Loss Prevention Standards – Asset Classes

Cyber Security - Homeworking

Version: 1.4
Date: 06th August 2024

This document provides guidance on implementing cyber security controls and procedures to protect assets when employees work remotely.

AVIVA

Cyber Security: Homeworking

Introduction

As the business world continues to navigate the new normal of remote working, it is necessary that organisations ensure all online activities are protected. The progression of technology and the reliance on the internet, has made working from home a necessity in many organisations (especially post 2020), but this way of working comes with its own challenges, especially in relation to cyber security. Cyber security threats are becoming more prevalent and sophisticated, making it increasingly more important for organisations to be aware of the risks and implement effective security measures.

With any remote working, it is important to establish clear policies and procedures that are regularly reviewed and updated to ensure the highest level of protection is maintained against cyberthreats. This document will help employers and employees work safely from home, discuss the importance of network security, password management, privacy, and safe device use. By implementing these recommendations, organisations can maintain a productive, efficient, and secure remote workforce. This is of utmost importance in our increasingly connected world.

Recommendations For Cyber Security When Remote Working

Password Complexity and Management

It is essential for businesses to protect their information and data stored by ensuring users access systems by entering a strong password. A system needs to be in place to make sure rules are complied with. Using capitals, lower case letters, numbers, and special characters over a minimum number of digits, usually eight (the more the better) is a good rule, for example, £Magenta6. The National Cyber Security Centre recommends using three random words, for example, bluemonkeyflag, and this could be made more complex and secure by adding numbers and special characters, e.g., 27bluemonkeyflag&.

There are certain words/details that should never be used, such as, date of birth, place of birth, favourite sports team, pet's name, partners name, or children's name, etc. These can be found by cyber criminals or could be relatively easy to guess.

Multi-factor Authentication (MFA)

Having two forms of identification to gain access is a simple and effective way to increase your information/data security. This can be achieved by password and then a randomly generated code, sent to you by text message or an app. There are several ways to provide MFA, and this will greatly increase security.

User Privileges

A rule that should be always applied, but especially important where employees are working remotely. In short, give individuals access only to those systems, functions, software, and areas that they need to do their job. Allowing wide or open access can provide employees with access to secure areas of the business, that they may not even realise they have. This could leave this open to cyber criminals, should they gain access into a user account.

Virtual Private Networks (VPN)

A VPN extends a private network across a public network, allowing users to send and receive data as if their devices were connected to the private network. This will give the data the benefit of the private network's security including password protection, and encryption.

Removable Media

Unsolicited SD cards or USB memory sticks can introduce viruses into a computer, which can spread through a network. There should be a policy that no removable media is to be used, and the ports on devices disabled to protect against this threat. Where memory sticks have previously been used internally in the business, use email or cloud storage to transfer the data instead.

Use of Own Equipment

Allowing users to access a business's network from their own devices can introduce security issues and should be prohibited. Any device supplied by the business should be of standard build with consistent security measures and restrictions in place to protect the business's data and information.

A user's own laptop for example, could already be infected and introduce a virus into the network. Even if it is not infected it could well have out of date security or anti-virus software. There can be the issue of individuals sharing use of the device with family members, increasing the potential for accidental data loss. It could also be that data loss, or an infiltration, goes on longer without detection due to the lack of monitoring, etc.

Anti-virus and Software Updates

Sometimes software updates can be an irritation to users, as they can take time, but it cannot be emphasised strongly enough that as soon as an update is available it should be completed. This point should be made clear to all employees, as the latest updates will also include the latest security improvements. Where possible software and anti-virus updates should happen automatically on employee hardware.

Quick Reference Guides

If a business has many remote workers, e.g., because of an incident closing a building, or a sudden pandemic outbreak, then uncertainty about accessing the network remotely, or unfamiliarity with different systems and applications, can give rise to increased query traffic to an IT Helpdesk. Production of easy to use, brief and accurate 'How To' user guides can reduce the impact on the IT Team and reduce the chance of employees creating an IT security issue.

Encryption

This is the process of encoding a message or information in such a way that only authorised parties can access it. It will not on its own, stop a cyber-attack, but it does make the data contained there useless to the cybercriminal. This is a very good security measure and should be considered to protect all data being transferred.

