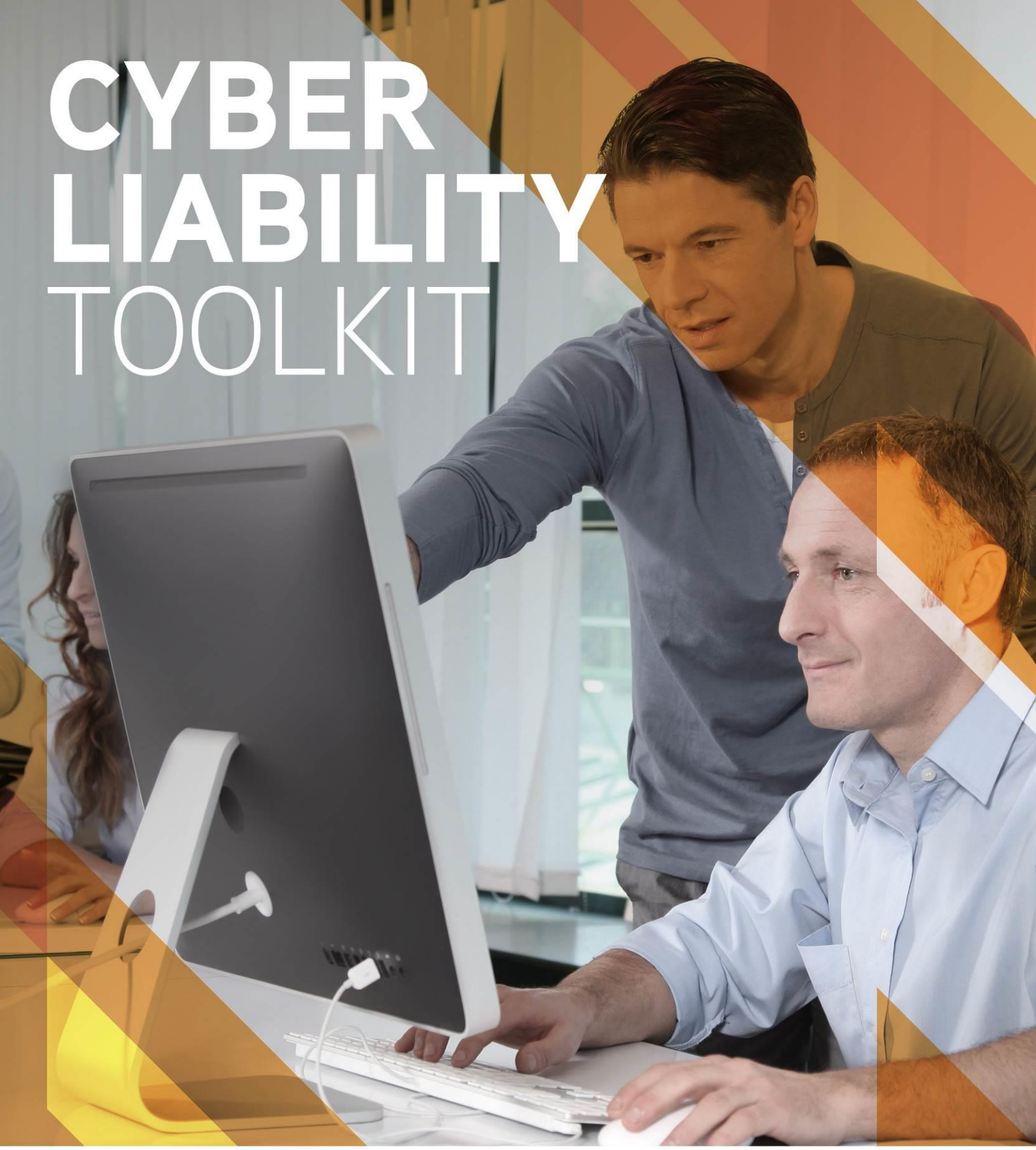
CYBER LIABILITY TOOLKIT



Crendon Insurance Brokers

Provided by: Crendon Insurance Brokers Ltd

The CIB A Building – 146 Hagley Road
Edgbaston, Birmingham, West Midlands, B16 9NX
0121 45 45 100
www.crendoninsurance.co.uk

How to Use This Toolkit

Businesses both large and small need to be proactive in order to protect against growing cyber threats. As larger companies take steps to secure their systems, smaller, less secure businesses are becoming increasingly attractive targets for cyber criminals.

This planning toolkit is designed to help employers protect their business, information and customers from cyber threats. This guide is not intended to be exhaustive nor should any discussion or opinions be construed as legal advice. It is generally recommended that businesses using sophisticated networks with dozens of computers consult a cyber security expert in addition to using this toolkit.

As you begin taking control of your cyber liability, use the checklist at the beginning of the toolkit and revisit it as you progress. You will also find sample policies at the end of the toolkit to help you implement your cyber liability initiatives.

Table of Contents

Getting Organised

Cyber Liability Toolkit Checklist 3-7

Understanding the Risks

Understanding and Responding to a Data Breach 8-10

Defining, Identifying and Limiting Cyber Crime 11-12

Spam, Phishing and Spyware Defined 13-14

Identifying and Managing Your Exposures

Data

Keeping Your Data Secure 15-16

Physical Protection of Cyber Assets 17-18

Devices

Mobile Device Security 19-20

Safely Disposing of Your Device 21-22

Systems

Network Security 23-24

Website Security 25-27

Protecting Your Email 28-29

Reducing Your Risks

Basic Loss Control Techniques 30-31

Managing Password Threats 32-34

Policies to Manage Cyber Risk 35-36

Protecting Against Online Fraud 37-38

Proper Employee Management to Reduce Occupational Fraud 39-40

Sample Policies

General Email/Internet Security and Use Policy 41-47

Data Breach Response Policy 48-50

Cyber Liability Toolkit Checklist

Complete the following checklist as you utilise the Cyber Liability Toolkit. This checklist serves as an outline and a reminder of the risks and issues your business should be monitoring. Work with your IT department to implement and update any policies and make sure all employees are trained on best practices.

UNDERSTANDING THE RISKS

UNDERSTANDING AND PREVENTING DATA BREACHES	YES	NO	NOTES
Can you define what a data breach is? Would you be able to recognise it if it occurred?			
Do you know your responsibilities and what actions you should take if a data breach occurs?			
Have you established organisation-wide procedures to isolate and contain the breach to limit damage, including conducting a risks assessment regarding the data that was compromised?			
Do you have procedures in place to notify affected parties and appropriate regulatory bodies?			
Do you regularly review your cyber security policies and procedures to make sure everything is up to date?			How often?

DEFINING, IDENTIFYING AND LIMITING CYBER CRIME	YES	NO	NOTES
Do you stay up to date on emerging cyber risks?			How?
Are you familiar with any computer intrusions, such as viruses, worms, Trojan horses, spyware and logic bombs?			List any computer intrusions you know of but are not familiar with:
Does your organisation use any of the following to limit intrusions? • Firewalls or routers • Antivirus programs • Policies			List :

SPAM, PHISHING AND SPYWARE DEFINED	YES	NO	NOTES
Do you have an email and internet usage policy?			

Are your employees trained to recognise electronic scams such as spam, phishing and spyware?			
Do you regularly remind or train employees to keep electronic scam prevention top of mind?			

IDENTIFYING AND MANAGING YOUR EXPOSURES: DATA

KEEPING YOUR DATA SECURE	YES	NO	NOTES
Have you identified what types of data your business holds and stores? This can include customer data, financial information, buying habits, preferences and much more.			List data types:
Have you classified your data into different categories to identify potential areas of vulnerability?			
Do you know where all of your data (including physical, website and virtual data) is stored?			Locations:
Have you assessed how secure your data transfer procedures and storage areas are?			
Have you established data access restrictions based on employee role?			
Do you use more than one security mechanism to protect your data?			List the mechanisms you use:
Is data backed up regularly to a secure location?			

PHYSICAL PROTECTION OF CYBER ASSETS	YES	NO	NOTES
Have you secured your organisation's facilities?			Methods:
Do you require badge identification for visitors?			
Do employee computer screens face away from public traffic?			
Do you use cable locks or tracking software to help prevent laptop theft?			
Have you established procedures to minimise and safeguard printed materials with sensitive information?			

Is your post/mail centre secure?			
Do you have procedures in place to properly dispose of papers containing sensitive materials?			
Do you have procedures in place to securely dispose of electronic equipment?			
Are your employees trained in all facility security policies and procedures?			

IDENTIFYING AND MANAGING YOUR EXPOSURES: DEVICES

MOBILE DEVICE SECURITY	YES	NO	NOTES
Do your mobile devices have complex passwords or PINs with time-sensitive, automatically locking security features?			
Are all mobile devices set to reject open Wi-Fi or Bluetooth connections without user permission?			
Have you established a Mobile Device Policy and trained employees on it?			
If you allow employees to use their own mobile devices, have you established a Bring Your Own Device Policy?			
Are all mobile devices kept updated with the most current software and antivirus programs?			
Is content from mobile devices backed up regularly?			

SAFELY DISPOSING OF YOUR DEVICES	YES	NO	NOTES
Do you have set procedures in place to properly remove information from and dispose of your devices?			

Do you use one or a combination of the following methods to dispose of your devices? • Physical destruction • Overwriting • Restoring to factory settings • Sending it to a specialist • Formatting			List methods used:

IDENTIFYING AND MANAGING YOUR EXPOSURES: SYSTEMS

NETWORK SECURITY	YES	NO	NOTES
Have all devices and connections on organisational networks been identified?			
Have boundary points been identified and evaluated to determine best security controls?			
Is the network separated from the public internet with strong user authentication mechanisms and policy enforcement systems such as firewalls and web filtering proxies?			
Are monitoring and security solutions such as antivirus programs and intrusion detection system used?			
If cloud-based services are used, have you consulted with your providers about the terms of service to ensure company information and activities are fully secure?			
Is your organisation's Wi-Fi secure and encrypted?			
Has all sensitive organisational data been encrypted?			
Are all systems, software and equipment updated in a timely fashion (including all patches and firmware upgrades)?			
If remote access is allowed, is it secured through a Virtual Private Network (VPN) and accompanied by two-factor authentication?			
Do you have a safe-use policy regarding flash drives?			

WEBSITE SECURITY	YES	NO	NOTES
Have you developed appropriate web management security practices and policies?			
Is a proper team assembled to manage the deployment and continued operation of the web server and supporting infrastructure?			
Do all web server operating systems and applications meet your security requirements? Are servers configured to meet your specific security needs?			
Do you employ a strategy to prevent inappropriate or sensitive information from being published on the website?			
Are there procedures in place to prevent unauthorised access or modification to the site?			

PROTECTING YOUR EMAIL	YES	NO	NOTES
Do you have a spam filter set up?			
When sending sensitive information through email, is the information properly encrypted?			
Do you have an email retention policy?			

Understanding and Responding to a Data Breach

No company, big or small, is immune to a data breach. Many small employers falsely believe they can elude the attention of a hacker, yet studies have shown the opposite is true. According to Verizon Communication's 2012 Data Breach Investigations Report, 72 per cent of the 855 data breaches analysed were at companies with 100 or fewer employees.

Data breach response policies are essential for organisations of any size. A response policy should outline how your company will respond in the event of a data breach, and lay out an action plan that will be used to investigate potential breaches to mitigate damage should a breach occur.

Defining a Data Breach

A data breach is an incident where personal data is accessed and/or stolen by an unauthorised individual. Examples of personal data include:

- National insurance numbers
- Credit card information (credit card numbers—whole or part, credit card expiry dates, cardholder names, cardholder addresses)
- Business identification numbers; employer identification numbers
- Biometric records (fingerprints, DNA, or retinal patterns and other measurements of physical characteristics for use in verifying the identity of individuals)
- Payroll information
- Medical information for any employee or customer (doctor names and claims, insurance claims, prescriptions, any related personal medical information)
- Other personal information of a customer, employee or contractor (dates of birth, addresses, phone numbers, maiden names, race, religious belief, sexual orientation, commission or alleged commission of an offence, etc)

Data breaches can be costly. According to PricewaterhouseCoopers' *Information Security Breaches Survey*, commissioned by the Department for Business, Innovation and Skills, the average cost to a small business for its worst security breach of the year is between £75,200 and £310,800. But that pales in comparison to the average cost to a large organisation for its worst security breach of the year—between £1.46 million and £3.14 million.

