POLICING
YORKSHIRE & THE HUMBER
REGIONAL CYBER CRIME UNIT

Yorkshire and Humber Regional Cyber Crime Unit

(West Yorkshire, North Yorkshire, South Yorkshire and Humberside)

Guidance on protecting your business pre and post cyber-attack

Owner; Detective Chief Inspector Vanessa Smith

Author(s); Lisa Drayton – Regional Cyber Crime Unit Intelligence Analyst

Created; December 2016

This document is designed to be guidance for your business only and should **not** be taken as definitive instructions that must be implemented. This information is intended to assist in minimising the risk to your business from a cyber-attack but the implementation of any of the details in this document are not definitive methods for preventing any cyber-attack.

Foreword

Dear Local Business,

Following your cyber-crime report to Action Fraud, The Yorkshire and Humber Regional Cyber Crime Unit (Y&H RCCU) would like to supply you with information which provides comprehensive advice and guidance to your business, which if implemented ***may*** *reduce the risk of your company becoming a victim of cyber-crime in the future. The link to the online guidance is http://www.yhrocu.org.uk/home/protect-yourself.aspx. Alternatively, if you would like a copy emailing please contact us on yhcyberprotect@westyorkshire.pnn.police.uk*

Cyber-crime is ever evolving and criminals are capitalising on vulnerabilities within companies, and indeed in existing technology, for their own criminal gains. By adopting some or preferable all the measures contained in this document, relating to the 10 Steps Cyber Security, you ***may*** *minimise the risk of your business becoming a repeat victim. The implementation of cyber security measure may help to safeguard your business information technology and protects your staff and customers.*

Y&H RCCU also invite you to become a member Cyber–security Information Sharing Partnership (CiSP). This is a joint industry and government initiative set up to exchange cyber threat information in real time, in a secure, confidential and dynamic environment, increasing situational awareness and reducing the impact on UK business. This service is free of charge. For further details about the CiSP please go to www.ncsc.gov.uk/cisp.

Victim Support is an independent charity offering free, confidential support to people affected by crime (including cyber-crime), and traumatic incidents. Whilst Victim Support can't compensate you for your financial loss, they may be able to provide support and practical advice that will help you to move beyond the crime, even where you decide not to report the matter to the Police or Action Fraud.

To contact Victims Support please visit the charity's website at victimsupport.org.uk or call the Victim Support team for free and confidential information and support on 0300 303 1971.

Yours Sincerely

Yorkshire and Humber Regional Cyber Crime Unit.

http://www.yhrocu.org.uk/home/protect-yourself.aspx www.victimsupport.org.uk

https://www.ncsc.gov.uk/

For more information please contact; yhcyberprotect@westyorkshire.pnn.police.uk

Introduction

A large number of businesses rely on the internet and computer systems to conduct their daily business. Protecting the information which is held on a business's computer systems is critically important to the sustainability of the business. There are a number of methods that can be used to protect the data held by your business such as;

- Ensure your business has online and physical security for devices and computer systems
- Restrict user privileges
- Ensure that staff are educated on the potential risks to your businesses data and computer systems
- Have a business continuity plan which is rehearsed regularly
- Back up your data regularly

Being prepared for a cyber-attack and putting security measures in place in the first instance could be better for your business than becoming the victim of a cyber-attack. However, implementing security measures for your business is not a guarantee that your business will not be a victim of a cyber-attack.

This document is intended to highlight the different security measures which could be implemented by your business to improve the security of your business before and after a cyber-attack.

