Westerly Owners' Association

WESTERLY OWNERS' ASSOCIATION INFORMATION ASSURANCE

By
Robert Walker CEng, MIET, Rear Commodore WOA

TABLE OF CONTENTS

CONTENTS

1. INTRODUCTION

1.1 General

1.1.1 The Westerly Owners Association (WOA), hereafter referred to as the 'association,' is bound by the Data Protection Act 2018 which is the UK's implementation of the General Data Protection Regulation (GDPR) and everyone responsible for using personal data must follow strict rules called 'data protection principles.'

1.1.2 The personal information of circa 3 thousand members is the responsibility of the Association to ensure that it is adequately protected and to recognise the risk, accountability and resilience against the loss of such data.

1.1.3 This White Paper will address the risks, our accountability and resilience to recover from data loss. The final section of this paper is the proposed recommendations to the WOA for review and implementation as necessary.

1.2 Information Assurance Standard (UK)

1.2.1 The primary standard for Information Assurance (IA) in the UK and referenced throughout this paper is:

Information Technology Security Techniques Information Security Management Systems Requirements (ISO/IEC 27001:2022)

1.2.2 The following is an extract from ISO/IEC 27001:2022.

This International Standard has been prepared to provide requirements for establishing, implementing, maintaining and continually improving an information security management

system. The adoption of an information security management system is a strategic decision for an organization. The establishment and implementation of an organization's information security management system is influenced by the organization's needs and objectives, security requirements, the organizational processes used and the size and structure of the organization. All of these influencing factors are expected to change over time.

The information security management system preserves the confidentiality, integrity and availability of information by applying a risk management process and gives confidence to interested parties that risks are adequately managed.

1.3 Data

1.3.1 When we talk about data, it is important to understand what we mean in the context of IA. In general terms, Data is the digital information that encompasses every aspect of information we collect, process, store and communicate which contains personal information as well as administrative data, organisational policies and procedures.

1.3.2 The definition of 'Loss' of data in this paper includes the following:

- Accidental release or loss of data by individuals in the organisation.
- Access by external 3rd parties[1] or individuals within the organisation with malicious intent.
- Denial of Service (DoS), generally caused by malicious software (Malware) to render the Information Technology (IT) useless.

1.4 Scope

1.4.1 The scope shall cover the whole of the IT infrastructure used to perform the association's business. The boundary of the scope must be clearly defined in terms of the business needs and being able to manage it. Figure 1, below illustrates a typical scope and its boundary which is akin to the association.

[1] Within the realms of cyber security, such individuals are referred to as **Threat Actors** who can be individuals, state sponsored or acting for organised crime.