Responsibilities upon Learning of a Breach

The Data Protection Act 1998 and the Privacy and Electronic Communications (EC Directive) Regulations 2003 and subsequent amendments establish requirements that organisations must follow concerning data protection. A breach or a suspected breach of personal information must be immediately investigated. Since all personal information is of a highly confidential nature, only personnel necessary for the data breach investigation should be informed of the breach. The following four elements should be included in any breach management plan:

1. **Containment and Recovery**

   Establish procedures to isolate and contain the breach in order to limit the damage. Consider whether there is anything you can do to recover any of the breached data or equipment. Once basic information about the breach has been established, management should make a record of events and people involved, as well as any discoveries made over the course of the investigation to determine whether or not a breach has occurred.

2. Assessment of the Risks

Once a breach has been verified and contained, perform a risk assessment that rates the:

- Sensitivity of the personal information lost (customer contact information alone may present a smaller threat than financial information)
- Amount of personal information lost and number of individuals affected
- Likelihood personal information is usable or may cause harm
- Likelihood the personal information was intentionally targeted (increases chance for fraudulent use)
- Strength and effectiveness of security technologies protecting personal information (eg, encrypted personal information on a stolen laptop, which is technically stolen personal information, will be much more difficult for a criminal to access)
- Ability of your company to mitigate the risk of harm

3. Notification of the Breach

Responsibility to notify individuals, the Information Commissioner's Office (ICO) or appropriate regulatory body depends on the sector your organisation is in, type of data accessed, and the individual circumstances of the data breach. Any information found in the initial risk assessment should be turned over to the appropriate legal professional of your company who will review the situation to determine if, and to what extent, notification is required. Notification should occur in a manner that ensures the affected individuals will receive actual notice of the incident. Notification should be made in a timely manner, but make sure the facts of the breach are well established before proceeding.

In the case that notification must be made:

- Only those that are legally required to be notified should be informed of the breach. Notifying a broad base when it is not required could raise unnecessary concern in those who have not been affected.
- A physical copy should always be mailed to the affected parties no matter what other notification methods are used (eg, phone or email).
- A help line should be established as a resource for those who have additional questions about how the breach will affect them.

The notification letter should include:

- A brief description of the incident, the nature of the breach and the approximate date it occurred.
- A description of the type(s) of personal information that were involved in the breach (the general types of personal information, not an individual's specific information).
- Explanation of what your company is doing to investigate the breach, mitigate its negative effects and prevent future incidences.
- Steps the individual can take to mitigate any potential side effects from the breach.
- Contact information for a representative from your company who can answer additional questions.

4. Evaluation and Response

It is important for you to investigate the causes of the breach and the effectiveness of your response to it. Identify and review your existing policies and procedures to see where improvements can be made to prevent future data breaches.

For more information on how to respond to a data breach, please visit the Information Commissioner's Office at www.ico.gov.uk.

Insurance is Important

Chances are your company doesn't have funds saved to pay for data breach remediation. Fortunately, there are insurance options available to make recovery easier. Cyber liability insurance policies can cover the cost of notifying customers and replace lost income as a result of a data breach. In addition, policies can cover legal expenses a business may be required to pay as a result of the breach.

Defining, Identifying and Limiting Cyber Crime

A vast amount of information is now stored on computer servers and databases, and it's growing every day. Because that information has great value, hackers are constantly looking for ways to steal or destroy it.

Cybercrime is one of the fastest growing areas of criminal activity. It can be defined as any crime where:

- A computer is the target of the crime
- A computer is used to commit a crime
- Evidence is stored primarily on a computer, in digital format

Understanding the various types of cybercrimes can help identify and plan for a potential cybercrime against your firm.

Computer Intrusions

It is a crime to gain unauthorised access to a computer system. There are several different offences that can be characterised as unauthorised access or computer intrusion, some include:

- Obtaining national security information
- Compromising confidentiality
- Trespassing in a government computer
- Accessing to defraud and obtain value
- Damaging a computer or information
- Trafficking in passwords
- Threatening to damage a computer

Types of Computer Intrusions

Computer intrusions can come from an internal source, such as a disgruntled employee with an intimate knowledge of the computer systems, or an external source, such as a hacker looking to steal or destroy a company's intangible assets. The hacker can use a host of different means to try and steal or destroy your data in the following ways:

- **Viruses**: A virus is a small piece of software that attaches itself to a program currently on your computer. From there, it can attach itself to other programs and can manipulate data. Viruses can quickly spread from computer to computer, wreaking havoc the entire way. Email viruses became a popular method for hackers to infect computers in the late 1990s. These viruses were triggered when a person downloaded an infected document. When the document was opened, the virus would send that document to the first few recipients in the person's email address book. Some email viruses were so powerful that many companies were forced to shut down their email servers until the virus was removed.

- **Worms**: A worm is a computer program that can copy itself from machine to machine, using a machine's processing time and network's bandwidth to completely bog down a system. Worms often exploit a security hole in some software or operating system, spreading very quickly and doing a lot of damage to a business.

- **Trojan horses**: Common in email attachments, Trojans hide in otherwise harmless programs on a computer and, much like the Greek story, release themselves when you're not expecting it. And also like the story, the computer user has a part in letting the Trojan into the system. Trojans differ from viruses in that they must be introduced to the system by a user. A user can knowingly or unknowingly run an .exe file that will let a Trojan into the system.

- **Spyware**: Spyware can be installed on a computer without the user ever knowing it, usually from downloading a file from an untrusted source. Spyware can be used by hackers to track browsing habits or, more importantly, collect personal information such as credit card numbers.

- **Logic bombs**: Logic bombs are pieces of code that are set to trigger upon the happening of an event. For example, a logic bomb could be set to delete all the contents on a computer's hard drive on a specific date. There are many examples of disgruntled employees creating logic bombs within their employer's computer system. Needless to say, logic bombs can cause serious damage to a company's digital assets.

- **Denial of Service (DoS) and Distributed Denial of Service (DDoS) Attacks**: DoS and DDoS attacks are used to send an overwhelming amount of data to a target server, rendering that server useless. A hacker does this by gaining control of several or more computers and then sends a large amount of data to a target server that it can't possibly handle. The result could be thousands or millions of pounds in lost sales for an online retailer and a complete loss of productivity for many businesses.

Limiting Intrusions

A computer intrusion could put your valuable digital assets at risk. That's why your company should have the following measures in place to limit computer intrusions and protect your assets:

- **Firewalls:** Firewalls are pieces of software that control the incoming and outgoing network traffic on a computer system and decide whether it should be allowed through or not. Most computer operating systems now come with a preinstalled firewall for security. While they are not the be-all end-all of preventing intrusions, they are a reliable start.

- **Routers:** Routers are pieces of hardware that keep unwanted traffic out of a computer system. They differ from firewalls in that they are standalone devices that must be bought separately– they are not included in an operating system.

- **Antivirus programs:** As their name implies, antivirus programs are designed to catch and eliminate or quarantine viruses before they can harm a computer system. Antivirus programs run in the background to ensure your computer is protected at all times. While they are updated frequently, they may not catch the newest viruses that are floating around.

- **Policies**: Every company, no matter its size, should have policies in place to educate employees on the dangers of computer intrusions and ways to prevent them. Make sure your employees know not to open, click on or download anything inside emails from untrusted sources. Employees with an intimate knowledge of the company's computer network should also be alerted of the potential consequences of hacking into the system.

- **Common sense:** Everyone claims to have it, but if that were actually the case, many viruses, worms and Trojans would cease to exist. The simple fact is that everyone in the company needs to exhibit some common sense when using a computer. Encourage employees to disregard emails with subject lines and attachments that seem bogus or too good to be true.

Review Your Risks and Cover Options

A computer intrusion could cripple your company, costing you thousands or millions of pounds in lost sales, damages and sanctions.

Spam, Phishing and Spyware Defined

A computer intrusion could cripple your company, costing you thousands or millions of pounds in lost sales and/or damages. Hackers can obtain access to personal information in many ways, including spam, phishing and spyware. Below are definitions and examples of these three types of scams.

Spam

Spam is any unsolicited electronic content, often known as junk mail. It can take the form of a text message, direct mailer, phone call or email message. Spam emailing in particular is quite common, and spam emails often contain some form of scam, virus and/or invasive or inappropriate content.

Prevent your company from falling victim to scams and viruses in spam messages by teaching employees to ask the following questions while using company email:

- *Do you know the sender?* If employees don't recognise the sender's name, they should not open the email.
- *Is the grammar and spelling poor?* Sometimes spammers intentionally misspell words or use words incorrectly to sneak emails past your company's spam filter. Encourage employees to be on the lookout for this trick.
- *Have you received something from this sender before, but now the email looks drastically different?* It could be a fraudster. Encourage employees to look at all emails with a discerning eye, even those coming from known senders.
- *Does it sound too good to be true?* If it sounds too good to be true, it probably is.
- *Is it in your spam folder?* Make sure employees know the danger of opening messages that go straight to their spam folders. Many people consider spam to be annoying but harmless. However, the majority of computer viruses are 'caught' via email. Employees should never open messages that your system has designated as spam.

Additionally, company policies regarding computer use are an effective way to reduce the impact that spam has on your system. Minimally, your policy should require employees to:

- Turn off computers before leaving the office each day. Spam and viruses can strike a computer at any time when it is sitting idle and still connected to the internet.
- Keep work email communications separate from personal communications. Employees should use a personal email that is not connected to the company email for personal communications.
- Limit the amount of time employees can spend on social media sites (for example, only allow them to use the sites during breaks), or prohibit their access entirely during the working day.

Phishing

A phishing scam is a phony email or pop-up message used to lure unsuspecting internet users into divulging personal information, such as credit card numbers and account passwords, which will later be used by hackers for identity theft. A phisher's email can be very persuasive and believable if he or she is impersonating a well-known organisation or individual.

Keep employees safe from phishing scams by teaching them to:

- Be extremely wary of urgent email requests for any personal or financial information (their information or a client's).
- Call the company or individual in question with the number listed on the corporate website or in the phone book. Avoid using phone numbers within the email, as they could be phony too.

- Do not use the links included in the email unless you are certain that the email is legitimate.
- Do not divulge personal or financial information via the internet unless the site is secure (sites that start with ‘https’).
- Never disable anti-virus software.

Spyware

Spyware is software that can be installed on a computer without the user’s permission, usually as a result of the user opening an attachment and/or downloading an infected file from an untrusted source. Spyware can be used by hackers to ‘spy’ on internet users, track browsing habits and collect personal information such as credit card numbers.

Signs that spyware may be installed on a computer:

- The computer starts to suddenly run more slowly.
- Pop-ups appear when the user is offline.
- Internet browser settings are modified. New shortcuts, icons or toolbars may appear.

As most spyware is installed when users download free files from the internet, it’s important to ensure that your employee internet usage policy has a clause banning employees from opening or downloading personal files on work machines.

Many Internet Service Providers (ISPs) will offer security software to businesses at no charge, so be sure to ask. It is important to be vigilant and cautious about the content your employees open while using the internet. Risky employee internet use can have serious consequences for your company.

Keeping Your Data Secure

Data security is crucial for all businesses. Customer and client information, payment information, personal files, bank account details—this information is often impossible to replace if lost and is extremely dangerous in the hands of criminals. Data lost due to disasters such as a flood or fire is devastating, but losing it to hackers or a malware infection can have far greater consequences. How you handle and protect your data is central to the security of your business and the privacy expectations of customers, employees and partners.

What kind of data do you have?

