IP
Wales

Protecting your ideas

SME Guide to IP Cybersecurity

IP cybercrime

Intellectual Property (IP) is the area of law used by businesses to differentiate their products and services in the commercial marketplace via distinctive branding or endorsement; new inventions or creations; novel appearance or design. IP can be a critical asset for your business but one which is at risk of attack from cybercriminals if your business trades online, has a website or even just email.

IP crime is traditionally viewed as counterfeiting (false branding) and piracy (illegal copying) but cybercriminals are increasingly coming to recognise the value of confidential data held by your business, be it sensitive information about your business operation or customer information such as credit card details (note EU General Data Protection Regulation 2018).

Your Trade Secrets which may be subject to online attack include:
technical & scientific data – formulas; software code; know-how details; product information relating to design/composition/performance; manufacturing information relating to raw materials; refining processes; specialised machinery.
commercial data – business plan; marketing strategy; contract terms; supplier arrangements; customer profiles/preferences/requirements; sales methods.
financial data – internal cost structure; price lists; salaries.
negative data – dead-end research projects; failed manufacturing processes.

In reality, any data which could be of value to your business is a worthwhile target for the cybercriminal. Attacks on data are happening with increasing rapidity and ever more complexity. Zero-day vulnerabilities (where hackers have discovered and exploit a software security breach before a fix is available) are increasing exponentially. When compared to making money from traditional crimes against tangible property cyberattacks on SMEs is a relatively low-cost and low-risk proposition, especially for those residing in jurisdictions where the activity is not actively prosecuted by State authorities.

Dispelling myths

My business is too small to be a target and does not have data worth stealing – in the two seconds it has taken you to read this 25 people online just became the victims of cybercrime. Cybercrime is often indiscriminate in nature. Research carried out by IP Wales for the Welsh Government in 2011 reported over 50% of our respondent SMEs had been subjected to malware (malicious software) attack in an era of 2.3 million items of malware, as compared to over 430 million items of malware today.

My free software protection does the trick – whilst free cyber security solutions are readily available they do not offer comprehensive protection (Fazio Mechanical is thought to have used a free version of malware protection – see below).

My computer is a Mac so I'm safe - with tight security features and a largely virus-free ecosystem Apple users might be forgiven for having a greater sense of protection. However, the 2016 'Transmission BitTorrent app hack' shows the danger of any complacency and cyberattacks on the Apple mobile devices platform are increasing in regularity.

Types of cyberattack

'*Network confidentiality*' – the main IP cyber threat, the aim here is to steal or release confidential data held by your business. Research carried out by IP Wales for the Welsh Government in 2011 reported over 80% of our respondent SMEs did not scan staff emails for confidential data or have any controls over the use of USB sticks at work, 70% did not encrypt customer payment details and nearly 40% did not encrypt their wireless network. In 2013 US retailer Target was the subject of a network confidentiality attack which resulted in the loss of sensitive data relating to 70 million customers, including 40 million credit card numbers. The hack resulted in over 90 lawsuits being filed against Target by customers and banks for negligence and compensatory damages. Whilst Target had just spent U$1.6m on a malware detection tool, investigations revealed the hackers acquired the data through Fazio Mechanical (a third party supplier of less than 100 employees) by accessing the network credentials given to it by Target (an attack technique known as 'island hopping', where the cybercriminals target the weakest link in the cybersecurity chain).

'*Network availability*' – typically known as denial-of-service (DoS) or distributed denial-of-service (DDoS) attacks, the aim is to render the web site inoperable by flooding it with a massive number of requests (e.g. a 'botnet attack' – co-ordinated attack using hacked PCs, printers & web-connected 'smart' home devices such as CCTV cameras, kettles, toasters etc. under the "internet of things"). Following a US Secret Service investigation in 2016 Frazer-Mann of Elite Loans admitted five charges in Cardiff Crown Court of commissioning DoS attacks on rival pay-day loan companies. He offered hackers from Costa Rica U$100 to take competitor websites down.

'*Network integrity*' – the aim is to cause damage to hardware, infrastructure, or real-world systems. Delivered by a rogue employee using a USB drive the 2012 'Shamoon hack' on Saudi Aramco's computer network resulted in 30,000 company computers requiring replacement.