Top Tips

A number of security measures on protecting your business are highlighted within this document. However, the top 10 tips relating to protecting your business are summarised below;

1. **Secure configurations** - Use strong passwords with at least 8 characters long which contain upper and lower case letters, numbers and special characters such as # or $ and change any default passwords.
2. **Monitoring and backups**- Back up all of your computer systems and data regularly and monitor traffic coming in and out of you network.
3. **Incident management** - Ensure that your business has a business continuity plan which has been practiced and is kept up to date.
4. **Manage user privileges**- ensure that user privileges are restricted to minimise the risk.
5. **Removable media controls** - Limit the types of removable media that can be used.
6. **Malware protection** - Use encryption to protect your data from cyber-attacks such as malware.
7. **Information risk management** - Be aware of legislation and data protection laws which affect your business.
8. **Network Security** - Ensure that antivirus software and firewalls are installed and kept up to date.
9. **User education and awareness** - Employee education about the risks and awareness of cyber-crime.
10. **Home and mobile working** - Know how to protect the physical and online security or your computer systems and devices.

Passwords

Passwords are used to access a number of services, such as online banking, but passwords are also used to access devices. Many devices, such as routers, come with a default administrative password which are easily obtainable through online searching. It is essential to change all default passwords on all devices and computer services.

When choosing passwords try to make them as difficult as possible to guess or crack. Try to avoid using full words or words relating to your business. Passwords should be a minimum length of 8 characters with a combination of upper and lower case letters, numbers and special characters for example R35b@cPe%

Do not use the same password on different devices or accounts and change the password regularly. Try to make your passwords memorable so that you do not have to write them down.

System back up

The data which is held on your businesses computer systems and devices is very important and may be irreplaceable. It is vital to ensure that the data and systems used by your business are backed up frequently and stored independently from your network. In the event that your systems become encrypted and a ransom to decrypt your data is received, rather than paying the suspect you could restore your data from a previous back up. However, this scenario can only be utilised if your business has frequently backed up the data. Checks need to be performed to ensure that backups can be run correctly in the event of a cyber-attack.

There are a number of methods which can be utilised to ensure that your business has sufficient backups of data such as portable hard drives and online backups such as the cloud. When considering utilising a method of backing up data it is important to determine which would be the best method for your business in the event of total loss of your data.

Insider threat

A potential risk to your business is an insider threat which is the potential for a current or former employee, contractor or business partner to accidentally or maliciously misuse their trusted access to harm the business' employees, customers, assets, reputation or interests[1]. It is important to have a contingency plan which is continuously assessed to detect potential insider threats. The impact of an insider threat capability not only depends on technology but also processes and people. There are a number of insider threats that could occur with different intents. For example an employee may accidentally leak sensitive data but not for a hostile reason and another employee could have a hostile intent to use stolen sensitive data to commit fraud or attempt to destroy a business' reputation. Insider threats are not limited to threats against digital data but can also include hard copies of data.

[1] http://resources.sei.cmu.edu/asset_files/WhitePaper/2015_019_001_451069.pdf

Online and physical security

Protecting your devices and computer systems online is equally as important as physically protecting your devices and computer systems.

A physical device such as a laptop, smartphone or server can be physically accessed to obtain data or install malicious software such as ransomware but they can also be damaged, lost or stolen causing a loss of data. It is important to ensure that all devices and computer systems have strong passwords, access to the devices and computer systems are limited and are suitably backed up. In the event of loss, theft or damage to the devices all passwords should be changed and the data restored from a previous backup.

Any computer that is used by your business that connects to the internet should have a firewall, either personal or hardware, installed and switched on at all times. A firewall can protect your business from cyber criminals gaining access to the computer and/or network and prevent your business computers from being infected with a variety of viruses.

Antivirus software should be utilised to examine both the inbound and outbound data from your business. A large number of viruses are detected and prevented by antivirus software but new viruses are constantly being created. By installing and keeping your antivirus software up to date you can reduce the risk of a cyber-attack. Antivirus software will not protect your business from criminal activity which is not related to a virus.

Most businesses use Wi-Fi as part of their IT network and it is essential to ensure that the wireless router is secure in order to ensure that there is no unauthorised access to the router. If a Wi-Fi router is accessed it can be used to intercept any information being sent by your business, reduce the speed of your Wi-Fi by taking up bandwidth and data allowance can be used. Ensure that any default Wi-Fi passwords are changed as well as removing the password which is printed onto the router to ensure that access to the router is restricted.