Your business data may include customer data such as account records, transaction accountability and financial information, contact and address information, purchasing history, and buying habits and preferences, as well as employee information such as payroll files, direct payroll account bank information, home addresses and phone numbers, and work and personal email addresses. It can also include proprietary and sensitive business information such as financial records, marketing plans, product designs and tax information. If you collect personal information, make sure you have a privacy policy that explains how the information will be used and what individuals' rights are regarding the data.

Complete a data inventory to identify and classify all of your potential areas of vulnerability. Common data classifications include the following:

- **Highly confidential**: This classification applies to the most sensitive business information that is intended strictly for use within your company. Its unauthorised disclosure could seriously and adversely impact your company, business partners, vendors and/or customers in the short and long term. It could include credit card transaction data, customer names and addresses, card magnetic stripe contents, passwords and PINs and employee payroll files.

- **Sensitive**: This classification applies to sensitive business information that is intended for use within your company; information that you would consider to be private should be included in this classification. Examples include employee performance evaluations, internal audit reports, various financial reports, product designs, partnership agreements, marketing plans and email marketing lists.

- **Internal use only**: This classification applies to sensitive information that is generally accessible by a wide audience and is intended for use only within your company. While its unauthorised disclosure to outsiders should be against policy and may be harmful, the unlawful disclosure of the information is not expected to negatively impact your company, employees, business partners or vendors.

Classifying your data allows your company to set parameters for how the data is accessed, transported, shared and ultimately kept secure.

Where is your data stored?

Data is most at risk when it's on the move. If all your business-related data resided on a single computer or server that is not connected to the internet, and never left that computer, it would be very easy to protect. But to be meaningful, data must be accessed and used by employees, analysed and researched for marketing purposes, used to contact customers and even shared with key partners. Every time data moves or changes hands, it can be exposed to different dangers.

It's important to create a company policy that dictates safe data transfer and storage. The policy should include information on how to back up, transport and safely store physical and virtual data.

- **Physical data:** Keep in mind that physical media, such as a disc or drive used to store data or a data back-up, is vulnerable no matter where it is located, so make sure you guard any physical data stored in your office or off-site, and make sure that your physical data storage systems are encrypted. As much as possible, try to avoid data transport on physical media

such as flash drives or CDs. These media can easily end up in the wrong hands.

- **Website data:** Your website can be a great place to collect information, from transactions and payments to purchasing and browsing history, and even newsletter signups, online inquiries and customer requests. This data must be protected, whether you host your own website and manage your own servers or whether your website and databases are hosted by a third party. If a third party hosts your website, be sure to discuss systems it has in place to protect your data from hackers and outsiders as well as employees of the hosting company.

- **Virtual data:** Storing data virtually is a very common practice, but it has certain risks you need to consider. If your company contracts with a third party to house data virtually, be sure to keep an updated, thorough contract that outlines who accesses your data, how it is encrypted and how it is backed up. Additionally, be sure you are aware of the location of the company you are trusting with your data.

Who accesses your data?

Once you have identified, classified and located your data, you must control access to it. The more sensitive the data, the more restrictive the access should be. As a general rule, access to data should be on a need-to-know basis. Only individuals who have a specific need to access certain data should be allowed to do so.

Not every employee needs access to all of your information. For example, your marketing staff shouldn't need or be allowed to view employee payroll data, and your administrative staff may not need access to all your customer information.

The first step in controlling access to your data is assigning rights to that data. Doing so simply means creating a list of the specific employees, partners or contractors who have access to specific data, under what circumstances, and how those access privileges will be managed and tracked. As part of this process, you should consider developing a straightforward plan and policy—a set of guidelines—about how each type of data should be handled and protected based on who needs access to it and the level of classification.

How do you protect your data?

Once you understand the type of data your company makes use of, where it is located and who accesses it, you can begin planning how you will protect it. Protecting data, like any other security challenge, is about creating layers of protection. The idea of layering security is simple: You cannot and should not rely on just one security mechanism—such as a password—to protect something sensitive. If that security mechanism fails, you have nothing left to protect you.

Businesses have many affordable backup options, whether it's backing up to an external drive in the office, or backing up online so that all data is stored at a remote and secure data centre.

Are you planning for the future?

Every business has to plan for the unexpected, and that includes the loss or theft of data from your business. Not only can the loss or theft of data hurt your business, brand and customer confidence, it can also expose you to the often costly violations of the Data Protection Act that cover data protection and privacy. Data loss can also expose you to significant legal actions.

That's why it's critical to understand exactly which data or security breach regulations affect your business and how prepared you are to respond to them. At the very least, all employees and contractors should understand that they must immediately report any loss or theft of information to the appropriate company officer.

Identifying your exposures will help you figure out how to protect your data. In additional to data security measures, insuring your data is crucial.

Physical Protection of Cyber Assets

When it comes to securing cyber assets, many people often think only of mitigating cyber risks like spam, phishing and malware. However, cyber assets can also be compromised physically. This article examines the physical exposures your cyber assets face and provides steps for mitigating these risks.

Secure company facilities

The physical security of a facility depends on a number of security decisions that can be identified through a comprehensive risk-management process. It is easy to think about physically securing your company's facility as merely an exercise in maintaining control of access points and ensuring there is complete visibility in areas that are determined to be high-risk—either because of the threat of easy public access or because of the value of information located nearby. However, maintaining facility security also includes the physical environment of public spaces. For instance:

- Employees whose computers have access to sensitive information should not have their computer monitors oriented towards publicly accessible spaces such as reception areas, check-in desks and waiting rooms. Employees should be trained to not write out logon information on small pieces of paper affixed to computer equipment viewable in public spaces.

- Easy-to-grab equipment that could contain sensitive or personal information, such as laptops, tablets and mobile phones, should be located away from public areas. If you have an environment where employees are working in a waiting room or reception area, train them to not leave these types of devices out on their desks unsecured.

- Consider using cable locks as an easy way to increase security for laptop computers. Most laptops feature a lock port for a cable which can be connected to the user's desk. Be sure to store the key to the cable lock in a secure location away from the desk the computer is locked to.

- If extremely sensitive information is stored on a laptop, consider installing tracking software. Most tracking software programs run unnoticed, and allow stolen computers to be located more easily. Many also allow administrators to wipe the hard drive remotely if necessary.

- Consider implementing a badge identification system for all employees, and train employees to stop and question anyone in the operational business area without a badge or who appears to be an unescorted visitor.

Minimise and safeguard printed materials with sensitive information.

The most effective way to minimise the risk of losing control of sensitive information from printed materials is to minimise the quantity of printed materials that contain sensitive information. Establish procedures that limit the number of copies of printed reports, memoranda and other material containing personal information.

Safeguard copies of material containing sensitive information by providing employees with locking file cabinets or safes. Make it a standard operating procedure to lock up important information. Train employees to understand that simply leaving the wrong printed material on a desk, in view of the general public, can result in consequences that impact the entire company and your customers.

Ensure mail security.

Your organisation's post centre can introduce a wide range of potential threats to your business. Your centre's screening and handling processes must be able to identify threats and hoaxes and eliminate or mitigate the risk they pose to facilities, employees and daily operations. Your company should ensure that managers understand the range of screening procedures and evaluate them in terms of your specific operational requirements.

Dispose of rubbish securely.

Too often, sensitive information, including customers' personal information, company financial data, and company system access information, is available for anyone to find in the rubbish. Invest in business-grade shredders and buy enough of them to make shredding convenient for employees. Alternatively, subscribe to a trusted shredding company that will provide locked containers for storage until documents are shredded. Develop standard procedures and employee training programmes to ensure that everyone in your company is aware of what types of information need to be shredded.

Dispose of electronic equipment securely.

Be aware that emptying the recycle bin on your desktop or deleting documents from folders on your computer or other electronic device may not delete information forever. Those with advanced computer skills can still access your information even after you think you've destroyed it.

Disposing of electronic equipment requires skilled specialists in order to ensure the security of sensitive information contained within that equipment. If outside help, such as an experienced electronic equipment recycler and data security vendor, is not available or is too expensive, you should at a minimum remove computer hard drives and have them shredded. Also, be mindful of risks with other types of equipment associated with computer equipment, including CDs and flash drives.

Train your employees in facility security procedures.

A security breach of customer information or a breach of internal company information can result in a public loss of confidence in your company and can be as devastating for your business as a natural disaster. In order to address such risks, you must devote your time, attention and resources (including employee training time) to the potential vulnerabilities in your business environment and the procedures and practices that must be a standard part of each employee's working day.

And while formal training is important for maintaining security, the daily procedures you establish both in how you normally conduct business and in the way you model good security behaviours and practices are equally important. In short, security training should be stressed as critical and reinforced through daily procedures and leadership modelling. Establishing procedures and training employees to physically protect your company's cyber assets will allow for a secure work environment.

Mobile Device Security

Because of their convenience, smartphones and tablet devices have become a universal presence in the modern business world. As usage soars, it becomes increasingly important to take steps to protect your company from mobile threats, both new and old.

The need for proper phone security is no different from the need for a well-protected computer network. Gone are the days when the most sensitive information on an employee's phone was contact names and phone numbers. Now a smartphone or tablet can be used to gain access to anything from emails to stored passwords to proprietary company data. Depending on how your organisation uses such devices, unauthorised access to the information on a smartphone or tablet could be just as damaging as a data breach involving a traditional computer system.

Lost or Stolen Devices

Because of their size and the nature of their use, mobile devices are particularly susceptible to being lost or stolen. One-third of all reported UK cyber security incidents were due to mobile devices being exploited. Since most devices automatically store passwords in their memory to keep users logged in to email and other applications, gaining physical possession of the device is one of the easiest ways for unauthorised users to access private information.

To prevent someone from accessing information on a lost or stolen device, the phone or tablet should be locked with a password or PIN. The password should be time sensitive, automatically locking the phone out after a short period of inactivity. Most devices come with such security features built in. Depending on your mobile provider, there are also services that allow you to remotely erase or lock down a device if it is lost or stolen. Similarly, it is possible to program a mobile device to erase all of its stored data after a certain number of login failures.

Malicious Attacks

Mobile devices are just as susceptible to malware and viruses as computers, yet many businesses don't consider instituting the same type of safeguards. Less than 20 per cent of mobile devices have antivirus software installed, which is practically an invitation to thieves or hackers to pillage whatever information they want from an unprotected device. Furthermore, it doesn't matter what operating system the devices have, whether it be Android, Apple's iOS, Blackberry or Windows Mobile—all are vulnerable to attacks.

As reliance on these devices continues to grow, so will their attractiveness as potential targets. Third-party applications (apps) are especially threatening as a way for malware to install itself onto a device. These apps can purchase and install additional apps onto the phone without the user's permission. Employees should never install unauthorised apps to their company devices. Apps should only be installed directly from trusted sources.

Hackers can use 'ransomware' to restrict a user's access to their device's data, contacts, etc, and then demand a ransom to get it back. Even if the user pays the ransom, there is no guarantee that he or she will get the data back. Employees should know to never pay the ransom if this type of software finds its way onto a company device.

A big difference between mobile devices and laptops and other computers is the ability to accept open Wi-Fi and Bluetooth signals without the user knowing. Hackers can take advantage of this by luring devices to accept connections to a nearby malicious device. Once the device is connected, the hacker can steal information at will. To prevent this, make sure all mobile devices are set to reject open connections without user permission.

Preventive Measures

While the current mobile device security landscape may seem lacking, there are plenty of ways to be proactive about keeping company devices safe from threats.

1. **Establish a Mobile Device Policy**

   Before issuing mobile phones or tablets to your employees, establish a device usage policy. Provide clear rules about what constitutes acceptable use as well as what actions will be taken if employees violate the policy. It is important that employees understand the security risks inherent to mobile device use and how they can mitigate those risks. Well informed, responsible users are your first line of defence against cyber attacks.

2. **Establish a Bring Your Own Device (BYOD) Policy**

   If you allow employees to use their personal devices for company business, make sure you have a formal BYOD policy in place. Your BYOD security plan should also include the following:

   - Installing remote wiping software on any personal device used to store or access company data.
   - Educating and training employees on how to safeguard company data when they access it from their own devices.
   - Informing employees about the exact protocol they must follow if their device is lost or stolen.