The techniques used by cybercriminals to give effect to these attacks, targeted or otherwise, include:
<u>(Spear-)phishing/smishing</u> – an innocent looking email or sms message (to a targeted individual) enticing them to click on a link or download a file which then infects the user's system, spreading to infect other users. With so much information now publicly available about targeted individuals on social media cybercriminals are becoming increasingly sophisticated with their 'baiting' email or message.
<u>Watering-holes & exploit kits</u> – a compromised web site with predator code waiting to exploit the unsuspecting visitor.
<u>Ransomware</u> – be it 'locker ransomware' (locking the screen) or 'crypto ransomware' (preventing access to your own files or data via encryption – see the 'wcry'/'WannaDecrypt0r' attack on the NHS in May 2017).

Cyber espionage

Disgruntled employees, hackers, hacktivists, industrial competitors may not be the only potential intruders into your network. An American IP Report published in 2013 estimated the annual losses to IP theft, primarily from China, exceeding U$300 billion with many attacks targeted against SMEs. In 2014 the US Justice Department indicted 5 officers from China's People's Liberation Army Unit 61398 for stealing intellectual property to help China's state-owned and state supported enterprises, a charge denied by a Chinese spokesperson.

Data content driven business

If yours is a data content driven business then you need to be able to monitor both the unauthorised and unlawful promotion and distribution of your digital content e.g. files of films/tv programmes, music, software, computer games, books, reports or 3D printing designs.

A Report published by the World Intellectual Property Organization (WIPO) in 2015 predicts that most firms will soon need to familiarise themselves with the legal realities of the 3D printing 'revolution'. The Report notes that the distinction between industrial versus personal 3D printing (also known as 'additive manufacturing') is fading as the personal segment of the market becomes more commercial but *"personal 3D printing potentially raises issues of large-scale infringement of existing IP rights. Underlying this challenge is the tension between what is legal and what is enforceable in practice".*

Established in 2013 under funding from the UK Intellectual Property Office, the City of London Police established the world's first Police Unit dedicated to combating IP Crime. The Police Intellectual Property Crime Unit (PIPCU) has a wide remit under which to launch initiatives such as 'Operation Creative', which targets websites that provide free illegal downloads of films & music in order to draw down online advertising revenue. However, these sites typically operate beyond PIPCU jurisdiction, so the policy has had to become one of disrupting rather than dismantling this borderless online IP crime.

The commercial strategy for addressing the unauthorised/unlawful use of your digital content is for your business to determine, with legal compliance/policing & enforcement often treated as two sides of the same coin. Microsoft's Digital Crimes Unit (MDCU) uses the civil law (with its lower burden of legal proof) to take action against cybercriminals, while seeking to work with national law enforcement to seize their physical infrastructures.

IP Cybersecurity

If data is the raw material for the new information age, then cybersecurity is the prerequisite to businesses operating securely within the new digital environment.

We are familiar with security precautions safeguarding the tangible property of a business but unlike the burglar alarm which only alerts the business to an intrusion and hopefully deters, cybersecurity can proactively protect your intellectual assets by blocking the majority of intrusions into your network before infection. It can rapidly detect and remediate any infection which has infiltrated your network. It can also stop data breaches from lost or stolen end points (desktops, laptops, tablets, smartphones, USB sticks etc.); safeguard online financial transactions; secure your password management; manage back-ups. It can even pre-empt future data attacks via automated risk assessments.

Cybersecurity is mission critical for any IP active business with an online presence. A failure of cybersecurity carries with it the risks of:

- *Leakage of sensitive data* – allowing both internal and external attackers to compromise confidential business/customer data held by your business or conduct unauthorised releases of sensitive information, causing reputational damage and a loss of trust in your business.

- *Import/Export of Malware* – importing of malware into your network and/or the exporting of malware to your business partners or the general public at large.

- *Your exclusion from Supply Chains* – excluding your business from supply chains to prevent attackers from inflicting reputational and/or financial damage to partner organisations and their customers ('island hopping').

A breach of your firms' cybersecurity is at best an inconvenience and at worst could prove critical for the survival of your business. Yet in research conducted by IP Wales for the Welsh Government only 1 firm allocated 10% or more of their IT budget towards cybersecurity measures. Recent research into 500 UK SMEs funded by Trend Micro (see below) revealed that over half the firms surveyed had no internet security tools to protect their business from cyberattack.

Officially launched in February 2017 the UK National Cyber Security Centre (NCSC) – a part the UK Government Communications Headquarters (GCHQ) - has warned SMEs,"*if you openly demonstrate weaknesses in your approach to cybersecurity by failing to do the basics you will experience some form of cyberattack…**doing nothing is no longer an option***".

