- What if an employee inadvertently defames someone or binds the company to a damaging contract by email? Email can be used as evidence in a court of Law.
- What if someone takes you to an employment tribunal claiming a hostile working environment? Damages in discrimination cases are potentially unlimited.
- How much productivity can you afford to lose to 'cyber slacking' – employees browsing non-work related websites on company time? Social media websites blur the boundaries between work & leisure and many employees expect to be able to access these type of sites at work.
- What would happen if an employee sent sensitive information to a competitor or disclosed confidential information to an unauthorised person by email? Would you be able to enforce company policies, or even track the breach? One of the eight principles of the Data Protection Act is that personal information must be 'secure'. Reckless disclosure is a criminal offence.

These are important questions. The issues they raise are not the result of outside attack but the consequences are still real, clients still leave and careers still crash and burn. Companies need to write and enforce acceptable use policies, and they need technology to help them do it.

**THE FIRST  
STEP IS  
NOT ABOUT  
TECHNOLOGY  
– IT'S ABOUT  
ASKING  
SOME SIMPLE  
BUSINESS  
QUESTIONS .**

## >HOW TO ASSESS YOUR RISKS

Security starts with putting a business value on different kinds of risks so that you can allocate resources to reducing them. It makes sense to prioritise: you don't have an infinite IT budget, and some risks are more threatening than others. Therefore, the first step is not about technology - it is about asking some simple business questions.

1. What are you trying to protect? Typical issues include legal requirements, such as the Data Protection Act, and professional obligations such as client confidentiality. Then there are straightforward business issues. Nobody wants to publicise sensitive information like plans, lists of potential customers and so on. You may have mission-critical systems such as your email, ecommerce site and accounting records. Don't forget intangibles such as management time, IT resources, your company's reputation and morale.
2. What are the risks? There are external risks from outsider attacks, such as viruses and hackers and increasingly targeted Trojans aimed at specific individuals within an organisation with the purpose of compromising networks for corporate espionage. Internal risks are on the rise and no organisation is immune from incidents of staff misuse or abuse of IT systems. These can raise legal concerns, such as the risk of employee misbehaviour landing you in an Employment Tribunal.
3. Who is responsible for IT security? It is not enough to delegate the question to your IT department or supplier. You need to see IT security as a business-wide issue and address it at a board level. If you know what you want to protect and what the risks are, setting priorities, delegating responsibility and allocating budgets all fall in line with what is important to the business. Which manager is going to take the lead? Who is responsible for creating and implementing a plan? What budgets are available and appropriate? For example, compare your IT security budget with your insurance costs.
4. Where's the plan? Even if it is a couple of pages, an IT security plan is the first step to protecting your business. It's better to have a good plan now - and carry it out - than wait until you have a perfect plan next year. Do you have the right software and technology? Do you have appropriate staff policies and training? What is the budget and timetable?

## >WHAT TO DO ABOUT IT

So far, we've talked about the business risks and taken a management view of IT security. Now we're going to talk about the steps you need to take to protect yourself. You can use this checklist as a starting point.

- Virus and spyware protection. You need to stop viruses and other unwanted programs from getting in the door. With thousands of new virus variants materialising each month, it is critical that your protection is able to keep up with new and previously unknown threats as they emerge.
- Spam filtering. Blocking spam will save employees time and reduce the risk of fraud from phishing emails.
- Firewall. A firewall will stop viruses that spread directly over the internet, and it can also keep hackers away from your network and servers.
- Access control. Make sure that employees only have access to the information they need to do their job. To give an obvious example, don't let the whole company have access to payroll records.
- Policy enforcement. You need effective staff policies about employee use of the internet backed up with training that covers policies and practical matters such as the use of strong passwords. Technology can help enforce company policies on appropriate use of the internet, such as bans on downloading inappropriate images or sending certain information by email.
- Encryption. Consider encrypting data on laptops and other portable devices to prevent thieves accessing sensitive information if they are stolen. Also, consider email encryption to protect the confidentiality of messages between your business and its partners. By default, email travelling over the internet is not encrypted which means that it can be read – like the text on a postcard – as it moves from sender to recipient.
- Physical security. Don't forget that a stolen server is as much of a risk as a virus-infested one. Locks, alarms, secure server rooms and visitor access control are all part of IT security.
- Backup. Critical data, including email archives and business databases, need to be regularly backed up with copies stored offsite. Test the restore process regularly too.
- Software updates. Make sure that all the computers in your business are kept up to date with manufacturers' updates. These are published regularly by the major vendors and fix known flaws and vulnerabilities. Virus writers exploit these vulnerabilities to attack people who do not update quickly enough.

## >CASE IN POINT: MESSAGELABS HELPS ACORN ASSESSORS



Acorn Assessors is a firm of independent engineers who work with lawyers and insurance companies to investigate accident-damaged vehicles. Acorn Assessors has approximately 50 staff members using MessageLabs Email Security Services (Anti-Virus, Email Anti-Spam, Image Control and Content Control). The IT department at Acorn Assessors spent most of their time dealing with spam and viruses. Spam had become such an issue that the volume of unwanted email was clogging the mail server, causing it and the company's website—which runs on the same server—to crash.

Jonathan Townsend, IT director, was asked to look into Acorn Assessors' options. "I was familiar with MessageLabs, having used it with a previous employer," he explains. "But I also looked at software to bolt onto the exchange server. It would mean buying large license packs, rather than adding licenses as we expanded."

Townsend also discovered that the software option would mean that his team would have to provide ongoing maintenance and support. Townsend continues: "What we get with MessageLabs is a comprehensive solution that would have required multiple pieces of software and more cost. The MessageLabs service is managed by experienced professionals and uses world-leading software, so it's one of those 'set it and forget it' services that you know will work as it should."

By pointing incoming and outgoing email messages to MessageLabs Hosted Email Security service to filter messages before they reach Acorn Assessors, staff only receive legitimate email meaning that bandwidth use is streamlined.

"Before we had to sort out the bandwidth issues and sort out viruses, which takes time and costs money. With MessageLabs that time can now be spent streamlining business processes, creating new software, and ensuring that staff desktops are performing efficiently.