3. **Keep the devices updated with the most current software and antivirus programs.**

   Software updates to mobile devices often include patches for various security holes, so it's best practice to install the updates as soon as they're available.

   There are many options to choose from when it comes to antivirus software for mobile devices, so it comes down to preference. Some are free to use, while others charge a monthly or annual fee and often come with better support. In addition to antivirus support, many of these programs will monitor SMS, MMS and call logs for suspicious activity and use blacklists to prevent users from installing known malware to the device.

4. **Back up device content regularly.**

   Just like your computer data should be backed up regularly, so should the data on your company's mobile devices. If a device is lost or stolen, you'll have peace of mind knowing your valuable data is safe.

5. **Choose passwords carefully.**

   The average internet user has about 25 accounts to maintain and an average of 6.5 different passwords to protect them, according to a recent Microsoft study. This lack of security awareness is what hackers count on to steal data. Use the following tips to ensure your mobile device passwords are easy to remember and hard to guess:

   - Require employees to change the device's login password every 90 days.
   - Passwords should be at least eight characters long and include uppercase letters and special characters, such as asterisks, ampersands and pound signs.
   - Don't use names of spouses, children or pets in the password. A hacker can spend just a couple minutes on a social media site to figure out this information.

Safely Disposing of Your Devices

New, revolutionary technology is released constantly. Every day, new gadgets are touted as the must-have tool to ensure future business success. Some businesses, in their scramble to cash in on the technological gold rush, ditch their old devices without a second thought.

Neglecting to safely dispose of your devices can spell disaster for your business. However you dispose of them—whether donating, selling or recycling—you must remove the sensitive information on the devices to prevent third parties from obtaining it.

But removing that information is harder than it seems. Systems are constructed to protect users from losing the information they need. Take extra steps to remove information from your computing devices before you discard them, lest your data ends up in the wrong hands. Private data such as account information and passwords represent a significant vulnerability to your business' cyber security. The theft of sensitive data can threaten your business' reputation and customer confidence, and can generate steep fines under the Data Protection Act.

Common Techniques for Removing Information

Simply hitting the delete key does not completely remove your sensitive data from devices. Deleting removes pointers to information on your device, but it does not remove the actual information. Deleting a file sends it to a 'holding area' from which you can restore it. So even when you think you have deleted a file, unauthorised people may be able to recover it.

Do not rely on file deletion. Instead, choose one or more of these five options recommended by the Information Commissioner's Office (ICO).

1. **Physical Destruction**

   Physically destroying a device can be a viable option for preventing others from retrieving your information. You can destroy your hard drive by drilling nails or holes into the device or even smashing it with a hammer. Never try to destroy a hard drive by burning it, putting it in the microwave or pouring acid on it.

   Some shredders are equipped to destroy flexible devices such as CDs and DVDs. If you smash or shred the device yourself, the pieces must be small enough that your data cannot be reconstructed—0.2 millimetres is ideal. Wrap the CD or DVD in a kitchen towel when destroying it to limit shrapnel.

   Magnetic devices such as tapes, hard drives and floppy disks can be destroyed by degaussing, which is exposing devices to a very strong magnet. You can rent or purchase degaussers. They destroy not only the device's information but also the firmware that makes the device run. You should only use degaussers when you plan to dispose of the entire device.

2. **Overwriting**

   Overwriting is effective on most computing devices. It replaces your sensitive data with random data, and because of this your data cannot be retrieved. While experts agree on the use of random data, they disagree on how many times one should overwrite to be safe. Some say that one time is enough, others recommend at least three times, followed by 'zeroing' the drive (writing all zeroes). There are software programs and hardware devices available that can overwrite your hard drives, CDs and DVDs. But because these programs and devices have varying levels of effectiveness, it is important to carefully investigate your options. When choosing software or a device to overwrite your data, look for the following characteristics:

   - **'Secure Erase' is performed.** Secure Erase is a standard in modern hard drives used to completely erase and overwrite all data on a hard drive.

   - **Data is written multiple times.** It is important to ensure that not only is the information erased, but new data is written over it. By erasing the original then adding new data, the

programme makes it difficult for an attacker to uncover any traces possibly left behind by the original. Two passes is usually sufficient.

- **Random data is used.** Using random data instead of easily identifiable patterns makes it harder for attackers to discover any original information buried underneath.

- **Zeroes are used in the final layer.** Regardless of how many times you overwrite your data, rely on programmes that use all zeroes in the last swipe—this adds an additional level of security.

3. Restoring to Factory Settings

Many devices have the capability to revert back to their factory settings. Activating this function will return the device to the state in which you bought it. Unlike other deletion methods, restoring to factory settings works for devices both with and without removable or accessible storage media. However, not all manufacturers implement a secure data wiping stage during the factory reset process. Check with your device's manufacturer to determine whether the factory reset process is sufficiently secure.

4. Sending It to a Specialist

There are numerous organisations which will securely delete data from a range of devices and types of media. These organisations erase or overwrite data for businesses and individuals. As an added bonus, some specialist organisations may be able to return, reuse or recycle your media or device after they have securely deleted your data. However, because you trust this business with wiping your devices clean, you should make sure their deletion processes are secure. If possible, perform another secure deletion method or restore your devices to their factory settings before sending them to a specialist organisation.

5. Formatting

To 'format' something means to prepare a storage medium like a hard drive for use. When you format a hard drive, your operating system erases all 'bookkeeping' information your drive uses to organise data. But formatting a hard drive does not erase all of that drive's data—it sequesters and retains it until it is overwritten. Formatting is often used in conjunction with overwriting to provide further assurance that data cannot be recovered. Formatting a drive without relying on any additional data deletion methods is never sufficient to remove data, since it can be easily recovered using freely available software.

Mobile Phone and Tablet Advice

Although the exact steps for clearing all information from your mobile phone or tablet vary among different brands and models, the general process, enumerated below, remains the same across the board.

1. Remove your device's memory card.

2. Remove the SIM (Subscriber Identity Module) card.

3. Under Settings, select Master Reset, Wipe Memory, Erase All Content and Settings (or a similarly worded option). You might need to enter a password you have set, or contact the manufacturer for assistance with a factory-set password.

4. Physically destroy the SIM and memory cards or store them in a secure place. Memory cards can typically be reused, and SIM cards can be reused in a phone that has the same carrier.

5. Ensure that your account has been terminated or switched to your new device.

For detailed information about your particular device, consult your manufacturer's online documentation or the staff at your local mobile store.

Network Security

As the amount of sensitive information on your computer network grows, so too does the need for appropriate measures to ensure this data is not compromised. To properly secure your company's network:

- Identify all devices and connections on the network,
- Set boundaries between your company's systems and others, and
- Enforce controls to ensure that unauthorised access, misuse or denial-of-service events can be thwarted or rapidly contained and recovered from if they do occur.

Use the following tips to create a safe and secure network.

Secure internal network and cloud services.

Your company's network should be separated from the public internet by strong user authentication mechanisms and policy enforcement systems such as firewalls and web filtering proxies. Additional monitoring and security solutions, such as anti-virus software and intrusion detection systems, should also be employed to identify and stop malicious code or unauthorised access attempts.

- **Internal network:** After identifying the boundary points on your company's network, each boundary should be evaluated to determine what types of security controls are necessary and how they can be best deployed. Border routers should be configured to only route traffic to and from your company's public IP addresses; firewalls should be deployed to restrict traffic only to and from the minimum set of necessary services, and intrusion prevention systems should be configured to monitor for suspicious activity crossing your network perimeter. To prevent bottlenecks, all security systems you deploy to your company's network perimeter should be capable of handling the bandwidth that your internet service provider offers.
- **Cloud-based services:** Carefully consult your terms of service with all cloud service providers to ensure that your company's information and activities are protected with the same degree of security you would intend to provide on your own. Request security and auditing from your cloud service providers as applicable to your company's needs and concerns and ensure the provider's policies and workflows comply with your jurisdiction's regulations governing how data is handled and stored. Make sure to review and understand service level agreements, or SLAs, for system restoration and reconstitution time. You should also enquire about additional services a cloud service can provide. These services may include backup-and-restore services and encryption services, which can further bolster your data security.

Develop strong password policies.

Generally, two-factor authentication methods, which require two types of evidence that you are who you claim to be, are safer than using only static passwords for authentication. One common example is a personal security token that displays changing passcodes to be used in conjunction with an established password.

Additionally, password policies should encourage your employees to use the strongest passwords possible without creating the need or temptation to reuse passwords or write them down. That means using passwords that are random, complex and long (at least 10 characters), that are changed regularly and that are closely guarded by those who know them.

Secure and encrypt your company's Wi-Fi.

Your company may choose to operate a Wireless Local Area Network (WLAN) for the use of customers, guests and visitors. If so, it is important that the WLAN be kept separate from the main company network so that traffic from the public network cannot traverse the company's internal systems at any point.

Internal, non-public WLAN access should be restricted to specific devices and specific users to the greatest extent possible while still meeting your company's business needs. Where the internal WLAN has less stringent access controls than your company's wired network, dual connections—where a device is able to connect to both the wireless and wired networks simultaneously—should be prohibited by technical controls on each such capable device. All users should be given unique credentials with preset expiry dates to use when accessing the internal WLAN.

Encrypt sensitive company data.

Encryption should be employed to protect any data that your company considers sensitive, in addition to meeting applicable regulatory requirements on information safeguarding. Different encryption schemes are appropriate under different circumstances. If you choose to offer secure transactions on your company's website, consult with your service provider about available options for a secure socket layer (SSL) certificate for your site.

Regularly update all applications.

All systems and software, including networking equipment, should be updated in a timely fashion as patches and firmware upgrades become available. Use automatic updating services whenever possible, especially for security systems such as anti-malware applications, web filtering tools and intrusion prevention systems.

Set safe web browsing rules.

Your company's internal network should only be able to access those services and resources on the internet that are essential to the business and the needs of your employees. Use the safe browsing features included with modern web browsing software and a web proxy to ensure that malicious or unauthorised sites cannot be accessed from your internal network.

If remote access is enabled, make sure it is secure.

If your company needs to provide remote access to your internal network over the internet, one popular and secure option is to employ a secure Virtual Private Network (VPN) system accompanied by strong two-factor authentication, using either hardware or software tokens.

Create a Safe-use Flash Drive Policy.

Ensure that employees never put any unknown flash drive or USBs into their computers. Businesses should set a clear policy so employees know they should never open a file from a flash drive they are not familiar with, and that they should hold down the Shift key when inserting the flash drive to block malware. By doing so, you can stop the flash drive from automatically running.

Website Security

Website security is more important than ever. Cyber criminals are constantly looking for improperly secured websites to attack, while many customers say website security is a top consideration when they choose to shop online. As a result, it is essential to secure servers and the network infrastructure that supports them. The consequences of a security breach are great: loss of revenue, damage to credibility, legal liability and loss of customer trust.

Web servers, which host the data and other content available to your customers on the internet, are often the most targeted and attacked components of a company's network. By securing your web server, you protect customers and prospects that use your company website. The following are examples of specific security threats to web servers:

- Cyber criminals may exploit software bugs in the web server, underlying operating system or active content to gain unauthorised access to the server.
- Denial-of-service attacks may be directed at the web server or its supporting network infrastructure to prevent or hinder your website users from making use of its services. Attacks can include preventing users from accessing email, websites, online accounts or other services. One of the most common attacks is flooding a network with information so that it can't process users' requests.
- Sensitive information on the web server may be read or modified without authorisation.
- Information on the web server may be changed for malicious purposes.
- Cyber criminals may gain unauthorised access to resources elsewhere in the organisation's network with a successful attack on the web server.
- The server may be used as a distribution point for attack tools, pornography or illegally copied software.

Take the following five steps to protect your company from the threats listed above.

Step 1: Form a plan and utilise the right people.

Because it is much more difficult to address security once deployment and implementation have occurred, security should be considered from the initial planning stage. Businesses are more likely to make decisions about configuring computers appropriately and consistently when they develop and use a detailed, well-designed deployment plan. Developing such a plan will support web server administrators in making the inevitable trade-off decisions between usability, performance and risk.