Planning your IP cybersecurity resilience

Preparations for a cyberattack on your business should include (a) vulnerability mitigation measures and (b) developing an incident response and disaster recovery capability i.e. a well-tested plan of what to do if those prevention measures fail.

Vulnerability mitigation measures

Preventing, detecting or disrupting an attack at the earliest opportunity limits potential business impact and reputational damage. ***Cyber Essentials*** is the UK government's minimum standard of protection for IP cybersecurity and promotes the use of[1]:

- *Firewalls & internet gateways* – detect and block executable downloads, block access to known malicious domains and prevent users' computers from communicating directly with the Internet.

- *Malware protection* – establish and maintain malware defences to detect and respond to known attack code.

- *Patch management* – patch known vulnerabilities with the latest version of the software.

- *Whitelisting & execution control* – prevent unknown software from being able to run or install itself (including Autorun on CD & USB drives).

- *Secure configuration* – restrict the functionality of every device, operating system and application to the minimum needed for your business to function (note the need here for *Cloud* security principles).

- *Password policy* – ensure an appropriate policy is in place.

- *User access control* – limit normal users' execution permissions and enforce the principle of least privilege.

If your business falls victim to a network availability or network integrity attack it will be self-evident but network confidentiality attacks are often less obvious. Internal system monitoring & external surveillance (e.g. dark web) provides a capability to detect actual or attempted attacks and is increasing in importance to comply with legal or regulatory requirements.

[1] Common Cyber Attacks *Reducing the Impact* (NCSC)

Other controls to mitigate the various stages of a cyberattack include:

Survey stage

- User education & awareness – train all users in the risks of public disclosure and spear-phishing techniques.

Delivery stage

- Network perimeter – block insecure or unnecessary services or only allow access to permitted websites.
- Malware protection – block malicious emails and prevent malware being downloaded.
- Password policy – improve the quality of passwords and lock user accounts after a low number of failed attempts.
- Secure configuration – restrict system functionality to the minimum needed for business operation on every device.

Breach stage

- Patch management – apply patches at the earliest possible opportunity.
- Monitoring – monitor and analyse all network activity to identify any malicious or unusual activity.
- Malware protection – protection within the internet gateway can detect malicious code.
- Secure configuration – remove unnecessary software and default user accounts. Change default passwords and ensure automatic features that could activate malware are turned off.
- User access – restrict the applications, privileges and data that users can access.
- User training – valuable in reducing the likelihood of successful social engineering attacks.
- Device controls – prevent unauthorised access to critical services or inherently insecure services that may still be required by the business.

Affect stage

- Planned controls for a bespoke capability attack – whereas the aforementioned controls can combat attacks using commodity (known) capabilities they are likely to be less effective against new malicious code or ‘zero day’ exploits.

Developing an incident response and disaster recovery capability (planning for the worst)

The NCSC has made clear that all SMEs can expect to experience a cybersecurity incident at some point and, ”*investment in establishing effective incident management policies and processes will help to improve resilience, support continuity, improve customer and stakeholder confidence and potentially reduce any impact*.”

Planning a cybersecurity incident response capability requires good preparation and a comprehensive review of the state of readiness of your business.

In terms of response, each incident will necessitate a proportionate response – overreacting can be detrimental.

The designated member(s) of staff should:

- Verify the breach and work to contain and then eradicate it.
- Confirm the extent of the breach and the data/services which have been affected.
- Identify the risks arising to the business and others from the breach.
- Implement any recovery of data via back-up files and recover any systems and connectivity.

In addition to keeping other members of the business apprised (ensuring media dialogue is co-ordinated through one person/team operating under legal advice), relevant parties who may need to be informed include the Police/Action Fraud; Banks/Credit Card Companies; Regulators (note the 72hr reporting deadline under GDPR 2018)/Insurers (SRA in the case of Solicitors) and potentially ‘Data Subjects”.

Litigation risk will need to be assessed and once matters have been addressed your business will need to conduct a structured review and lessons learned exercise.

Deception Technology

In recognition of the fact that no organisation can mount a perfect digital defence some businesses are reported as having employed deception technologies to hide their valuable data i.e. creating a shadow network to divert and mislead the malicious intruder into wasting their valuable resources.

Top 5 Corporate Endpoint Security Leaders

At the time of writing the International Data Corporation (IDC) has identified the following suppliers, prioritised by market share:

1. *Symantec* – (Head Office: USA) the company has recently reduced the number of versions of its Norton Antivirus line for SMEs.

2. *Intel Security* – (Head Office: USA) formerly McAfee.