It is imperative to monitor the network traffic and user activity including inbound and outbound traffic. Audit logs of all events (every log in, IP addresses used, files opened etc.) should be created which will assist with detection and recovery from a cyber-attack.

Social media can be used by cyber criminals to obtain information about your employees and/or business in order to commit an offence such as phishing. Employees using personal and/or business social media accounts should be educated to ensure that minimal personal and business information is placed on social media. For example, employees putting their employment details and job role could assist cyber criminals in creating more convincing phishing emails by using this personal information.

Manage user privileges

It is key to restrict and manage who has access to data held by your business by physically restricting access, being able to monitor who had accessed the data, what has been accessed and when. Not only should you restrict who has access to your systems but also restrict what can be accessed, for example restrict what folders can be opened by employees and who has administration rights. Records of which files or folders have been accessed by which employee on what date and time and any alterations made should also be logged.

Each employee should have a unique username and password to gain access to the business computer systems which minimises the risk of access to a computer and/or network being gained by an unauthorised person(s). Password should be mandatorily changed frequently such as every 30 days.

The internet is often used by employees to assist in conducting the day to day work for a business however, there are risks with allowing employees unrestricted access to the internet from a business computer or network. An employee could unintentionally or intentionally download viruses such as malware, use social media inappropriately or become a victim of social engineering. An acceptable usage policy for employees whilst using business computers to access the internet should be considered and/or implemented. Employee awareness and training is important to make sure that they are aware of any potential risks to the business.

An employee can inadvertently infect a computer by inserting a Universal Serial Bus (USB) drive which subsequently installs a virus. Your business should consider restricting the use of USB ports and USB drives in order to minimise the risk of infecting a computer and also data theft. All removable media should be scanned before inserting into a business computer or conducting any data transfers i.e. on a stand-alone computer which is separate to your business network.

Education and awareness

As well as ensuring that employees are aware of the acceptable and unacceptable use of the internet whilst on business computers, considerations should be made to train employees about identifying potential risks of cyber-attacks such as phishing. It may be appropriate to have a cyber-crime awareness section as part of employee initial and continued training.

Employee education can be essential in minimising the risk and/or likelihood of a cyber-attack.

It may be pertinent to get external training for your employees if your business does not have the capability or knowledge to train employees internally.

Encryption

Encryption can be used to protect and threaten your business. In simple terms encryption works by 'scrambling' the original message so that only the person with the 'key' can read it. For example, encryption can be 128 bit which means that the key is a sequence of 128 bits making it difficult to crack. The implementation of encryption software is advised to be carried out by your IT department and the type of encryption should be in accordance with the needs of your business. Encryption should be considered for any removable media used by your business.

Ransomware is a form of malware that severely restricts access to a computer, device or file until a ransom is paid by the user[2]. The user will see a 'pop-up window' appear on screen which will inform the user that a ransom must be paid in order to unlock the computer, device or file. There are many different forms of ransomware including variants which accuses the user of conducting illegal activity. There are a number of different ways that a computer can be infected with malware;

- Inserting USB/CD/DVDs into the computer
- Clicking on malicious links on websites, emails, social media etc.
- Opening a malicious attachment
- Visiting a website which is corrupt

In order to minimise the risks from ransomware and other viruses, it is crucial to educate employees regarding the risk of opening attachments, clicking links, visiting untrusted websites and inserting any removable media into the computer. Keeping antivirus software up to date and ensuring that regular back-ups of your business' information are made will reduce the risk and impact of ransomware and viruses.

If your business has become the victim of a ransomware incident contact your IT department or a trusted IT security professional for further advice. Any ransomware incidents should be reported to the Police and Action Fraud.