Make sure to define appropriate management security practices, such as identification of your company's information system assets and the development, documentation and implementation of policies, as well as guidelines to help ensure the confidentiality, integrity and availability of information system resources.

Businesses also need to consider the human resource requirements for the deployment and continued operation of the web server and supporting infrastructure. Consider the personnel you will need on your team—for example, system and web server administrators, webmasters, network administrators and information systems security personnel. Additionally, consider the level of training (initial and ongoing) that will be required to maintain this team.

Step 2: Ensure that web server operating systems and applications meet your organisation's security requirements.

When securing a web server, you must first secure the underlying operating system. Most web servers operate on a general-purpose operating system. Many security issues can be avoided if the operating systems underlying web servers are configured appropriately. Default hardware and

software configurations are typically set by manufacturers to emphasise features, functions and ease of use at the expense of security. Because manufacturers are not aware of each organisation's security needs, web server administrators must configure new servers to reflect their business' security requirements and reconfigure them as those requirements change. Take the following steps as appropriate to your business:

- Patch and upgrade the operating system.
- Change all default passwords.
- Remove or disable unnecessary services and applications.
- Configure operating system user authentication.
- Configure resource controls.
- Install and configure additional security controls.
- Perform security testing of the operating system.

Step 3: Publish only appropriate information.

Company websites are often one of the first places cyber criminals search for valuable information. Still, many businesses lack a web publishing process or policy that determines what type of information to publish openly, what information to publish with restricted access and what information should not be published to any publicly accessible repository. Some generally accepted examples of what should not be published or what should at least be carefully examined and reviewed before being published on a public website include the following:

- Classified or proprietary business information
- Sensitive information relating to your business' security
- Detailed physical and information security safeguards
- Details about the network and information system infrastructure—for example, address ranges, naming conventions and access numbers
- Information that specifies or implies physical security vulnerabilities
- Detailed plans, maps, diagrams, aerial photographs and architectural drawings of business buildings, properties or installations
- Any sensitive information about individuals that might be subject to privacy laws

Step 4: Prevent unauthorised access or modification on your site.

It is important to ensure that the information on your website cannot be modified without authorisation. Users of such information rely on its integrity. Content on publicly accessible web servers is inherently more vulnerable than information that is inaccessible from the internet, and this vulnerability means businesses need to protect public web content through the appropriate configuration of web server resource controls. Examples of resource control practices include the following:

- Install or enable only necessary services.
- Install web content on a dedicated hard drive or logical partition.
- Limit uploads to directories that are not readable by the web server.

- Define a single directory for all external scripts or programs executed as part of web content.
- Disable the use of hard or symbolic links.
- Define a complete web content access matrix identifying which folders and files in the web server document directory are restricted and which are accessible, and by whom.
- Disable directory listings.
- Deploy user authentication to identify approved users, digital signatures and other cryptographic mechanisms as appropriate.
- Use intrusion detection systems, intrusion prevention systems and file integrity checkers to spot intrusions and verify web content.
- Protect each backend server (database server or directory server) from command injection attacks.

Step 5: Continuously protect and monitor web security.

Maintaining a secure web server requires constant effort, resources and vigilance. Securely administering a web server on a daily basis is essential. Maintaining the security of a web server will usually involve the following steps:

- Configuring, protecting and analysing log files
- Backing up critical information frequently
- Maintaining a protected authoritative copy of your organisation's web content
- Establishing and following procedures for recovering from compromise
- Testing and applying patches in a timely manner
- Testing security periodically

Taking proactive measures to secure your website by carefully setting up and maintaining your web server can save your business from experiencing crushing losses of revenue, customer loyalty and proprietary information.

Protecting Your Email

Email has become a critical part of everyday business, from internal management to direct customer support. The benefits associated with email as a primary business tool far outweigh the negatives. However, businesses must be mindful that a successful email platform starts with basic principles of email security to ensure the privacy and protection of customer and business information.

Set up a spam email filter.

It has been well documented that spam, phishing attempts and otherwise unsolicited and unwelcome email accounts for more than 60 per cent of all email that an individual or business receives. Email is the primary method for spreading viruses and malware. Consider using email-filtering services that your email service, hosting provider or other cloud providers offer. A local email filter application is also an important component of a solid anti-virus strategy. Ensure that automatic updates are enabled on your email application, email filter and anti-virus programs. Additionally, ensure that filters are reviewed regularly so that important email and/or domains are not blocked in error.

Protect sensitive information sent via email.

With its proliferation as a primary tool to communicate internally and externally, business email often includes sensitive information. Whether it is company information that could harm your business or personal information, it is important to ensure that such information is only sent and accessed by those who are entitled to see it.

Email in its native form is not designed to be secure, so incidents of misaddressing or other common accidental forwarding can lead to data leakage. If your business handles sensitive information, you should consider whether it should be sent via email, or at least consider using email encryption. Encryption is the process of converting data into unreadable format to prevent disclosure to unauthorised personnel. Only individuals or organisations with access to the encryption key can read the information. Cloud services can offer secure web-enabled drop boxes that allow secure data transfer for sensitive information, which is often a better approach to transmission between companies or customers.

Implement a sensible email retention policy.

It's important to manage the email that resides on your company messaging systems and your users' computers. You should document how you will handle email retention, and you should also implement basic controls to ensure information is retained for the necessary period. Some industries may have specific rules that dictate how long emails can or should be retained, but the basic rule of thumb is only as long as it supports your business efforts.

To ensure compliance, consider mandatory archiving at a chosen retention cycle end date and automatic permanent email removal after another set point, such as 180-360 days in archives. In addition, discourage the use of personal folders on employee computers (most often configurable from the email system level), as this will make it more difficult to manage company standards.

Develop an email usage policy.

Policies are important for setting expectations for your employees or users, and for developing standards to ensure adherence to your published polices.

Your policies should be easy to read, understand, define and enforce. Key areas to address include what the company email system should and should not be used for, and what data is allowed to be transmitted. Other policy areas should address retention, privacy and acceptable use.

Depending on your business, you may have a need for email monitoring. The rights of the business and the user as they relate to monitoring should be documented in your email usage policy. The policy should be part of your general end user awareness training and reviewed for updates on a yearly basis.

Train your employees in responsible email usage.

The last line of defence for all of your cyber risk efforts lies with the employees who use email and their responsible and appropriate use and management of the information under their control. Technology alone cannot make a business secure. Employees must be trained to identify risks associated with email use, how and when to use email appropriate to their work and when to seek professional assistance. Employee awareness training is available in many forms, including printed media, videos and online training.

Consider requiring security awareness training for all new employees and offering refresher courses every year. You can provide monthly newsletters, urgent bulletins when new viruses are detected and even posters in common areas to remind your employees of key security and privacy to-do's.

Basic Loss Control Techniques

Protecting your business from cyber risks can be an overwhelming venture. A new day means more viruses are being discovered, more spam is being delivered to your inbox and yet another well-known company is the victim of a data breach.

The world will never be free of cyber risks, but there are many loss control techniques you can implement to help protect your business from exposures.

1. **Install a firewall for your network.**

   Operating systems often come with pre-installed firewalls, but they are generally designed to protect just one computer. Examine the firewall's options and select the best configuration to keep the computer safe.

   If your business has a network of five or more computers, consider buying a network firewall. They can be pricey but network firewalls provide a fine level of coverage for an entire network.

2. **Install anti-virus, anti-malware and anti-spyware software.**

   This loss control technique is the easiest and most effective way to increase security at your business. Make sure to install the software on each computer in your network—computers that don't include these types of software are much more likely to be exposed and can possibly spread malware to other computers in the network. There are a host of viable options for each type of software, ranging in price from free to an annual subscription. Be sure to keep the software as up-to-date as possible.

3. **Encrypt data.**

   No firewall is perfect. If a hacker manages to get through your firewall and into your network, your data could be a sitting duck. Encryption will make the data unreadable to a hacker. Consider using an encryption program to keep computer drives, files and even email messages safe from hackers.

4. **Use a Virtual Private Network (VPN).**

   A VPN allows employees to connect to your company's network remotely. VPNs eliminate the need for a remote-access server, saving companies lots of money in remote server costs. In addition to these savings, VPNs also provide a high level of security by using advanced encryption and authentication protocols that protect sensitive data from unauthorised access. If your company has salespeople in the field or employs workers who work from home or away from the office, a VPN is an effective way to minimise cyber risks.

5. **Implement an employee password policy.**

   One of the most overlooked ways to keep your business safe is instituting a password policy. Essentially, a password policy should force employees to change work-related passwords every 90 days. The policy should encourage the creation of easy-to-remember, hard-to-guess passwords that include letters, numbers and special characters. For example, an easy-to-remember, hard-to-guess password could be 'M1dwbo2510'. (My first daughter was born on the 25th of October)

   Passwords that contain words from the dictionary or contain sensible combinations (abc123, qwerty, etc) should never be allowed. Let employees know that they should not write passwords down and leave them in a desk or out in the open. If they are having trouble remembering passwords, there are password-keeping programs available for download.

6. **Back up data regularly.**

   Important data should be backed up daily and in multiple locations, one being off-site. In addition to being safe from cyber risks, off-site data would not be exposed from physical attacks, like a fire

or natural disaster.

Restrict access to backed up data. The public should never have access to it. If the data is tangible, keep it in locked filing cabinets in a locked room, and only issue keys to those who absolutely need them.

7. Develop a business continuity plan.

If the worst should happen and your company suffers a data breach or similar attack, you should have a business continuity plan in place. A business continuity plan helps:

- Facilitate timely recovery of core business functions
- Protect the well-being of employees, their families and your customers
- Minimise loss of revenue/customers
- Maintain public image and reputation
- Minimise loss of data
- Minimise the critical decisions to be made in a time of crisis

The plan should identify potential cyber risks, along with the recovery team at your company assigned to protect personnel and property in the event of an attack. The recovery team should conduct a damage assessment of the attack and guide the company towards resuming operations.

Managing Password Threats

Organisations trust passwords to protect valuable assets such as data, systems and networks. Passwords are versatile—they authenticate users of operating systems (OS) and applications such as email, labour recording and remote access, and they guard sensitive information like compressed files, cryptographic keys and encrypted hard drives.

Because passwords protect such valuable data, they are often a prime target of hackers and thieves. Although no method of password protection is 100 per cent effective, it is still important to understand and mitigate threats to password security so you can protect your company and its assets.

Types of Password Threats

Implementing security measures starts with anticipating security threats. There are four main ways that attackers attempt to obtain passwords: capturing passwords, guessing or cracking passwords, replacing passwords and using compromised passwords.

1. **Password Capturing**

   An attacker can capture a password through password storage, password transmission or user knowledge and behaviour. OS and application passwords are stored on network hosts (a computer connected to a network) and used for identification. If the stored passwords are not secured properly, attackers with physical access to a network host may be able to gain access to the passwords. Never store passwords without additional controls to protect them. Security controls include:

   - Encrypting files that contain passwords
   - Restricting access to files that contain passwords using OS access control features
   - Storing one-way cryptographic hashes for passwords instead of storing the passwords themselves

   Hashes are the end result of putting data, like passwords, through an algorithm that changes the form of the original information into something different. For example, the password ‘default’ could be mapped as an integer such as 15. Only the network host knows that 15 stands for the password ‘default’.

   Using hashes allows computers to authenticate a user’s password without storing the actual password. However, organisations should assess which applications are allowed to store passwords or hashes based on the risks, rather than on convenience for the user. This assessment should be reflected in the organisation’s password policy.

   Even when passwords are protected with hashes, an attacker can still uncover them via transmission. When a user enters a password into a computer, the password or hash is often transmitted between hosts over the network to authenticate that user. This transmission action is vulnerable to attack. You can reduce this risk by encrypting your passwords or the transmissions containing the passwords.

   Organisations can also avoid transmission risks by storing passwords on paper. Such papers should be physically secured in a locked safe or file cabinet. Be sure to properly discard any password-containing papers by shredding them.