3. *Trend Micro* – (Head Office: Japan) in 2015 the company funded research into 500 UK SMEs which revealed only 18% thought they had data worth stealing.

4. *Sophos* – (Head Office: UK) the company has placed an emphasis on serving the needs of SMEs.

5. *Kaspersky Lab* – (Head Office: Russia) the company is developing a US federal arm to bid for US government contracts.

To build an effective IP cybersecurity resilience for your business may require the selection and management of external suppliers beyond just malware protection. External support for a cybersecurity incident response, as well as STAR (Simulated Targeted Attack & Response) penetration testing, can be provided by UK approved member firms of CREST (visit www.crest-approved.org). In the alternative, the following pages list firms recommended by the North & South Wales Cybersecurity clusters.

5 lessons you can learn the easy way

- You may not be able to stop your business becoming a target for cybercriminals but there is a lot your business can do to protect itself from becoming the victim of cybercriminals.

- Programmes which have not been updated are the number one route used by cybercriminals to ‘hack’ businesses. Using pirated software, inadvertently or otherwise, exposes your business to far greater digital risk.

- Working on the move is now part of everyday life and cybercrime is increasingly directed towards mobile devices. Using unprotected wi-fi (e.g. public wi-fi in coffee shops & airports etc.) carries an increased risk of your data being intercepted.

- Users can be a significant source of vulnerabilities. Using the same password in both a professional and private context should be avoided. However strong it may have been, a compromised password used for multiple purposes can lead to an even bigger security breach.

- Trusted sources cannot always be trusted as they may have been compromised. It is becoming ever more difficult to identify baiting emails under ‘spear-phishing’.

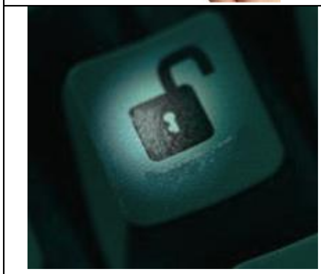
Firms which can support your business to acquire Cyber Essentials & Cyber Essentials Plus:

