Superfast Business Wales

Business Guide

IT Security

Security is surrounded by hype, myth and scare-mongering, especially when linked to the internet. While Superfast Broadband will offer your new business opportunities through online sales and marketing, mobile services, and the like, it is all too easy to worry that its use will pose dangers to your business.

www.business.wales.gov.uk/superfastbusinesswales | 03000 6 03000

Busnes Cymru Business Wales

UNDEB EWROPEAIDD EUROPEAN UNION

Llywodraeth Cymru Welsh Government

Cronfa Datblygu Rhanbarthol Ewrop
European Regional Development Fund

Llywodraeth Cymru
Welsh Government

IT Security

Security is surrounded by hype, myth and scare-mongering, especially when linked to the internet.

While Superfast Broadband will offer your new business opportunities through online sales and marketing, mobile services, and the like, it is all too easy to worry that its use will pose dangers to your business. Security is actually about ensuring that your business assets – information, knowledge, finances, etc. – are adequately protected. It is about understanding what is of value to your business, how it could be compromised (lost, altered, misused) and how that could affect you financially and legally, or affect your reputation.

It is about taking sensible precautions against risks to your business as part of your overall business strategy. It is too easy to implement basic IT security controls and think that you are secure.

Security is about identifying your valuable assets, and reducing the risk to them to acceptable levels. This guide looks at information security from a number of perspectives, including use of the internet, giving basic information on some of the key issues you need to think about. It does not provide a guaranteed solution – all businesses are different and need to tailor their security solutions to their specific perceived risks.

Understand

The Way Forward

It is vital for any business to adequately protect its information and systems. The consequences of not doing so include impact on revenue, business interruption, poor legal compliance, compromised reputation or, at worst, business failure. Therefore, businesses need to take a systematic approach to security and the place to start is to compile and implement an effective information security plan.

All this looks daunting, but just requires a methodical approach. The key is to write a security plan that identifies what you need to protect and why. You can then decide what security controls you consider necessary or appropriate to reduce those risks to an acceptable level.

Writing and implementing a security plan does not have to be a huge task. A good plan today is better than a perfect plan tomorrow, and it can always be updated and refined later.

There is no such thing as absolute security. It is about balancing the cost of security against the risk of damage to your business. A good place to start is the Business section of the **getsafeonline website** (www.getsafeonline.org) which describes the security issues, and possible mitigations, for a number of business activities. Use this as a check-list of things to think about. Not all issues may apply to you.

If you accept payment by credit card you may need to conform to the PCI standard set by the credit card industry. Details can be found at www.pcisecuritystandards.org

Most of the security requirements are common sense and a good foundation for your security plan.

What Are The Real Threats?

There are plenty of scare stories about malicious attacks. In reality the vast majority of security problems are the result of deliberate or accidental actions by authorised users. Any reasonably secure system will be resistant to casual random external attacks. More likely are security breaches through, for example, people opening rogue emails, looking at a rogue web site, connecting an infected personal device to your network or processing a fraudulent order.

You should take the same precautions against unreliable customers when doing business over the internet as you would when doing business face-to-face. For example, you could enforce verifiable registration before approving purchases over a certain value.

> There is good advice about fraud scenarios, and how to minimise their effect, on the **Action Fraud website at** www.actionfraud.police.uk/support_for_you An excellent source of information on typical scams, not all via the internet, can be found in the **Little Book of Big Scams, downloadable from** www.met.police.uk/docs/little_book_scam.pdf

Adopt

What Does Security Cover?

You need to consider four areas:

- **Technical** - ensuring that your information systems are well protected from misuse–not just the computers in your office, but those supporting your web services and those with remote access.

- **Personal** - people are all too often the weakest link. You need to make sure all those who can access your systems have the right privileges, and know what their responsibilities are.

- **Procedural** - processes need to be put in place to ensure people understand and follow your security policies.

- **Legal** - there are specific legal obligations that you will need to be aware of which require particular security measures to be in place.

There is also physical security - access controls into buildings, etc. This should be part of your overall security approach – for example, it may be easier to provide strong access control to your office rather than to install complex software controls on every computer in that office to prevent visitors misusing your systems.

Exploit

Key Areas to Think About

Security is broad in scope, but there are a number of basic principles that underpin most security decisions.

Basic system protection

All systems should have basic security protection installed at the device level (e.g. antivirus/ antispyware), network level (e.g. firewalls) and application level (eg. activity, logs, encryption). All such software must be kept up-to-date.

Access to information

Managing who has access to which information is vital in any business. Make sure people only have access to those facilities and information they need–for example only a few trusted people should have administrator rights. Equally important is the need to know who accessed what information and when.

Whether your data is stored on a local or remote server or in the cloud, the same rules should apply, as they do whether people are accessing your systems locally or remotely – for example from a laptop in a public place or a computer at home. For remote access you need to make sure the method of access is secure, even where, for example, a public wifi service is being used. Technology such as VPN services are ideal for this, and are commonly available.

You may also have contracted out business processes to a third party – for example, payroll. While you may not have direct remote access to such services, you still need to ensure that they protect your data according to your security plan.