   However, storing passwords on paper cannot protect against means of capturing passwords that rely on user behaviour such as malware. For example, Trojan horses and keylogger malware observe user activity, such as which keys a user presses, to discover his or her username and passwords. Mitigate these threats by regularly scanning your computers with antimalware and antivirus software.

   Users can also endanger password security by responding to phishing attempts, which relocate a

user to a malicious website posing as a legitimate one that asks for sensitive information such as usernames and passwords. Caution your employees against downloading files from unknown sources.

2. Password Guessing and Cracking

Attackers attempt to discover weak passwords through guessing, and recover passwords from password hashes through cracking.

Guessing is simple: An attacker attempts to uncover a password by repeatedly guessing default passwords, dictionary words and other possible passwords. Anyone who has access to the authentication interface can try to guess a password. That is why strong passwords are necessary for cyber security. Never pick a password that someone could easily guess, and make sure to reasonably limit the number of authentication attempts to prevent unlimited guessing.

Cracking is a little more complicated. Attackers gain access to password hashes and attempt to discover a character string that will produce the same encrypted hash as the password. If the hash algorithm is weak, cracking is much easier. Hash functions should be one-way, meaning passwords only go from original to encrypted, not vice versa. Hash functions make it nearly impossible to derive the original text from the character string. As with guessing, cracking can also be prevented by choosing strong passwords and periodically changing them.

3. Password Replacing

When users forget their passwords, they have two options: reset the password (change it to a new one) or recover the password (get access to the current one). If the user's identity is not properly verified in a reset or recovery request, an attacker could easily pose as the user, gain unauthorised access to the system, application or data and provide a password that only he or she knows. This replaces the user's original password with something unknown, barring the user from the system.

All attempts to reset or recover a password should start with a rigorous verification process. Verification should not hinge on information that can be easily obtained, such as birth date, employee number or mother's maiden name. Instead, consider personal or subjective information that only the user knows.

4. Compromised Passwords

When an attacker compromises a password through any of the previously mentioned methods, that attacker will have unauthorised access until the user changes his or her password. For this reason, many organisations use automatic password expiry measures to ensure no password remains valid forever.

Yet password expiry is futile if the root cause of a compromised password is not fixed. For example, if an attacker uses cracking to obtain a password, automatic password expiry will not solve the security problem because the attacker can simply use the same process again. If you use automatic password expiry, make sure you have a plan in place to secure your system and reset passwords in the event of a security breach. When one password is compromised, reset all passwords just to be safe.

Password Management

On-going password management will help prevent unauthorised attackers from compromising your organisation's password-protected information. Effective password management protects the integrity, availability and confidentiality of an organisation's passwords.

Integrity and availability should be ensured by typical data security controls, such as using access control lists to prevent attackers from overwriting passwords and having secured backups of password files. Confidentiality, on the other hand, is much harder to ensure—it involves implementing diverse security measures and making decisions about the nature of passwords themselves. For example, organisations should encourage users to choose long, complex passwords with a mixture of numbers and letters. However, complex passwords are harder to remember, which means users are

more likely to write them down and subsequently endanger the system's security. This presents a dilemma in which one security measure (choosing a long, complex password) conflicts with another (never writing down your password).

Protecting Your Passwords

You can help resolve conflicting security measures by implementing the following security recommendations:

- Create a password policy that specifies all of the organisation's password management-related requirements.
- Protect passwords from attacks that capture passwords.
- Configure password mechanisms to reduce the likelihood of successful password guessing and cracking.
- Determine requirements for password expiry based on balancing security needs and usability.

Policies to Manage Cyber Risk

All companies should develop and maintain clear and robust policies for safeguarding critical business data and sensitive information, protecting their reputations and discouraging inappropriate behaviour by employees. Many companies already have these types of policies in place, but they may need to be tailored to reflect the increasing impact of cyber risks on everyday transactions, both professional and personal. As with any other business document, cyber security policies should follow good design and governance practices—not so long that they become unusable, not so vague that they become meaningless, and reviewed regularly to ensure that they stay pertinent as your business' needs change.

Establish security roles and responsibilities.

One of the most effective and least expensive means of preventing serious cyber security incidents is to establish a policy that clearly defines the separation of roles and responsibilities with regard to systems and the information they contain. Many systems are designed to provide for strong role-based access control (RBAC), but this tool is of little use without well-defined procedures and policies to govern the assignment of roles and their associated constraints. At a minimum, such policies need to clearly identify company data ownership and employee roles for security oversight and their inherent privileges, including:

- Necessary roles, and the privileges and constraints accorded to those roles
- The types of employees who should be allowed to assume the various roles
- How long an employee may hold a role before access rights must be reviewed
- If employees may hold multiple roles, the circumstances defining when to adopt one role over another

Depending on the types of data regularly handled by your business, it may also make sense to create separate policies governing who is responsible for certain types of data. For example, a business that handles large volumes of personal information from its customers may benefit from identifying a sole manager for customers' private information. The manager could serve not only as a subject matter expert on all matters of privacy, but also as the champion for process and technical improvements to handling of personal information.

Develop a privacy policy.

Privacy is important for your business and your customers. Continued trust in your business practices, products and secure handling of your clients' unique information impacts your profitability. Your privacy policy is a pledge to your customers that you will use and protect their information in ways that they expect and that adhere to your legal obligations.

Your policy should start with a simple, clear statement describing the information you collect about your customers (physical addresses, email addresses, browsing history, etc), and what you do with it. There are a growing number of regulations protecting customer and employee privacy, such as the Data Protection Act, which often carry costly penalties for privacy breaches.

That's why it's important to create your privacy policy with care and post it clearly on your website. It's also important to share your privacy policies, rules and expectations with all employees and partners who may come into contact with that information. Your employees need to be familiar with your privacy policy and what it means for their daily work routines.

Establish an employee internet usage policy.

The limits on employee internet usage in the workplace vary widely from business to business. Your guidelines should allow employees the maximum degree of freedom they require to be productive (for example, short breaks to surf the web or perform personal tasks online have been shown to increase productivity). At the same time, rules of behaviour are necessary to ensure that all employees are

aware of boundaries, both to keep themselves safe and to keep your company successful. Some guidelines to consider:

- Personal breaks to surf the web should be limited to a reasonable amount of time and to certain types of activities.

- If you use a web filtering system, employees should have clear knowledge of how and why their web activities will be monitored, and what types of sites are deemed unacceptable by your policy.

- Workplace rules of behaviour should be clear, concise and easy to follow. Employees should feel comfortable performing both personal and professional tasks online without making judgement calls as to what may or may not be deemed appropriate. Businesses may want to include a splash warning upon network sign-on that advises employees about the company's internet usage policy so that all employees are on notice.

Establish a social media policy.

Social networking applications present a number of risks that are difficult to address using technical or procedural solutions. A strong social media policy is crucial for any business that seeks to use social networking to promote its activities and communicate with its customers. At a minimum, a social media policy should clearly include the following:

- Specific guidance on when to disclose company activities using social media, and what kinds of details can be discussed in a public forum

- Additional rules of behaviour for employees using personal social networking accounts to make clear what kinds of discussion topics or posts could cause risk for the company

- Guidance on the acceptability of using a company email address to register for, or get notices from, social media sites

- Guidance on selecting strong passwords for social networking accounts

All users of social media need to be aware of the risks associated with social networking tools and the types of data that can be automatically disclosed online when using social media. Taking the time to educate your employees on the potential pitfalls of social media use may be the most beneficial social networking security practice of all.

Identify potential reputation risks.

All organisations should take the time to identify potential risks to their reputations and develop a strategy to mitigate those risks with policies or other measures as available. Specific types of reputation risks include:

- Being impersonated online by a criminal organisation (such as an illegitimate website spoofing your business name and copying your site design, then attempting to defraud potential customers via phishing scams or other methods)

- Having sensitive company or customer information leaked to the public via the web

- Having sensitive or inappropriate employee actions made public via the web or social media sites

All businesses should set a policy for managing these types of risks and plan to address such incidents if and when they occur. Such a policy should cover a regular process for identifying potential risks to the company's reputation in cyber space, practical measures to prevent those risks from materialising and plans to respond to and recover from incidents as soon as they occur.

Protecting Against Online Fraud

While computers have improved the speed and efficiency of how we work, they have also allowed thieves and con artists an easier avenue by which to steal from people and businesses. One of the ways these cyber criminals use computers to steal is through online fraud, one of the fastest-growing crimes today.

Types of Online Fraud

Your company's intangible assets could be at risk if you or your employees are not mindful of online fraud attempts. Understanding and identifying different types of online fraud could save your company thousands, or even millions of pounds in lost sales, damaged reputation, legal expenses, etc.

- **Social engineering** is the act of taking advantage of human behaviour to commit a crime. Social engineers can gain access to buildings, computer systems and data simply by exploiting the weakest link in a security system—humans. For example, social engineers could steal sensitive documents or place key loggers on employees' computers at a bank—all while posing as an IT consultant from a well-known company. Social engineers can be tough to spot because they are masters at blending in.

- **Phishing** is attempting to acquire information such as usernames, passwords, credit card numbers and other sensitive information by pretending to be a trusted entity in an electronic communication, such as email. One of the more common phishing scams is receiving an email that asks the user to verify his or her account information. A quick check of your email's Spam folder would likely result in a few examples of phishing.

- **Pagejacking and pharming** occurs when a computer user clicks on a link that brings them to an unexpected website. This can happen when a hacker steals part of a real website and uses it in the fake site, causing it to appear on search engines. As a result, users could unknowingly enter personal information or credit card numbers into the fake site, making it easy for a hacker to commit online fraud. Pharming is the name for a hacker's attack intended to redirect a website's traffic to a fake site**.**

- **Vishing** is similar to phishing and pharming, except victims of vishing attacks are solicited via telephone or another form of telecommunications. The hacker can easily pose as a representative of a bank or other institution and collect personal information that way.

Corporate Identity Theft

It doesn't matter if you are a large international company or a local shop, cyber thieves are always looking for their next score. It is often assumed that smaller businesses are too small to escape attention from cyber crooks, but 74 per cent of data breaches were at companies with 100 or fewer employees. No company of any size is completely safe from cyber thieves.

There are many ways a cyber-thief can steal a company's identity in addition to the various types of online fraud listed above:

- **Stealing credit history**: A cyber thief could steal and use a company's credit history for his or her own financial gain, and then use it to set up a dummy company, racking up huge debt for the real company.

- **Rubbish bin diving**: All too often, papers with sensitive information are recklessly tossed in the rubbish bin instead of being properly shredded and discarded.

- **Hacking**: Having proper security measures in place for your computer system is essential to keep intangible assets safe. Make sure you are using firewalls, routers and other security devices to protect your assets.

Prevent Online Fraud

Understanding and being able to identify potential online fraud techniques is the key to keeping your company safe. Use the following tips to protect your intangible assets and ensure protection against a data breach:

- Never give sensitive information like credit card numbers out over the phone unless you know the person on the other line.
- Shred all credit reports and other sensitive data before disposal.
- Educate employees about phishing and pharming scams. Remind them to not click on anything that looks suspicious or seems too good to be true.
- If your company doesn't have an IT department, hire an outside company to set up the proper security measures for your computer network.
- Always monitor credit reports and other financial data for the company. If you see things that don't belong, investigate.
- Do not allow employees to write down passwords in the office.
- Always encrypt sensitive data.

If You are a Victim

It is common to have an 'it will never happen to us' philosophy when it comes to fraud. Unfortunately, that thinking can lead to lax security measures and carelessness when it comes to protecting intangible assets. If you become a victim of online fraud:

- **Act quickly.** Report the fraud immediately to local police. Notify important suppliers, vendors and partners.
- **Alert your customers.** If there is a data breach involving customers' personal information, activate your plan to alert them. This information could be incredibly harmful to your customers, so alert them as soon as possible.
- **Do an investigation.** If you do not have the resources to do an internal investigation, consult a third party. The quicker the breach can be dealt with, the fewer negative effects your company will endure.
- **Take measures to lessen the chance of a future breach.** Fortunately, cases of online fraud can be good learning tools for your company. Analyse why the breach happened and take steps to make sure it doesn't happen again.