Wolfberry	Vendor neutral, 100% client focused. Wolfberry can identify the weaknesses in your ICT system, which will help you better understand how to protect what needs protecting. We pride ourselves on being a professional and ethical company, we feel that the integrity of the services we provide is vital, as a result we do not deliver general IT services, these are provided by your existing IT team, nor do we sell software or hardware solutions, we provide a framework that will enable your ICT systems to become secure, working with you to reduce your exposure to cyber risk, so you can rest assured that the advice we give is in the best interest of your company. For more information please contact Damon Rands, 07809 482185, drands@wolfberry.uk.com
ACCELERODIGITAL BUSINESS ALIGNED SOFTWARE	At Accelero Digital our mission is simple: to use our extensive software development experience to deliver tangible business results enabling our clients to profit from the advanced use of technology. Using our innovative EnGenero platform, we are able to develop bespoke, data-driven applications in less time with higher quality. EnGenero enables systems to be built securely as standard, delivering consistent outcomes in which our clients can have confidence. We provide training in good cyber security practices and steps to achieving certification, helping organisations to defend against data breaches and attacks. Accelero also performs information assurance audits that allow our clients to demonstrate their cyber security compliance. For more information please contact Huw John, 01656 648200, huw.john@accelero-digital.com
Arcanum CYBER SECURITY	Arcanum IS Ltd provides independent specialist security services through the G-Cloud for your Public Service Network (PSN). All of our security consultants are security cleared, UK based and most are CLAS registered. We have considerable experience and expertise in providing: Security Accreditation Services for IL2-IL6 networks; Technical Security Risk Assessments; Risk Management and Accreditation Document Sets; Privacy Impact Assessments; Risk Balance Cases; HMG Information Assurance Standards & Policy advice including the Security Policy Framework & CESG Standards & Policy; Security Audits to ISO 27001; Secure Architecture Design; Computer Forensics; Security Incident Management; Security Requirements; Business Continuity Planning; IT Health Checks, Penetration Testing and reports; Physical Security Surveys and Reports. For more information please contact Russ Wardle, 01558 669 140, russ.wardle@arcanumis.com
Astrix™	Whilst a great deal of technology is focused on improving our lives for the better, unfortunately there are those whose agenda is about creating chaos and disruption where ever and when ever they can. At Astrix our focus is about creating a safe and stable environment for businesses to thrive and prosper and that means IT security is an essential part of business contingency planning. Talk to us about arranging a free consultation about your IT contingency planning requirements today! For more information please contact Mostyn Thomas, 0845 22 66 572, mostyn.thomas@astrix.co.uk
Systemau Gwybodaeth BOYNS.NET Information Systems	Boyns Information Systems Ltd. is a supplier of IT related Products and Services and both a Managed Service Provider (MSP) of equipment and a Support team to our Customers' staff. We support equipment supplied by us and inherited from other suppliers. Trading since 1996 and incorporated in 2003. We are both an ISO 9001 and a CompTIA Trustmark Plus regulated company. Products and Services we Supply and Support in summary include (detailed in other sections): Computer Networks (Servers, Computers, Printers, Switches, Firewalls, Routers, Managed Wireless, Cabling etc..); Computer Hardware (PC's, Laptops, Tablets etc..); Hardware Repair and Upgrade Service – We offer a comprehensive repair of B2B, B2C and B2E computers laptops and peripherals; Cloud Based Services (Email – Office 365, Hosted Servers, Websites and Hosting etc..)l Disaster Recovery and Business Continuity Services; Telephone, EPOS and CCTV Systems
CAPITAL NETWORK SOLUTIONS	We provide innovative business enabling IT solutions and services that increase productivity, increase security, reduce costs and increase revenue. CNS works with many enterprise class customers supplying network and communications solutions and supporting them via our Managed Services portfolio on a 24x7 basis. We understand the constant drive for cost savings, increased productivity, world class customer service and innovation and are able to develop the appropriate technical solution to address the business challenges. For more information please contact Mark Edwards, 0845 305 4118, mark.edwards@capitalnetworks.co.uk
Morgan&Morgan IT & Telecoms Division	With over twenty years' industry experience, Morgan and Morgan offer unrivalled knowledge and expertise when it comes to providing IT solutions for 21st century businesses. We recognise that every business is unique, with its own set of objectives, its own structure, processes and people. Every solution we deliver is bespoke, designed with your business in mind. By offering complete, tailor-made IT solutions we have built up strong business relationships with private and public sector organisations across the UK. Our growth and success is based on providing clients with detailed advice and direction, backed up with quality products and first class service. For further information, please contact Michael Morgan on 01269 842242 or email: michael.morgan@mmbt.co.uk
PiSYS.net	Pisys.net is an award-winning IT support company providing honest and reliable IT support services to business of all sizes across the UK. We are certified partners with a number of global brands including Microsoft, IBM and Dell. This industry recognition is core to our business, enabling us to offer quality and cost-effective IT support services founded on the reliability of the world's leading software and hardware providers. With offices in Swansea and Aberdeen, our IT support services cover the whole of the UK. So whether you're looking for IT support in Scotland, South Wales or anywhere in between, cast your net over Pisys.net. For more information please contact Steve Bain, 01792 46 47 48, steve@pisys.net

Safonda	Safonda Limited was formed in Ruthin, North Wales by Rob Boyns and Jason Davies with the sole purpose of helping SMEs to secure their data and protect themselves from IT based threats to their businesses. With over 30 years of combined experience in the IT and Information Security industries, Rob and Jason have built solid reputations through their individual companies (Boyns Information Systems and Hashtag Marketing) for delivering high quality and easy to understand services. In addition to their professional endeavours in Cyber Security, Jason and Rob are also active members of the community helping to raise funds and support local projects as well as running the North Wales Cyber Security Cluster with the aim of helping to raise awareness as well as support businesses and professionals to increase their cyber security capabilities.
Wolfberry	Vendor neutral, 100% client focused. Wolfberry can identify the weaknesses in your ICT system, which will help you better understand how to protect what needs protecting. We pride ourselves on being a professional and ethical company, we feel that the integrity of the services we provide is vital, as a result we do not deliver general IT services, these are provided by your existing IT team, nor do we sell software or hardware solutions, we provide a framework that will enable your ICT systems to become secure, working with you to reduce your exposure to cyber risk, so you can rest assured that the advice we give is in the best interest of your company. For more information please contact Damon Rands, 07809 482185, drands@wolfberry.uk.com

Firms which can assist with an Incident Response & Disaster Recovery capability:

•888•Group•	888-Group Ltd specialise in Resilience, meaning your ability to maintain your business when faced with an event. Whether this be criminal or accidental it is our view that all events are foreseen and companies need to be aware and mitigate the possible effects. We can support with Health and Safety, Crisis Management, Security, Emergency Response, Business Continuity, Cyber Security and ISO Standards at 9001, 14001 and 27001. Our skills come from Senior levels in the Police and Olympics and Industry. For further information please contact Steve Gallagher +44 (0) 7969 975888, sgallagher@888-group.com
ACCELERODIGITAL BUSINESS ALIGNED SOFTWARE	At Accelero Digital our mission is simple: to use our extensive software development experience to deliver tangible business results enabling our clients to profit from the advanced use of technology. Using our innovative EnGenero platform, we are able to develop bespoke, data-driven applications in less time with higher quality. EnGenero enables systems to be built securely as standard, delivering consistent outcomes in which our clients can have confidence. We provide training in good cyber security practices and steps to achieving certification, helping organisations to defend against data breaches and attacks. Accelero also performs information assurance audits that allow our clients to demonstrate their cyber security compliance. For more information please contact Huw John, 01656 648200, huw.john@accelero-digital.com
AnturTeifi Building Better Business	As Telemat, Antur Teifi's , IT Support Service we are still leading the way having been awarded the prestigious IT Business Trustmark by Comp TIA for the quality of our service and plans for growth – one of only five businesses in Wales to have received this recognition during 2013. Our qualified bilingual IT Support technicians backed up by our Call Support Centre, work with many organisations ranging from small to large businesses, charities and the public sector throughout Wales. In addition we supply and install IT hardware & software, broadband, wired & wireless networks as well as offering a wide array of IT security and Cloud based services and products.
Arcanum CYBER SECURITY	Arcanum IS Ltd provides independent specialist security services through the G-Cloud for your Public Service Network (PSN). All of our security consultants are security cleared, UK based and most are CLAS registered. We have considerable experience and expertise in providing: Security Accreditation Services for IL2-IL6 networks; Technical Security Risk Assessments; Risk Management and Accreditation Document Sets; Privacy Impact Assessments; Risk Balance Cases; HMG Information Assurance Standards & Policy advice including the Security Policy Framework & CESG Standards & Policy; Security Audits to ISO 27001; Secure Architecture Design; Computer Forensics; Security Incident Management; Security Requirements; Business Continuity Planning; IT Health Checks, Penetration Testing and reports; Physical Security Surveys and Reports. For more information please contact Russ Wardle, 01558 669 140, russ.wardle@arcanumis.com
Astrix™	Whilst a great deal of technology is focused on improving our lives for the better, unfortunately there are those whose agenda is about creating chaos and disruption where ever and when ever they can. At Astrix our focus is about creating a safe and stable environment for businesses to thrive and prosper and that means IT security is an essential part of business contingency planning. Talk to us about arranging a free consultation about your IT contingency planning requirements today! For more information please contact Mostyn Thomas, 0845 22 66 572, mostyn.thomas@astrix.co.uk
Systemau Gwybodaeth BOYNS•NET Information Systems	Boyns Information Systems Ltd. is a supplier of IT related Products and Services and both a Managed Service Provider (MSP) of equipment and a Support team to our Customers' staff. We support equipment supplied by us and inherited from other suppliers. Trading since 1996 and incorporated in 2003. We are both an ISO 9001 and a CompTIA Trustmark Plus regulated company. Products and Services we Supply and Support in summary include (detailed in other sections): Computer Networks (Servers, Computers, Printers, Switches, Firewalls, Routers, Managed Wireless, Cabling etc..); Computer Hardware (PC's, Laptops, Tablets etc..); Hardware Repair and Upgrade Service – We offer a comprehensive repair of B2B, B2C and B2E computers laptops and peripherals; Cloud Based Services (Email – Office 365, Hosted Servers, Websites and Hosting etc..)l Disaster Recovery and Business Continuity Services; Telephone, EPOS and CCTV Systems
CAPITAL NETWORK SOLUTIONS	We provide innovative business enabling IT solutions and services that increase productivity, increase security, reduce costs and increase revenue. CNS works with many enterprise class customers supplying network and communications solutions and supporting them via our Managed Services portfolio on a 24x7 basis. We understand the constant drive for cost savings, increased productivity, world class customer service and innovation and are able to develop the appropriate technical solution to address the business challenges. For more information please contact Mark Edwards, 0845 305 4118, mark.edwards@capitalnetworks.co.uk
COAST CONSULTANTS IT FOR SOUTH AND WEST WALES	Coast Consultants is a nineteen year old IT consultancy specialising in software development projects, based in Saundersfoot, Pembrokeshire, in West Wales with many year's experience of helping local businesses with their IT. Coast was formed in 1993 after Stephen John had spent 10 years working for ICL (the UK's largest computer company at the time) so that he could have more say in the projects and locations that he wanted to work in. Specialist areas include Business Continuity - how to make sure your business survives anything from a computer failure to flooding of the premises?, Data Security - How safe is your business data and how secure are your staff procedures in the changing, mobile world of IT?, and Client Retention - are you spending lots of time and effort looking for new clients when you could be getting extra business from your old ones? For more information please contact Steve John, +44 (0)1834 814 814, steve@coast-consultants.co.uk