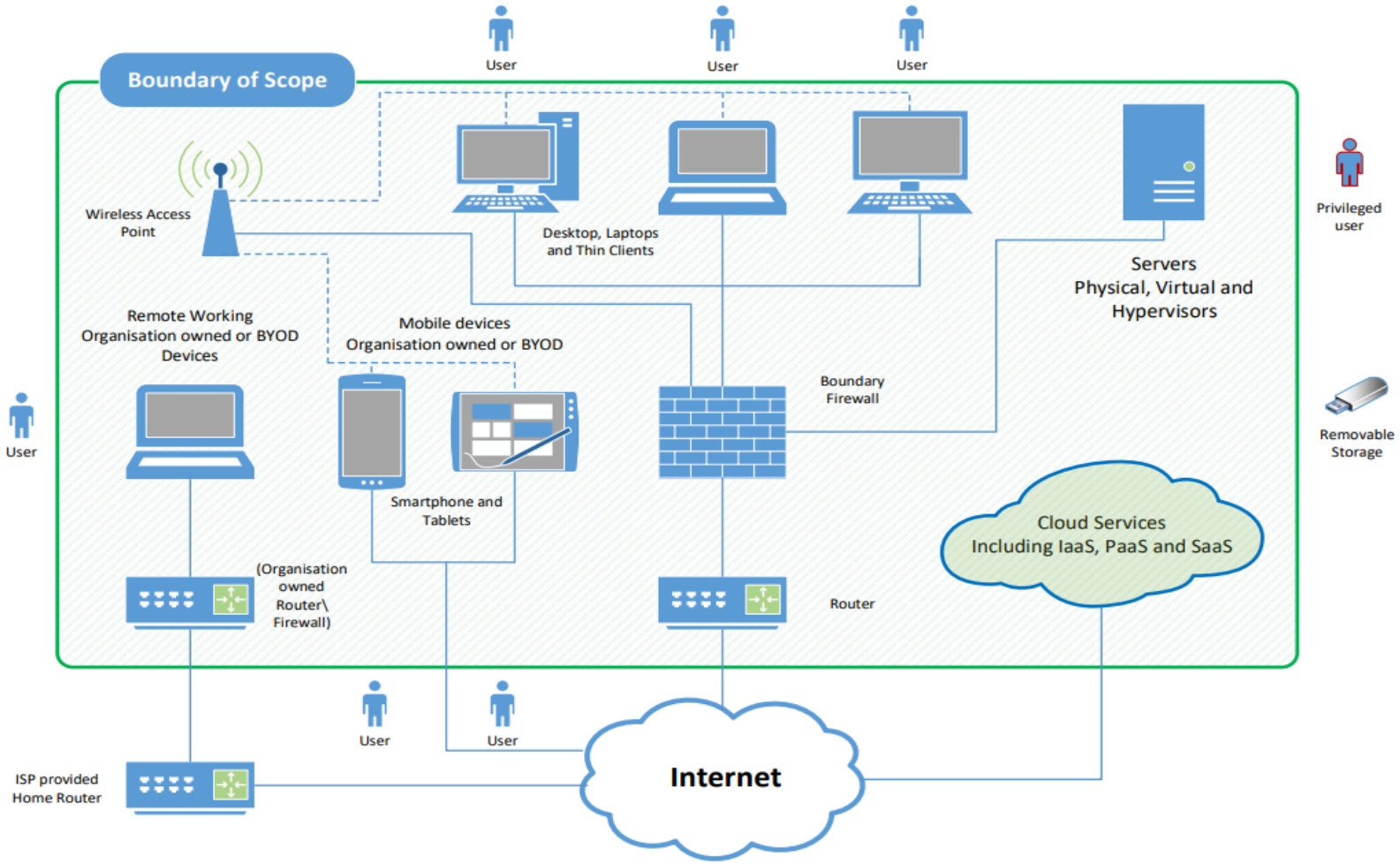


Figure 1: IT Infrastructure Boundary (Courtesy of the National Cyber Security Centre)

2. RISK STATEMENT

2.1 Risk Review & Analysis

2.1.1 A provisional risk assessment was completed on 22 February 2023. The assessment is available electronically along with associated tools and information. This can be obtained by applying to the Rear Commodore rear-commodore@westerly-owners.co.uk

2.1.2 Analysis of the provisional assessment shows 4 critical and 3 major risks. The following table summarises the 4 critical risks.

Security Risk	Information Asset Affected	Business Area Affected	Severity
No information Security Management structure within the Association with a consequent lack of cyber security awareness.	BYOD/PEDs and Cloud Server	Association	Critical
Uncontrolled number of threat vectors created by the transfer, Storage and Processing of personal data on PCs	BYOD/PEDs and Cloud Server	Association	Critical
Inability to recover from a catastrophic loss of data or a Denial of Service	PEDs	Association, AGs	Critical
Yearbook containing personal data falling into the wrong hands which can then be used for malicious purposes	Yearbook	Association	Critical