Proper Employee Management to Reduce Fraud

It's an employer's worst nightmare—an employee is dissatisfied with his or her job and decides to defraud or steal from the company. There are plenty of stories about employees committing these crimes and causing enormous damage. By recognising signs of occupational fraud and implementing practices to prevent it, you can lead a happy and productive workforce.

Fraud Facts

Types of fraud include embezzling, insider trading, forging checks, expense reports and vendor invoices, or any other type of internal fraud.

The average cost of a cyber attack varied widely—from £115,000 to £1.46 million—depending on the size of the organisation and the nature of the attack. For a small company, this could mean the end of the business. Small businesses are more at risk because owners inherently treat their employees like family, leading to complacency and lax security measures. Small businesses also tend not to have anti-fraud measures in place as many lack the know-how and enforcement capabilities of larger businesses. Nearly half of victim organisations do not recover any losses that they suffer due to fraud.

The Fraud Triangle

Certain conditions are present when an employee commits fraud—these three conditions are known as the 'fraud triangle'.

1. **Motive.** The defrauder must have a motive to commit fraud, and this motive is often pressure. This can come from feeling too much stress at work to meet deadlines or trying to live a lifestyle that is above his or her means. Outside problems can exist as well, such as a gambling addiction. Monetary gain is often the motive behind employee fraud.

2. **Opportunity**. If anti-fraud measures are too lax, the opportunity can be there for fraud to occur. Even if the perpetrator is financially stable, the opportunity to commit fraud for financial gain might be too much to pass up. Being employed in a high-level, trustworthy position can also lead to opportunity.

3. **Rationalisation.** The perpetrator must be able to justify his or her actions. If employees sense some sort of wrongdoing from the company, they might be able to justify the fraud. They may also tell themselves they are just 'borrowing' money from the company with no intention to pay it back, or they might feel entitled to a raise and will commit fraud to give themselves that 'raise'.

Understanding these conditions can be the key to recognising if fraud is occurring at your business.

Recognising Employee Fraud

It is often difficult to recognise when a fraudulent act has occurred. Frauds last a median of 18 months before being detected, according to the ACFE study. Workplace frauds are much more likely to be detected by anonymous tip than by any other means. Because of this, many companies have set up employee tip lines to try and catch the person(s) responsible for wrongdoing.

While detecting fraud may be a difficult task, there are a variety of warning signs that an employee might be defrauding your business, including the following:

- **Invoices from fake vendor**: an employee can create a fictitious vendor, post a cheque to the fake vendor with your business' name on it and then cash the cheque for themselves.

- **Missing property**: laptops or other computing equipment can be an easy target for employees.

- **Fraudulent expense reports**: some company reports are merely skimmed over for approval, offering an employee an easy way to fake expenses.

- **Forged cheques**: if an employee consistently works around a high-level executive, it becomes easy for the employee to forge signatures.

- **Employee lives beyond his or her means**: if an employee is living a lavish lifestyle on a modest salary, he or she could defrauding the business. Alternatively, an employee who is having financial troubles yet seems to be living within his or her means may indicate fraud is a possible cause.

- **Unusually close association with a competitor:** if an employee seems to have a close relationship with a direct competitor, he or she could be sharing your trade secrets in return for money.

Preventing Employee Fraud

- If you run a small business, chances are you have a few employees that are in charge of several different areas of the organisation. Split up the duties among a larger pool of employees to decrease the likelihood of fraud.

- Perform a pre-employment screening on all potential employees. A resume might not tell the entire story about a prospective employee's past.

- Let employees know there are policies on employee theft in place. Don't assume they are already aware of the policies and the consequences of fraud.

- Frauds occur most often from employees in one of six departments: accounting, operations, sales, executive/upper management, customer service or purchasing. Recognise these high-risk departments as potential sources of fraud and implement the proper policies to prevent it.

- Establish an anonymous tip line that employees, clients or vendors can use to report cases of fraud.

- Don't get complacent. Any employee can commit fraud at any time. While most fraud is committed for monetary gain, that doesn't mean an employee won't commit fraud if the opportunity is there.

- Conduct random audits. Work with an accounting professional to set up and maintain effective internal financial controls to ensure you're not losing money as a result of fraud.

Proper Employee Management

One of the best ways to prevent employee fraud at your company is to ensure all your employees are satisfied with their work and the company as a whole. Lead by example—if you and your high-level management team conduct business properly and ethically, your employees will likely do the same. Good ethics also carry over into the market, where your company will be looked on favourably, which can lead to higher revenue and greater goodwill from the community.

Reward employees for doing well. Let them know how important they are to the success of the business. Don't emphasise only the things that haven't been achieved—focus on the positive, too.

POLICY

General Email / Internet Security and Use

Location:
Effective Date:
Revision Number:

CUSTOMISE AND ADAPT TO YOUR ORGANISATION'S SPECIFIC NEEDS.

GENERAL SECURITY POLICY

The General Email/Internet Security and Use Policy forms the foundation of the corporate Information Security Programme. Information security policies are the principles that direct managerial decision making and facilitate secure business operations. A concise set of security policies enables the IT team to manage the security of information assets and maintain accountability. These policies provide the security framework upon which all subsequent security efforts will be based. They define the appropriate and authorised behaviour for personnel approved to use information assets.

Applicability

The General Email/Internet Security and Use Policy applies to all employees, interns, contractors, vendors and anyone using assets. Policies are the organisational mechanism used to manage the confidentiality, integrity and availability issues associated with information assets. Information assets are defined as any information system (hardware or software), data, networks and components owned or leased by or its designated representatives.

General Policies

All employees, contractors, vendors and any other person using or accessing information or information systems must adhere to the following policies.

- All information systems within are the property of and will be used in compliance with policy statements.
- Any personal information placed on information system resources becomes the property of .
- Any attempt to circumvent security policy statements and procedures (ie, disconnecting or tunnelling a protocol through a firewall) is strictly prohibited.
- Unauthorised use, destruction, modification and/or distribution of information or information systems is prohibited.
- All users will acknowledge understanding and acceptance by signing the appropriate policy statements prior to use of information assets and information systems.
- At a minimum, all users will be responsible for understanding and complying with the following policy statements:
    - General Security Policy
    - System Security Policy
    - Desktop Service Security Policy
    - Internet Acceptable Use Policy
    - Personal Equipment Policy
    - Virus, Hostile and Malicious Code Policy
- All users will report any irregularities found in information or information systems to the IT team immediately upon detection.
- information systems and information will be subject to monitoring at all times. Use of information systems constitutes acceptance of this monitoring policy.

- Use of any information system or dissemination of information in a manner bringing disrepute, damage or ill-will against is not authorised.
- Release of information will be in accordance with Policy Statements
- Users will not attach their own computer or test equipment to computers or networks without prior approval of the IT team or its designated representative.
- If a user fails to comply with this policy, they will face disciplinary proceedings. Penalties can range from a verbal warning to dismissal. The actual penalty applied will reflect the severity of the violation and prior violations.

SYSTEM SECURITY POLICY

's System Security Policy addresses access control, use of hardware, operating systems, software, servers and backup requirements for all systems maintained and operated by .

Applicability

The System Security Policy applies to all employees, contractors, vendors and any other person using or accessing information or information systems. Exceptions to this policy must be approved by the CIO or his/her designated representative.

Password System Security

In today's information age, poorly selected, reusable passwords represent the most vulnerable aspects of information security. has adopted this policy to ensure that the private information of our clients and our proprietary corporate data are kept secure at all times. -authorised users must comply with creation, usage and storage policies to minimise risk to corporate information assets.

- Passwords will conform to the following criteria:
    - Passwords will be a minimum of seven characters
    - Passwords must consist of at least one uppercase letter, one lowercase letter and one number.
- The sharing of passwords is prohibited.
- Any suspicious queries regarding passwords will be reported to the IT team.
- Passwords will be protected as proprietary information. Writing them down or storing them unencrypted on the information system is prohibited.
- Users will be forced to change passwords every 90 days and may reuse passwords only after 10 different passwords have been used.
- Accounts will be locked out after five failed password attempts in a 30-minute time period. Accounts can be reset by contacting the IT team or by waiting 30 minutes for the account to reset automatically.
- Users will be forced to unlock their computers using their network password after 60 minutes of inactivity on their desktops.
- All system passwords will be changed within 24 hours after a possible compromise.
- When users leave the organisation, their accounts will be immediately disabled or deleted.
- If the user leaving the organisation was a privileged user or a network administrator, all system passwords will be changed immediately.

DESKTOP SERVICES SECURITY POLICY

The Desktop Services Security Policy addresses the authorised and legitimate use of hardware, operating systems, software, LAN, file servers and all other peripherals used to access any information system.

- No software of any kind will be installed onto a laptop or desktop computer without the approval of the IT team.
- Only system administrators will have the ability to install software.
- Unauthorised copying or distributing of copyrighted software is a violation of UK Copyright Law and will not be permitted.
- Personal software will not be installed on any machine.

- Users will not allow non-employees to use any machine or device without authorisation of the IT team.
- The following items are corporate policy for security monitoring:
    - All systems and network activities will be subject to monitoring. Use of systems and networks constitutes consent to this monitoring.
    - Disabling or interfering with virus protection software is prohibited.
    - Disabling or interfering with logging, auditing or monitoring software is prohibited.
    - All desktop services will be subject to inventory and inspection.
    - Security irregularities, incidents, emergencies and disasters related to information or system will be reported to the IT team immediately.
- The following items are corporate policy for system usage:
    - Sabotage, destruction, misuse or unauthorised repairs are prohibited on information systems.
- All repairs will be authorised and performed by the IT team.
    - Desktop resources will not be used to compromise, harm, destroy or modify any other service or resource on the information system.
    - All data on information systems at is classified as company proprietary information.
    - Users will secure all printed material and other electronic media associated with their use of information and information systems.
    - Storage, development or the unauthorised use of tools that compromise security (such as password crackers or network sniffers) are prohibited.

INTERNET ACCEPTABLE USE POLICY

Internet access is provided to employees to conduct business. While these resources are to be used primarily for business, the company realises that employees may occasionally use them for personal matters and therefore provides access to non-offensive personal sites during non-business hours.

- Non-business internet activity will be restricted to non-business hours. actively blocks non-business sites during working hours. Working hours are defined as Monday – Friday from 7:00–12:00 and from 12:45–17:00 hours.
- The definition of non-business sites is the sole discretion of the IT team. This definition can, and will, change without notice as the internet continues to evolve.
- Internet activity will be monitored for misuse.
- Internet activities that can be attributed to a domain address (such as posting to newsgroups, use of chat facilities and participation in email lists) must not bring disrepute to or associate with controversial issues (ie, sexually explicit materials).
- Internet use must not have a negative effect on operations.
- Users will not make unauthorised purchases or business commitments through the internet.
- Internet services will not be used for personal gain.
- Internet users will make full attribution of sources for materials collected from the internet. Plagiarism or violation of copyright is prohibited.
- Release of proprietary information to the internet (ie, posting information to a newsgroup) is prohibited.
- All internet users will immediately notify the IT team of any suspicious activity.
- All remote access to the internal network through the internet will be encrypted and authenticated in a manner authorised by the IT team.
- Accessing personal social networking accounts (including but not limited to Facebook®, Twitter®, Google+®, MySpace®, LinkedIn®, Foursquare® and TUMBLR®) or using email for social networking purposes is prohibited during working hours. The use of social networking sites for specific business purposes must be pre-approved or assigned by a manager/supervisor.

EMAIL SECURITY POLICY

The Email Security Policy specifies mechanisms for the protection of information sent or retrieved through email. In addition, the policy guides representatives of in the acceptable use of email. For this policy, email is described as any computer-based messaging including notes, memos, letters and data files that may be sent as attachments.

Applicability

The Email Security Policy applies to all employees, contractors, vendors and any other person using or accessing information or information systems. Exceptions to this policy must be approved by the CIO or his/her designated representative.

Policy

Authorised users are required to adhere to the following policies. Violators of any policy are subject to disciplinary actions, up to and including termination.