CiT IT SERVICES	Crystal IT Services Limited was formed by Chris Benson and Alan Jones to provide a quality layered service for businesses in the Vale of Glamorgan. Both directors have a passion for computers and have over 50 years experience between them in the IT service industry. They are committed to providing your business with Total Customer Service. Crystal-IT provides a first class pro-active and pre-emptive maintenance service for your computer system, supplying and installing quality components and peripherals, or even building a bespoke system to meet your exact requirements. For more information please contact Chris Benson, 01446 731 231, chris@crystal-it.co.uk
CyberCSI	CYBERCSI provides assistance in the investigation of online Cyber Crime. Offering advice and support when nobody else seems to want to know. We have experienced detectives and analysts that can assist you getting your crime investigated in a timely manner. We offer assistance to the Police to put their investigation on track. We can report your crime to Action Fraud for you, giving the relevant information they require to find the suspect. For more information please contact Ian Darlington, 07809 683 419, ian.darlington@cybercsi.co.uk
	High Tech Investigations - You suddenly find a situation within your organisation that breaches security, internal policy or even criminality. You probably have systems in place to deal with such incidents. In many cases however, there is not the capability to deal with any element of digital storage media. The method of seizure of computers, disks, USB drives etc has to be handled in a manner that would stand to scrutiny IF the matter were to end up before a Criminal or Civil court, Tribunal or any subsequent counter action! You can view our free advice page for more information. Of course once digital media has been seized, it still has to be handled, viewed and evidenced using accepted methodology. Here at High Tech Investigations, we have a full understanding of recovering digital storage devices and the data held on them. Whether its 'fishing' for information, through to full evidential package, we can assure you of a fully professional service from start to finish.
LOGiC iT	Technology is a key part of your business, but if it's down and you don't have the right support, your business will grind to a standstill. This is where LOGIC IT step in, we believe in offering you the customer honest, transparent and reliable IT support: IT Support – Reliable support all day and night to keep your business operational; Consultancy – Policy and advice to meet your business objectives and plan for the future; Backup & Security – We automatically backup your critical data safely and help protect you from viruses and identify risks; Cyber Security – Here at LOGIC IT we offer an independent information security consultancy, we will offer advice on how to help you identify the correct security needs for your business; Cloud – We will introduce you to the Cloud and guide you through the different options, and deliver secure, flexible and scalable hosted solutions; Telecoms – We will guide you through the different options for Internet, mobile and landline communications, supplying a complete solution.
Morgan&Morgan IT & Telecoms Division	With over twenty years' industry experience, Morgan and Morgan offer unrivalled knowledge and expertise when it comes to providing IT solutions for 21st century businesses. We recognise that every business is unique, with its own set of objectives, its own structure, processes and people. Every solution we deliver is bespoke, designed with your business in mind. By offering complete, tailor-made IT solutions we have built up strong business relationships with private and public sector organisations across the UK. Our growth and success is based on providing clients with detailed advice and direction, backed up with quality products and first class service. For further information, please contact Michael Morgan on 01269 842242 or email: michael.morgan@mmbt.co.uk
NETERIX	Neterix work in the areas of IT security, networking and software development. We provide a variety of services for organisations of all sizes, including ISO 27001 consultancy, ISMS audits, network design and testing, WiFi hotspots, data recovery and training.
Nibble IT Solutions	Nibble IT personally design, develop and implement our specialist servers and networks created specifically for our clients. We ensure continuous up time and high availability from within our secure networks. We spend time to ensure the components we install into your server and equipment used in your networks will cope with your business workload two times over. We all so include redundancy within your server hard drives ensuring if a drive fails your information is safe.
Option 13	We can help resolve your Information Security problems, whether you're just starting out, or you have an established Information Security programme. Problems we can solve include: Building an Information Security Management System, including risk assessment, risk analysis and risk management, and integrating it in to business as usual; ISO 27001 compliance requirements; PCI DSS compliance requirements; Cyber Essentials compliance requirements; Incident response, business continuity and disaster recovery planning; Information Security awareness training implementation and delivery
pescado	Pescado can put comprehensive IT security services in place for your business to prevent security issues and put you in a strong position. We will start by looking at your systems and identifying any potential weaknesses. We will put practical IT security solutions in place, such as spam filters to prevent those nuisance emails from landing in your inbox, and firewall solutions to protect your networks and critical data from any web security attacks. If the unthinkable has happened and you don't have the right network security in place, we can provide virus removal support. Once the problem is solved, we'll be happy to advise on hardware and software solutions to prevent it from happening again.