[2] usa.kaspersky.com/internet-security-center/**definitions**/**ransomware**

IT infrastructure

The physical IT infrastructure that is used by a business is not always located in the same location as the business itself. It is important to have an understanding about how your businesses IT infrastructure is set up, where it is located, who is the provider and how you can access the IT or contact the providers. In the event of a cyber-attack how does the IT provider respond in and out of office hours? Your business should know as much information as possible about the IT infrastructure your business uses.

If your IT infrastructure is located outside the United Kingdom does your business have a service level agreement with the provider to abide by any requests for information by your business or law enforcement. For example, a remote storage provider in United States of America may not wish to provide any information, such as data logs, to law enforcement without court orders from their own courts not a UK court. However, if there is a service level agreement in place with your business they may provide the information to the business without going through court proceedings.

Some businesses use external companies for remote storage of their business data and it is fundamental to know the location of the remote storage. It is also key to know how often back-ups of your business data are conveyed to the remote storage. In the event of a cyber-attack how would your business get hold of the back-ups? If there is a single point of contact at the remote storage location do you know who to contact and the preferred means of contact such as email or telephone calls.

The set-up of your businesses IT structure, contacts, out of hours response etc. should all be included in a business continuity exercise and the information should be regularly refreshed.

Business Continuity Plans

Ensuring that your business can maintain ‘business as usual’ in the event of a cyber-attack is crucial. Any disruptions to your services, operations and ability to conduct business can have serious consequences such as reputational damage or financial loss. By protecting your computer based equipment and information from unintended or unauthorised access, change, theft or destruction it can minimise the effect of a cyber-attack and potentially enhance the reputation of your business.

When creating a business continuity plan it is essential to ensure that the critical business functions are identified and the potential risks to the business which are associated with the loss of these functions. For example, the critical business functions for a business which conducts all sales through a website would be the website, computer and customer data. The risks would be the loss of business due to the inability to use the website and/or computer and any loss of customer data could incur heavy fines from The Information Commissioners Office.

A business continuity plan should be tested to ensure that staff know what to do in the event of a cyber-attack and also to identify any vulnerabilities in the plan so it may be improved. A response to a wide variety of incidents should be established including protocols for data recovery, obtaining technical assistance and liaising with the media. If your business uses outside IT infrastructure, such as an external data centre, do you know where they are based, how to access the functions in the case of a cyber-attack and is there appropriate resilience? It is important to practice a business continuity plan internally but also with partner agencies such as IT support or the Police. When creating your business continuity plan the below mnemonic should be considered;

Strengths – *can your business be strengthened by implementing additional security?*

Weaknesses – *identify weaknesses in physical and virtual security*

Opportunities - *have any opportunities been missed to ensure the security of your data?*

Threats – *plan for all potential threats to your business to ensure you are prepared*

A delay in gaining full control of affected assets may lead to delays in restoring critical business functions and progression of enquiries to identify a suspect. The business continuity plan should clearly state to whom incidents should be reported and when. Considerations should be made to include a strategy of liaising with the media including distributing any press releases. A list of law enforcement and other agencies who can assist with dealing with a cyber-crime and offer advice is provided on page 19.

If your business does become the victim of a cyber-attack it is vital to review your business continuity plan post-attack to see if there are any disparities which could be resolved to reduce the risk of another cyber-attack.

Business Continuity Exercises

In addition to implementing a business continuity plan it is imperative to conduct a business continuity exercise to ensure that the business continuity plan is fit for purpose and any disparities in the plan are identified.

A business continuity exercise should be devised to include areas such as;

- Who will be aware of the exercise prior to its commencement?
- The type of cyber-attack being simulated such as initial contact from a suspect or Distributed Denial of Service (DDoS) attack.
- Time and date the exercise will begin and conclude.
- A summary outlining the purpose of the exercise.
- The intended disruption level (minor, intermediate or major).
- Any actions that are required including any scripts being used and any specific tactics.
- The expected outcome of the exercise.
- The actual outcome of the exercise.
- Any additional notes of comments.