Personal devices

Employees increasingly want to bring their own devices (BYOD) into the workplace – whether laptops, smartphones, tablets or USB - connected devices. This can expose your systems to uncontrolled infection.

Allowing employees to put company data on a personal device results in some loss of control over that data. An employee’s device can be difficult to monitor effectively; it can be difficult to know what data is stored on the device if lost or stolen; and when the employee leaves it could be impossible to retrieve the data.

There are a number of packages that offer Mobile Device Management. These require all mobile and BYOD devices to include software that ensures integrity and consistency of data across your systems. They also enable the remote wiping of data if the device is lost or stolen. For it to be effective, you need to ensure that all devices that connect to your systems are included.

Protect your website

It is essential to protect an ecommerce or marketing website against external attack as well as technical failure. The consequences of not doing so include loss of service, reduced revenue and damaged reputation.

If you are hosting your own website rather than using a third party hosting company, ensure that the hardware and software is secure. For example, use the latest version of any ecommerce software; make sure the server is protected by an effective firewall and antivirus/antispyware software; monitor log files carefully to spot any attempts at intrusion; and never store customers' private information and credit card details on a publicly accessible ecommerce server.

Legal requirements

If you hold personal data on clients, employees or other individuals you will need to conform to the Data Protection Act (DPA) and register with the Information Commissioner's Office (ICO). This requires you to implement adequate security measures to protect the privacy and integrity of personal data wherever that data is held including, for example, on personal devices and remote clouds.

There are also limits to the extent to which you can monitor what your employees are doing on your systems A brief guide for SMEs on these topics can be found on the ICO website at:
http://www.ico.org.uk/for_organisations/guidance_index/~/media/documents/library/Data_Protection/Practical_application/quick_guide_to_the_employment_practices_code.ashx

A short security guide is also available at:
http://www.ico.org.uk/for_organisations/guidance_index/~/media/documents/library/Data_Protection/Practical_application/it_security_practical_guide.ashx

There are legal requirements on the need to provide access on your websites to your personal data privacy policies and policies on use of cookies, also covered by ICO guidance documents.

Staff policies

When employees have access to the internet at work, they can download viruses, create legal liabilities, and, potentially, leak valuable information. There is also potential for considerable timewasting and lost productivity. Good technical security and staff training can help.

It is essential to develop Acceptable Usage Policies that clearly define what behaviour is expected and what is not acceptable for all users with access to your systems. This should be part of your terms of employment. Strike a balance between practicality, trust and control.

Such a policy should include topics such as:

- When use of company facilities for private use is acceptable (including what sort of use)
- Guidelines on the installation of programs, downloading of data (e.g. films or music) or use of remote services without prior permission
- What personal devices can be connected to your network, and with what restrictions

Top Tips

Security is holistic

It is about identifying and addressing risks to the business, not just technical IT risks.

Prepare a security plan

Identify what is valuable to you, how it could be compromised, and how the risks can be reduced to an acceptable level.

People are key

Ensure all those with access to your business systems understand and follow your security plan, procedures and processes. Create Acceptable Usage Policies and make sure everyone with access to your systems signs and follows them.

Information is knowledge

Know where your information is. It might be on a remote service you do not control directly, or on a laptop, iPad or home computer. Ensure that information and services important to you are properly protected wherever they are.

Securing external services

Where you provide web services, make sure they are securely separated from your internal business systems, and that the web services themselves are properly secured – even if they are provided by a third party web service.

Conform to the law

Especially where you handle personal information.

Patch control

Ensure that you always have installed the latest version of software products and that you install promptly all critical patches and updates issued by product suppliers.

Review and update

The world does not stand still, nor will your business. Keep verifying that your security plan is valid and update it, and the underlying security implementations, as necessary.

Keep it simple

Security can be seen as a hindrance. Do as much as you consider necessary to protect your business, and to reduce risk to a level that you are comfortable with. Don't implement complex security systems without careful assessment of the benefit against the cost (which may be as much about people issues as technology).

Useful Resources

www.ecrimewales.com

e-Crime Wales is a partnership of organisations and agencies committed to equipping Welsh businesses with the knowledge and tools to be aware, vigilant, informed and ultimately safe from the destructive effects of e-Crime in all its forms.

NEXT STEPS

1. **Register to attend a fully-funded Business Development Workshop.**
   www.business.wales.gov.uk/superfastbusinesswales/events

2. **Make an appointment to see a Business Advisor who will help you create a personal action plan to grow your business.**
   www.business.wales.gov.uk/contact-us

For further information on IT Security take a look at:

See how other businesses in Wales have exploited Superfast Broadband
www.business.wales.gov.uk/superfastbusinesswales/superfast-success-stories

---

Find out how much your business could save with our
www.business.wales.gov.uk/superfastbusinesswales/savings-calculator

---

Other business guides that may interest you include:
www.business.wales.gov.uk/superfastbusinesswales/superfast-business-guides

---

For monthly updates on business development, technology news and events subscribe to the Business Wales Newsletter below.
https://public.govdelivery.com/accounts/UKWALES/subscriber/new

---

For more information call 03000 6 03000 or visit:
www.business.wales.gov.uk/superfastbusinesswales