PiSYS .net	Pisys.net is an award-winning IT support company providing honest and reliable IT support services to business of all sizes across the UK. We are certified partners with a number of global brands including Microsoft, IBM and Dell. This industry recognition is core to our business, enabling us to offer quality and cost-effective IT support services founded on the reliability of the world's leading software and hardware providers. With offices in Swansea and Aberdeen, our IT support services cover the whole of the UK. So whether you're looking for IT support in Scotland, South Wales or anywhere in between, cast your net over Pisys.net. For more information please contact Steve Bain, 01792 46 47 48, steve@pisys.net
Safonda	Safonda Limited was formed in Ruthin, North Wales by Rob Boyns and Jason Davies with the sole purpose of helping SMEs to secure their data and protect themselves from IT based threats to their businesses. With over 30 years of combined experience in the IT and Information Security industries, Rob and Jason have built solid reputations through their individual companies (Boyns Information Systems and Hashtag Marketing) for delivering high quality and easy to understand services. In addition to their professional endeavours in Cyber Security, Jason and Rob are also active members of the community helping to raise funds and support local projects as well as running the North Wales Cyber Security Cluster with the aim of helping to raise awareness as well as support businesses and professionals to increase their cyber security capabilities.
Secti Limited	Experience providing enterprise level IT Security. Specialising in routing and firewall management, PCI compliance, penetration testing, data loss prevention, project and risk management and systems deployment. Consultancy services available for both short and long term engagements
silcox INFORMATION SECURITY	Silcox Information Security is a small and specialist information security consultancy and one of the UK's foremost information security consultancies. We specialise in a multi-disciplinary and holistic security management solutions for Cyber Security, HMG Information Assurance and Business Continuity. We have a demonstrable record of successful certifications and accreditations to date. The company was formed in 2005 by Paul Silcox who over the years has been joined by a close-knit team of trusted, highly qualified associates. For more information please contact Paul Silcox, 01446 728 258, paul@information-assurance.co.uk
SteerIT STRAIGHT FORWARD SOLUTIONS	All IT support companies are technical. What makes us different is we are experts who are great at communicating with our customers, we believe that makes us the company to use. We're friendly, approachable people – we just happen to be very passionate about IT! And after a thorough appraisal of your IT infrastructure by our expert technicians, we're confident we'll know exactly how to take your business to the next level, and ensure its security, uptime and productivity for a long time to come. We believe we offer the best business IT support in the South Wales Area. Let us prove it! Some of our areas of expertise are:- Managed IT Solutions, Microsoft and Apple Certified Engineers, Server Solutions, GDPR Consultation and Implementation, Network Security, Disaster Recovery and Business Continuity. Contact on 02920 348877 or solutions@steerits.co.uk
team:work making ICT : work for you	Teamwork ICT is an independent affiliation that provides strategic and operational support to enable SMEs to utilise ICT (Information Communication Technology) both effectively and efficiently. Based in Wales but with clients across the whole UK, we ensure that your ICT investment will provide tangible business benefits. Teamwork ICT will be with you every step of ICT implementation, from conception to operation. With us, you will gain a dependable and trusted business partner. In addition, Teamwork ICT can identify appropriate funding or subsidies programmes that be used to partially cover of your business' ICT implementation costs. For more information please contact Lee Turner, 08000 803 003 or 07977 092 535, lee.turner@teamworkict.com
Wolfberry	Vendor neutral, 100% client focused. Wolfberry can identify the weaknesses in your ICT system, which will help you better understand how to protect what needs protecting. We pride ourselves on being a professional and ethical company, we feel that the integrity of the services we provide is vital, as a result we do not deliver general IT services, these are provided by your existing IT team, nor do we sell software or hardware solutions, we provide a framework that will enable your ICT systems to become secure, working with you to reduce your exposure to cyber risk, so you can rest assured that the advice we give is in the best interest of your company. For more information please contact Damon Rands, 07809 482185, drands@wolfberry.uk.com