Before a business continuity exercise is conducted the strategy for the exercise should be established. For example, a simulated cyber-attack is conducted by your businesses IT department and a member of staff rings your main reception to purporting to be the suspect advising your business of the attack. Besides senior management and the IT department no one else in the business is made aware of the exercise. Due to the internal knowledge of the business the management and IT department intentionally block the predetermined responses outlined in the business continuity plan to test the ability of your business to adapt. The strategies should be predetermined in the business continuity exercise plan.

It may be pertinent to create a ‘response group’ which is a group of people from specific departments such as management or IT, who will be the people involved in implementing business continuity plans in the event of a cyber-attack.

Media Policy

If your business becomes the victim of a cyber-attack it may be necessary to have a press release where information about the attack is provided to the public. This may include advising the public about the potential loss of customer data or reduction in services provided by your business. It is key to have a predetermined media policy for your business which outlines what information is provided to the media and by whom and policies regarding the need for a press release to be made. When creating a media policy and publishing any press releases there are a few essential points to consider such as;

- The impact the press release may have on your business.
- Does a press release need to be approved by senior management or board of directors prior to dissemination.
- How long after a cyber-attack should a press release be distributed?
- If customer data is lost are your customers contacted prior to a press release. If so, how are your customers to be contacted? Emails, Letters etc.
- How your business deals with the aftermath of the press release such as dealing with irritated customers making contact.
- Briefing your staff about the situation and ensure they know how to liaise with any media or customer queries.

If your business decides not to have a press release a clear and concise rationale should be documented as to why your business made this decision, including a potential review of the decision at a later date.

Any media policies should be included on your business continuity plans.

Bring your own devices (BYOD)

Bring your own devices (BYOD) is the practice untaken by businesses to allow their employees to bring and use their own device such as laptop or removable media into the workplace. BYOD can offer both benefits and risks to your business and the implementation of a BYOD policy may be required which is specifically tailored to your business.

BYOD can provide a number of benefits to your business such as increased working time flexibility and efficiency. However, BYOD can also raise a number of risks and data protection concerns such as;

- Ensuring that there is an acceptable usage policy on all devices in order to protect personal data.
- The device is owned by the employee not the business.
- Any personal data being processed on an employee's personal device must still be in compliance with the Data Protection Act 1998.
- Do the devices have appropriate security capabilities?
- The type of data being held and where it is stored.
- Theft of data by an employee or loss of data if the device is lost or stolen.
- Personal and business use of devices becoming distorted and potential non-compliance with acceptable usage policies.

Your business should consider whether a BYOD system is suitable for your business practices. The security of BYOD's is important, as employee devices may not have suitable security for your business and should also comply with other legal aspects such as Freedom of Information Act 2000. Data Protection Act and acceptable usage polices are also vital factors to consider when establishing using BYOD for your business.

BYOD will always have a personal element as the device belongs to the employee and they will use the device for personal business. It is imperative to ensure that an employee's personal usage remains personal. However, it is essential to be able to monitor and audit employee access and usage. The Information Commissioners Office has published guidance regarding BYOD in the ICO's Employment Practice Code[3].

For further information regarding BYOD read the Information Commissioners Office guidance on bring your own device; https://ico.org.uk/media/for-organisations/documents/1563/ico_bring_your_own_device_byod_guidance.pdf

[3] https://ico.org.uk/media/for-organisations/documents/1064/the_employment_practices_code.pdf

Legislation

Your business should be aware of any legal aspects that affect the management of your business such as the Data Protection Act 1998. The Information Commissioners Office role is to uphold information rights in the public interest and has the power to serve a monetary penalty notice on a data controller[4] if data protection is breached. For more information visit https://ico.org.uk/ and https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/

Data Protection Act 1998 is an act to make new provision for the regulation of the processing of information relating to individuals, including the obtaining, holding, use or disclosure of such information. It is designed to protect the privacy and integrity of data being held by businesses. The Data Protection Act has 8 principles which are guidelines for the best practice when handling personal data;

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless (a) at least one of the conditions in schedule 2 is met, and (b) in the case of sensitive personal data, at least one of the conditions in schedule 3 is also met.
2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
4. Personal data shall be accurate and, where necessary, kept up to date.
5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
6. Personal data shall be processed in accordance with the rights of the data subject under this act.
7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data[5].