Table 1: Summary of Critical Risks

2.2 Definition of Severity (Critical)

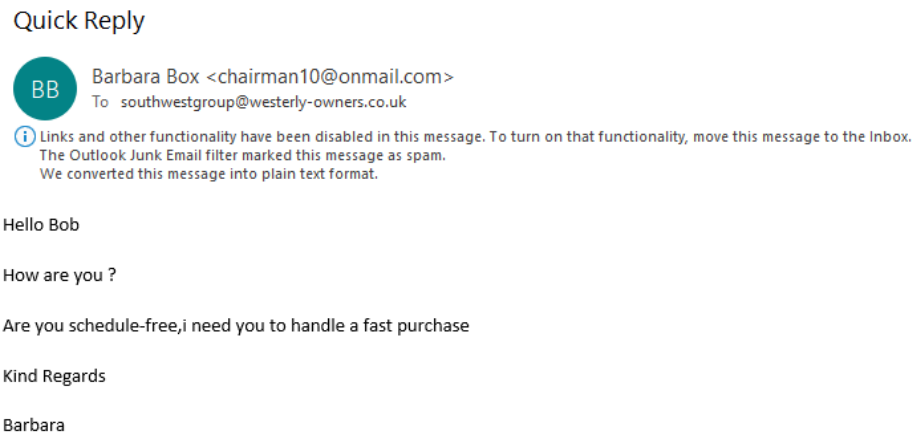
2.2.1 A critical risk is a function of the probability that the event will occur and the severity if it does. For a risk to be critical, the assessment is that the event will almost certainly occur and the consequences to the association can be profound. Once personal data has been released into the public domain either by accident or by malicious intent, then the association can be held responsible for whatever damages have or may occur. Typical definitions for 'Critical' include but not limited to:

- Catastrophic loss or compromise of information asset including an unknown amount of high-level personal data.
- Catastrophic financial loss due to claims for compensation.
- Damage to the Associations reputation.
- Litigation with catastrophic consequences, financial and/or reputational.

Given any of the consequences above, the worst case scenario is that the association will struggle to survive.

Example 1:
Yearbook falling into the wrong hands. A Threat Actor now has the names, telephone numbers and Email address of circa 3,000 association members. This will be enough for threat actors to use vulnerabilities in individuals' security to gain access to their PEDs and to steal private information which an individual could be bribed with.

Example 2:
This email is one of a number received indicating that an Actor has gained association information:


Quick Reply

BB

Barbara Box <chairman10@onmail.com>
To southwestgroup@westerly-owners.co.uk

Links and other functionality have been disabled in this message. To turn on that functionality, move this message to the Inbox.
The Outlook Junk Email filter marked this message as spam.
We converted this message into plain text format.

Hello Bob

How are you ?

Are you schedule-free,i need you to handle a fast purchase

Kind Regards

Barbara

3. KEY FINDINGS

3.1 General Summary

3.1.1 The key findings are in proportion to the size of the association and its structure of volunteers who manage and co-ordinate its activities. This review and the associated risk assessment has revealed critical vulnerabilities in the manner of how the association manages, processes, and distributes personal data of its members. Remedial actions are therefore urgently required but they should be balanced against their severity and realism for a small volunteer organisation which the association is.

3.2 Key Finding #1 (Web Hosting)

3.2.1 The findings show that the association utilises a web hosting environment provided by WordPress. This is a secure cloud-based platform which permits the association to access and edit its own web site. The hosting environment also has several additional applications which the association subscribe to, such as, Mailjet for bulk emails to the members and a Gallery where images and other media types can be linked to its web pages or outgoing emails vial Mailjet. Importantly, this is also the host site for the central register of all members including their personal data. WordPress are entirely responsible for the information security management of this register/database. The findings established that users have set privileges as defined by their role in the association and at AG. This has been established by the association Database Manger using the software tools provided by WordPress. There is also some resilience in that Flag Officers and Stow VA have editorial privileges to change user access if the Database Manger is not available to do so. This setup is necessary, but it does mean that each user represents a Threat Vector with access to the central register of members and services provided by WordPress.

3.2.2 It is also worth noting that no bank account details are held in the database/register.

3.2.3 As WordPress is a secure platform requiring usernames and passwords to access any personal data therein, the findings show that due to the current absence of policies and process in the association for information security management there is a residual risk that third party or threat actor could gain access to the central register if an authorised users username and password have been compromised due to poor diligence or inadequate security protection in their PC/PED.