Phishing

Phishing is defined as untargeted, mass emails sent to many people asking for sensitive information such as bank details, or encouraging them to click on a link, or visit a fake website.

Training employees to recognise a phishing email is essential, as they can be very convincing, but there are some points to remember:

- Look at the email address it has come from.
    - If it is supposed to come from a named organisation, does the email address look correct?
- Look at the grammar and spelling.
    - If the email is supposed to be from a reputable organisation, they would be far less likely to make such basic mistakes.
- Is it addressed to you by name?
    - If it is simply to Dear Customer, that can be a sign the sender does not know you or deal with you.
- Threats requesting payment.
    - Send details 'within 24 hours', etc., is not a usual business practice.
- Is it too good to be true?
    - As an example, a phishing attempt saying 'you have won a dream holiday' may need looking into in more detail. You would more than likely remember entering such a competition. Check the sender address or search the internet for the details.

Public Places

There are three main things to keep in mind when using devices in public:

1. **Security**: All users should receive device security training, i.e., to never leave devices unattended in public.
    - Even if using washroom facilities, phone, tablet, laptop etc. should be taken with you.
2. **Data**: Users should be aware of what's around them. Can someone look over your shoulder, etc? They not only could see what's on your screen, but may see keystrokes, etc. that give away passwords.
3. **Wi-Fi**: A public access wi-fi, in a coffee shop for example, with no password, has easy access for cyber criminals.
    - These should not be used at all.
    - Even if a password is required.
        - It may be available to everyone e.g., displayed on a wall.
        - It may not have been changed for months and may be seen from outside.
    - If a user must use a wi-fi hotspot, a mobile phone's 4G network has inbuilt security and tethering that improves the security.

Reporting Security Issues

Employees should be made aware that time is of the essence when it comes to reporting any security incident. Whether it's a lost phone, a stolen laptop, any breach of a system or a network, clicking on a bad email attachment or a link that doesn't look right, a password you think may be compromised, or any other threat or activity that causes a user concern. Being able to assess the situation quickly and organise a suitable response could help maintain a level of security, limit losses, speed up recovery and increase the chances of a perpetrator being caught.

Definitions

Antivirus: Software designed to detect, stop, and remove viruses and other kinds of malicious software.

Phishing: Defined as untargeted mass emails attempting to get a person to provide sensitive information. Within this there are two other terms:

- **Spear-phishing:** Targeted form of phishing. The email is designed to look like it's from a person the recipient knows and/or trusts.
- **Whaling:** Highly targeted phishing attacks (masquerading as legitimate emails) that are aimed at senior executives

Vishing: is a cybercrime that uses the phone to steal personal information from a victim.

Trojan: A type of malware (malicious software) or virus designed as legitimate software, that is used to hack into the victim's computer.

Ransomware: Malicious software that makes data unusable until the victim makes a payment.

Social Engineering: Manipulating people into carrying out specific actions or divulging information that is of use to an attacker.

Water-holing: Setting up a fake website (or compromising a real one) to exploit visiting users.

Sources and Useful Links

- National Cyber Security Centre (NCSC)
- ActionFraud

Additional Information

To find out more, please visit Aviva Risk Management Solutions or speak to one of our advisors.

Email us at riskadvice@aviva.com or call 0345 366 6666.*

*The cost of calls to 03 prefixed numbers are charged at national call rates (charges may vary dependent on your network provider) and are usually included in inclusive minute plans from landlines and mobiles. For our joint protection telephone calls may be recorded and/or monitored.

Please Note

This document contains general information and guidance only and may be superseded and/or subject to amendment without further notice. Aviva has no liability to any third parties arising out of ARMS' communications whatsoever (including Loss Prevention Standards), and nor shall any third party rely on them. Other than liability which cannot be excluded by law, Aviva shall not be liable to any person for any indirect, special, consequential or other losses or damages of whatsoever kind arising out of access to, or use of, or reliance on anything contained in ARMS' communications. The document may not cover every risk, exposure or hazard that may arise and Aviva recommend that you obtain specific advice relevant to the circumstances.

06th August 2024

Version 1.4

ARMSGI242024

LOSS PREVENTION STANDARDS