The Data Protection Act also covers employee monitoring which should be proportionate and clearly communicated to employees.

[4] https://ico.org.uk/

[5] Police National Legal Database

Post cyber-attack

Any of the previously mentioned security measures can be implemented prior and post cyber-attack. However, some post cyber-attack implementation can be difficult. For example, if your business has not kept back-ups or regular back-ups of data your business may not be able to restore the information if it becomes encrypted.

Any post cyber-attack actions which need to be implemented will be specific to your business however, below there are a few examples of post cyber-attack actions;

- Contact your local Police force and Action Fraud to make a report.
- Contact your IT department for advice and assistance.
- Change the passwords on all accounts.
- Scan your devices using anti-virus and anti-spyware software.
- Eliminate any vulnerabilities which have been exploited by a cyber-criminal.
- Secure and preserve any evidence including logs of events.
- Stay vigilant.

Cyber-security Information Sharing Partnership (CiSP)

CiSP is a joint industry and government scheme based in CERT-UK. CiSP is an online social networking tool and enables its members to exchange information on threats and vulnerabilities as they occur. CiSP does not investigate any cyber-crimes and is purely an information sharing platform. There are a number of organisations who are part of CiSP and all levels of cyber experience are catered to. CiSP and Regional Organised Crime Units (ROCU's) have set up regional nodes on CiSP so that businesses can share vulnerabilities and/or threats from within their region.

There are a number of benefits that CiSP members can benefit from such as;

1. Engagement with industry and government counterparts in a secure environment
2. Early warning of cyber threats
3. Ability to learn from experiences, mistakes, successes of other users and seek advice
4. An improved ability to protect their company network
5. Access to free network monitoring reports tailored to your business' requirements

To become a registered CiSP member you must be a UK registered company or other legal entity which is responsible for the administration of an electronic communications network in the UK and/or sponsored by either a government department, existing CiSP member or a trade body/association.

CiSP

A CATALYST FOR COLLABORATION

For further information visit https://www.ncsc.gov.uk/

Cyber Essentials

The Cyber Essentials scheme provides small to large businesses from all sectors with information regarding good basic cyber security practice with the hope that businesses will be better protected. The Cyber Essentials scheme was developed as part of the UK's National Cyber Security Programme.

There are two levels that your business can apply for;

To find out more information about Cyber Essentials visit;
https://www.cyberstreetwise.com/cyberessentials/

Glossary

Anti-spyware software – A type of program designed to prevent and detect unwanted spyware program installations and to remove these programs if installed[6].

Anti-virus software - program or set of programs that are designed to prevent, search for, detect, and remove software viruses, and other malicious software[7].

CiSP - CiSP delivers a key component of the UK's cyber security strategy in facilitating the sharing of information on cyber threats in order to make UK businesses more secure in cyberspace[8].

CERT-UK – The UK National Computer Emergency Response Team formed in response to the National Cyber Security Strategy which set out the importance of strengthening the UK's response to cyber incidents[9].

Data centre - A data centre is a dedicated space where companies can keep and operate most of the ICT infrastructure that supports their business. This would be the servers and storage equipment that run application software and process and store data and content. For some companies this might be a simple cage or rack of equipment, for others it could be a room housing a few or many cabinets, depending on the scale of their operation[10].

Distributed Denial of Service (DDoS) – a method of attacking a computer systems by flooding it with so many messages that it is obliged to shut down[11].

Encryption – Encryption is the process of encoding messages or information in such a way that only authorised persons can read it[12].