The following items are the corporate policy statements for Access Controls:

- All email on the information systems, including personal email, is the property of . As such, all email can and will be periodically monitored for compliance with this policy.
- Individual email accounts are intended to be used only by the person to whom they are assigned. Special arrangements can be made to share information between team members, such as between a producer and an account representative. In all other cases, no user is authorised to open or read the email of another without the express consent of senior management (ie, CEO, COO, CFO, CIO or VP of HR).
- Email is provided to the users of primarily to enhance their ability to conduct business.
- Email will be stored on the system up to a maximum of 75 MB per mailbox. Mailbox is defined as the combined total of deleted items, inbox, sent items and any user-created email folders. Users will receive a warning message stating that they need to clear out space when their mailbox size reaches 50 MB. However, once the mailbox storage space exceeds 75 MB, users will not be able to send new messages until the mailbox size falls below the 75 MB limit. In all cases, however, users will continue to receive incoming messages.
- The maximum size of any individual incoming email message will be 20 MB.
- Terminated employees will have all email access immediately blocked.
- Users who leave the company will have all new emails automatically forwarded to their supervisor, or their designated representative, for 30 days.
- The former employee's supervisor is responsible for disseminating stored emails to the appropriate party. Thirty days after the date of termination, the former employee's mailbox will be permanently removed from the system.

The following items are the corporate policy statements for Content:

- Use of profane, inappropriate, pornographic, slanderous or misleading content in email is prohibited.
- Use of email to spam (ie, global send) is prohibited. This includes the forwarding of chain letters.
- Use of email to communicate sexual or other harassment is prohibited. Users may not include any words or phrases that may be construed as derogatory based on race, colour, sex, age, disability, national origin or any other category.
- Use of email to send unprofessional or derogatory messages is prohibited.
- Forging of email content (ie, identification, addresses) is prohibited.
- All outgoing email will automatically include the following statement: 'This email is intended solely for the person or entity to which it is addressed and may contain confidential and/or privileged information. Any review, dissemination, copying, printing or other use of this email by persons or entities other than the addressee is prohibited. If you have received this email in error, please contact the sender immediately, and delete the material from your computer'.

The following items are the corporate policy statements for Usage:

- Any email activity that is in violation of policy statements or that constitutes suspicious or threatening internal or external activity will be reported.
- When sending email, users should verify all recipients to whom they are sending the message(s).
- Be aware that deleting an email message does not necessarily mean it has been deleted from the system.

PERSONAL EQUIPMENT POLICY

This policy provides guidelines for using corporate IT support resources for personally owned equipment and related software including, but not limited to: notebook computers, desktop computers, personal digital assistants (PDAs), smartphones and mobile phones.

Applicability

The Personal Equipment Policy applies to all employees, contractors, vendors and any other person using or accessing information or information systems. Exceptions to this policy must be approved by the CIO or his/her designated representative.

General Policy

recognises that personally owned equipment can play a valuable role in convenience, efficiency and productivity of its employees. Nonetheless, the use of corporate resources, human or otherwise, for personal gain must be monitored closely.

As a general rule, employees of will not use or request corporate IT resources in the use, network connectivity or installation of their personally owned equipment or software.

Personally owned notebooks and desktop computers will not be granted direct physical access to the network. Employees that wish to access the network from a remote location using their personally owned computer may do so using only -authorised software and only with the approval of the employee's supervisor or manager.

PDAs and smart phones, which include devices using BlackBerry®, iPhone®, Windows Mobile®, Android®, Linux® and Palm® technologies, will be supported according the following rules:

- Employees are responsible for learning, administering, installing and setting up their own PDAs or smartphones.
- Corporate IT resources should not be used for assistance in the basic operation of these devices.
- Upon request, the IT team will install the necessary synchronisation software to the employee's desktop or notebook computer.

VIRUS, HOSTILE AND MALICIOUS CODE SECURITY POLICY

The intent of this policy is to better protect assets against attack from destructive or malicious programmes.

- Any public domain, freeware or shareware software will be evaluated by the IT team prior to installation on any company resource.
- No unauthorised software will be downloaded and installed on end user machines without express approval from the IT team.
- System users will not execute programmes of unknown origin, as they may contain malicious logic.
- Only licensed and approved software will be used on any company computing resource.
- All licensed software will be write-protected and stored by the IT team.
- users will scan all files introduced into its environment for virus, hostile and malicious code before use.
- The IT team will ensure that obtains and deploys the latest in virus protection and detection tools.
- All information systems media, including disks, CDs and Universal Serial Bus (USB) drives, introduced to the environment will be scanned for virus, hostile and malicious code.
- All emails will be scanned for virus, hostile and malicious code.
- All internet file transfers will be scanned for virus, hostile and malicious code.
- The unauthorised development, transfer or execution for virus, hostile and malicious code is strictly prohibited.
- All users will report any suspicious occurrences to his/her supervisor or the IT team immediately.
- All company systems will be protected by a standard virus protection system.
- Virus engines and data files will be updated on at least a monthly basis.
- Viruses that are detected on a user's workstation will be reported to the IT team immediately for action and resolution.

- Anomalous behaviours of any software programme will be reported to the IT team immediately.

Facebook® is a registered trademark of Facebook, Inc. Twitter® is a registered trademark of Twitter, Inc. Google+® is a registered trademark of Google, Inc. MySpace® is a registered trademark of MySpace, Inc. LinkedIn® is a registered trademark of LinkedIn Corporation. Foursquare® is a registered trademark of Foursquare Labs, Inc. TUMBLR® is a registered trademark of Tumblr, Inc.

BlackBerry® is a registered trademark of Research in Motion Limited. iPhone® is a registered trademark of Apple, Inc. Windows Mobile® is a registered trademark of Microsoft Corporation. Android® is a registered trademark of Google, Inc. Linux® is a registered trademark of Linux Online, Inc. Palm® is a registered trademark of Palm, Inc.

General Email/Internet Security and Use Policy

Security of information, and the tools that create, store and distribute that information are vital to the long-term health of our organisation. It is for this reason we have established our General Email/Internet Security and use Policy.

All employees are expected to understand and actively participate in this programme. encourages its employees to take a proactive approach in identifying potential problems or violations by promptly reporting them to their supervisor.

Prior to using equipment, each employee is expected to have read the entire General Email/Internet Security and Use Policy, which includes:

- General Security Policy
- System Security Policy
- Desktop Service Security Policy
- Internet Acceptable Use Policy
- Personal Equipment Policy
- Virus, Hostile and Malicious Code Policy

If you have any uncertainty regarding the content of these policies, you are required to consult your supervisor. This should be done prior to signing and agreeing to the General Email/Internet Security and Use Policy.

I have read and understand ’s General Email/Internet Security and Use Policy, and I understand the requirements and expectations of me as an employee.

Employee Signature: _____

Date: _____

POLICY

Data Breach Response

Location:
Effective Date:
Revision Number:

CUSTOMISE AND ADAPT TO YOUR ORGANISATION'S SPECIFIC NEEDS.

PURPOSE

This policy establishes how will respond in the event of a data breach, and also outlines an action plan that will be used to investigate potential breaches and to mitigate damage if a breach occurs. This policy is in place to both minimise potential damages that could result from a data breach and to ensure that parties affected by a data breach are properly informed of how to protect themselves.

SCOPE

This policy applies to all incidents where a breach of customer or employee personal identifying information is suspected or confirmed.

DEFINITIONS

Personal Identifying Information (PII): information that can be used to distinguish or trace an individual's identity. PII includes, but is not limited to, any of the following:

- Credit card information (credit card numbers—whole or part, credit card expiry dates, cardholder names, cardholder addresses)
- VAT identification numbers; business identification numbers; employer identification numbers
- Biometric records (fingerprints; DNA, or retinal patterns and other measurements of physical characteristics for use in verifying the identity of individuals)
- Payroll information (pay cheques, paystubs)
- Medical information for any employee or customer (doctor names and claims, insurance claims, prescriptions, any related personal medical information)
- Other personal information of a customer, employee or contractor (dates of birth, addresses, phone numbers, maiden names, names, customer numbers)

Breach: any situation where PII is accessed by someone other than an authorised user, for anything other than an authorised purpose.

POLICY GUIDELINES

Upon Learning of a Breach

A breach or a suspected breach of PII must be immediately investigated. Since all PII is of a highly confidential nature, only personnel necessary for the data breach investigation will be informed of the breach. The following information must be reported to appropriate management personnel:

- When (date and time) did the breach happen?
- How did the breach happen?
- What types of PII were obtained? (Detailed as possible: name, account number, password, etc.) How many customers were affected?

Management will then make a record of events and people involved, as well as any discoveries made over the course of the investigation and determine whether or not a breach has occurred.

Perform a Risk Assessment

Once a breach has been verified and contained, perform a risk assessment that rates the:

- Sensitivity of the PII Lost (Customer contact information alone may present much less of a threat than financial information)
- Amount of PII Lost and Number of Individuals Affected
- Likelihood PII Is Usable or May Cause Harm
- Likelihood the PII Was Intentionally Targeted (increases chance for fraudulent use)
- Strength and Effectiveness of Security Technologies Protecting PII (eg encrypted PII on a stolen laptop. Technically stolen PII but with a greatly decreased chance of access.)
- Ability of to Mitigate the Risk of Harm

All information collected during the risk assessment must then be compiled into one report and analysed. The Risk Assessment must then be provided to appropriate personnel in charge of data breach response management.

Notifying Affected Parties

Responsibility to notify is based both on the number of individuals affected and the nature of the PII that was accessed. Any information found in the initial risk assessment will be turned over to a competent legal professional of who will review the situation to determine if, and to what extent, notification is required. Notification should occur in a manner that ensures the affected individuals will receive actual notice of the incident. Notification will be made in a timely manner, but not so soon so as to unnecessary compound the initial incident with incomplete facts or to make identity theft more likely through the notice.

In the case that notification must be made:

- Only those that are legally required to be notified will be informed of the breach. Notifying a broad base when it is not required could cause raise unnecessary concern in those who have not been affected.
- A physical copy will always be posted to the affected parties no matter what other notification methods are used (eg phone or email).
- A help line will be established as a resource for those who have additional questions about how the breach with affect them.

The notification letter will include:

- A brief description of the incident. The nature of the breach and the approximate date it occurred.
- A description of the type(s) of PII that were involved in the breach. (The general types of PII, not an individual's specific information.)
- Explanation of what is doing to investigate the breach, mitigate its negative effects and prevent future incidences.
- Steps the individual can take to mitigate any potential side effects from the breach.
- Contact information for a representative who can answer additional questions.

Mitigating Risks

Based off the findings of the risk assessment, a plan will be developed to mitigate risk involved with the breach. The exact course of action will be based on the type of PII that was involved in the data breach. The course of action will aim to minimise the effect of the initial breach and to prevent similar breaches from taking place.

- Affected individuals will be notified as soon as possible so they can take their own steps to mitigate potential risk.
- If there is a substantial concern for fraudulent use of PII, will offer affected individuals free access to a credit monitoring service.

 will also provide steps to mitigate risks that can be taken by affected individuals. The steps provided to affected individuals will depend on the nature of the data breach. If the breach has created a high risk for fraudulent use of financial information, customers may be advised to:

- Monitor their financial accounts and immediately report any suspicious or fraudulent activity.
- Contact credit bureaus and place an initial fraud alert on their credit reports. This can be extremely helpful in situations where PII that can be used to open new accounts.
- Avoid attempts from criminals that may see the breach as an opportunity to pose as employees in an attempt to deceive affected individuals into divulging personal information.

- File a report with appropriate agencies, regulators, local police or in the community where the breach took place.
- If required, complete an Information Commissioner's Office Security Breach Notification Form found at: www.ico.gov.uk/for_organisations/data_protection/~/media/documents/library/Data_Protection/Forms/security_breach_notification_form_v3_012012.ashx.

Instructions on what steps a customer can take to reduce their risk will be included in the notification letter. In addition to the information listed above, appropriate personnel, when possible, will provide additional information tailored to the individual breach.