Firewall – A firewall is a barrier between the internet and your computer or network which can prevent unauthorised visits to or egress from your systems[13].

Hardware Firewall - A firewall that is built into a router or a stand-alone device[14].

IT – Information Technology.

Information Commissioner's Office - role is to uphold information rights in the public interest and has the power to serve a monetary penalty notice on a data controller[15].

Malware – malware refers to software designed and distributed to gain unauthorised access to computers and other connected devices, disrupt their normal operation, gather sensitive or confidential information or spy on the device user(s)[16].

[6] http://whatis.techtarget.com/definition/anti-spyware-software

[7] https://www.webroot.com/in/en/home/resources/tips/pc-security/security-what-is-anti-virus-software

[8] https://www.gov.uk/government/news/government-launches-information-sharing-partnership-on-cyber-security

[9] https://www.cert.gov.uk/what-we-do/

[10] http://www.interxion.com/data-centres/

[11] http://www.collinsdictionary.com/dictionary/english/ddos

[12] https://en.wikipedia.org/wiki/Encryption

[13] https://www.getsafeonline.org/online-safety-and-security/firewalls/

[14] http://www.pcmag.com/encyclopedia/term/57774/hardware-firewall

[15] https://ico.org.uk/

[16] https://www.getsafeonline.org/online-safety-and-security/anti-malware/

Personal Firewall - Software installed in a user's computer that offers protection against unwanted intrusion and attacks coming from the Internet. Personal firewalls are available from numerous security vendors[17].

Phishing - A technique used to gain personal information for purposes of identity theft, using fraudulent e-mail messages that appear to come from legitimate businesses. These authentic-looking messages are designed to fool recipients into divulging personal data such as account numbers and passwords or credit card numbers.

Ransomware - a form of malware that severely restricts access to a computer, device or file until a ransom is paid by the user[18].

Social Engineering – A form of techniques employed by cyber-criminals designed to lure unsuspecting users into sending them their confidential data, infecting their computers with malware or opening links to infected sites[19].

[17] http://www.pcmag.com/encyclopedia/term/49135/personal-firewall

[18] usa.kaspersky.com/internet-security-center/**definitions/ransomware**

[19] https://usa.kaspersky.com/internet-security-center/definitions/social-engineering#.V72kpf72ZaQ

Contacts

Yorkshire and Humber Regional Cyber Crime Unit (Y&H RCCU)

The Yorkshire and Humber Regional Cyber Crime Unit is part of the Regional Organised Crime Unit providing specialist capability to the four forces within the Yorkshire and Humber Region to tackle the increasingly complex threat posed by organised crime.

POLICING
YORKSHIRE & THE HUMBER
REGIONAL CYBER CRIME UNIT

All incidents of cyber-crime should be reported to Action Fraud and your local Police force on 999 in an emergency and 101 in a non-emergency. The Y&H RCCU are happy to provide advice over the phone or by email but do not take crime reports directly.

If you would like to contact the Y&H RCCU please email; regional.cyber@westyorkshire.pnn.police.uk

For advice follow Y&H RCCU on Twitter; @YH_CyberProtect or Facebook https://www.facebook.com/YorkshireandHumberRCCU/ *(incidents cannot be reported on Twitter or Facebook*)

Action Fraud

Action Fraud is the UK's national fraud and cyber-crime reporting centre. All cyber-crime incidents should be reported to Action Fraud either online or by telephone. Action Fraud do not investigate crimes.

ActionFraud
Report Fraud & Internet Crime
0300 123 2040

Action Fraud work alongside the National Fraud Intelligence Bureau (NFIB) which is part of the City of London Police to identify established and emerging crime types as well as identifying organised crime groups. NFIB work alongside law enforcement to investigate crimes.

National Cyber Security Centre (NCSC)

The NCSC is part of the Government Communications Headquarters (GCHQ). The NCSC leads the UK's response to cyber-crime, supports partners with specialist capabilities and coordinates the national response to the most serious of cyber-crime threats. Working closely with the Regional Organised Crime Units (ROCUs), the public, organisations, partners within industry, Government and International Law Enforcement.

The NCSC do not take reports of cyber-crime directly and all reports must be reported to Action Fraud.

For further information on NCSC visit www.ncsc.gov.uk

CERT-UK

CERT-UK is the UK National Computer Emergency Response Team, formed in March 2014 in response to the National Cyber Security Strategy. The National Cyber Security Strategy, published in 2011, sets out the importance of strengthening the UK's response to cyber incidents.

CERT-UK has four main responsibilities that flow from the UK's Cyber Security Strategy:

1. National cyber-security incident management
2. Support to critical national infrastructure companies to handle cyber security incidents
3. Promoting cyber-security situational awareness across industry, academia, and the public sector
4. Providing the single international point of contact for co-ordination and collaboration between national CERTs

CERT-UK works closely with key partners to enhance the UK's ability to prepare for and manage national cyber-security incidents. This includes exercising with government departments and industry partners, sharing information with industry and academic computer emergency response teams and collaborating with national CERTs around the globe to enhance our understanding of the cyber threat.

CERT-UK works primarily with other CERTs and companies that own and manage the critical national infrastructure (CNI). Any reports of cyber-crime need to be made to Action Fraud or your local Police force.

For further information on CERT-UK visit https://www.cert.gov.uk/

Get Safe Online

Get Safe Online is the UK's leading source of unbiased, factual and easy to understand information on online safety. Get Safe Online do not investigate crimes.

GET SAFE ONLINE .org ®

www.getsafeonline.org

Expert advice for everyone

Crimestoppers

Crimestoppers are an independent charity helping law enforcement to locate criminals and help solve crimes but do not directly investigate crimes. Crimestoppers take anonymous reports.

CRIMESTOPPERS

0800 555 111

Victim Support

Victim Support is an independent charity offering free, confidential support to people affected by crime (including cyber-crime), and traumatic incidents. To contact Victims Support please visit the charity's website at victimsupport.org.uk or call the Victim Support team for free and confidential information and support on 0808 1689 111.

VS VICTIM SUPPORT

Questionnaire

Please indicate which security measures your business had implemented **prior** to a cyber-attack;

□ Implemented a business continuity plan

□ Conducted a business continuity exercise

□ Created a response group

□ Implemented a media policy

□ Have internal or external training for employees specifically relating to cyber-crime and cyber security

□ Use encryption on data

□ Use encryption on devices

□ Restrict user privileges

□ Restrict the use of removable media

□ Monitor network traffic (inbound and outbound)

□ Monitor user activity

□ Change default passwords

□ Change passwords regularly

□ Install and keep up to date antivirus software

□ Have a firewall (personal or hardware)

□ Back up data frequently

□ Store backed up data separately from your business network

□ Provide employees with cyber security advice and/or training

□ Became a CiSP member

□ Cyber Essentials certified

□ Aware of the law enforcement and partner agencies who can assist your business

Please indicate which security measures your business had implemented **after** a cyber-attack;

□ Implemented a business continuity plan

□ Conducted a business continuity exercise

□ Created a response group

□ Implemented a media policy

□ Have internal or external training for employees specifically relating to cyber-crime and cyber security

□ Use encryption on data

□ Use encryption on devices

□ Restrict user privileges

□ Restrict the use of removable media

□ Monitor network traffic (inbound and outbound)

□ Monitor user activity

□ Change default passwords

□ Change passwords regularly

□ Install and keep up to date antivirus software

□ Have a firewall (personal or hardware)

□ Back up data frequently

□ Store backed up data separately from your business network

□ Provide employees with cyber security advice and/or training

□ Became a CiSP member

□ Cyber Essentials certified

□ Aware of the law enforcement and partner agencies who can assist your business

Has this advice been helpful?

□ Yes

□ No

Please send any responses to regional.cyber@westyorkshire.pnn.police.uk