3.3 Key Finding #2 (Bring Your Own Device)

3.3.1 The greatest risk to IA occurs once personal data is copied or transferred from behind the security of the WordPress site into a PED also referred to as Bring Your Own Device (BYOD).

3.3.2 The findings show that both the association and AG committees, collect, process, store and communicate personal information routinely during their day-to-day activities. In some cases, such information is printed, and hard copies retained for record purposes. Many of these individuals are using PCs with legacy and in some cases obsolete Operating System, but the association cannot dictate to these individuals which versions of the operating system they must use and the same goes for anti-virus software and Virtual Private Networks (VPNs). The significance of the risk must be understood, and this is why!

The risk transpires from what are called 'Zero Day Vulnerabilities.' A Zero Day Vulnerability is a point in time when hackers discover and exploit a flaw in a piece of software that is unknown to the programmer. Many of these applications are inherent to our PCs which operate in the background and we never see or come across them, but they exist to make our PCs function and for us to enjoy the experience. Once a hacker can exploit this flaw, the details tend to be published on the dark web for other hackers to purchase, and this is exactly what happened to Javascript.

Javascript is a small software application which assists our computers to execute and run other programmes and so any Zero Day Vulnerability in Javascript provides hackers with a back door to enter our PCs. Javascript is not the only software to be exploited in this way, MS Windows has also experienced its own problems.

It is a race between hackers and programmers to identify such flaws, the hackers so that they can exploit it and make a bit of money and the programmer to remove the flaw using software patches.

3.3.3 In most cases our PCs are secure from Zero Day Vulnerabilities if we are conscientious in downloading the patches when we are prompted to do so but the findings have shown that some individuals are using unsupported operating systems that cannot be patched and probably haven't, ever? Hence, the risk assessment has flagged this finding as a critical vulnerability.

3.4 Key Finding #3 (Yearbook)

3.4.1 Another Key Finding and the most Critical of all is unfortunately the WOA Yearbook. Whilst this paper has gone into detail regarding information security management in the digital space, we publish it anyway in the Yearbook which therefore invalidates all the digital security measures we

may implement. When a risk is identified especially a critical risk, the first rule is to 'STOP' and cease the activity or seek an acceptable lower risk solution. This will be a contentious decision by the association who love their Yearbook but as times have changed then so must the association to protect not just its members, but its entire wellbeing as highlighted in Paragraph 2.2.

3.4.2 A review of similar yachting associations such as the Royal Yachting Association (RYA) and Royal Naval Sailing Association (RNSA) all secure their personal data behind a secure firewall and none of it is intentionally published in hardcopy or otherwise. By example; the RNSA do allow members with a valid username and password to access the RNSA web site to search the members list as does the association through the WOA web site. Therefore, the association is in line with these other 2 organisations in this respect.

3.4.3 It is currently possible to send a private message and engage in a chat session with other members via the 'Search Yearbook' in the WOA website. This is made possible without visibility of the members contact details which remain securely hidden behind the firewall and the automated software in the site connects the individuals by email or chat. The recipient receives alerts by email and can only view and reply to the message by following the link which requires their association username and password.

This feature is not prominent and doubtless not known to most members of the association. Two actions are recommended;

a. Improve the visibility and utility of this feature to make it more prominent and user friendly.
b. Improve the awareness of this feature with a publicity campaign.

3.4.4 The feature described in the preceding paragraph will somewhat compensate for the removal of personal data from the Yearbook. It is therefore recommended that 2024 Yearbook onwards should only contain the following:

a. Members name
b. Name of their yacht.
c. Class of yacht.
d. Mooring location
e. Area Group(s).

3.4.5 There might also be a benefit to the association with the development of a smart phone app which uses the Automatic Identification System (AIS) of member's yacht to show its location with embedded short cuts to a messaging app. User's of the app can decide on how much information is published, for example there could be an option to show all track/cruise history and proximity alerts to other registered association yachts. WOA could own the Intellectual Property Rights (IPR). This can be discussed at a later date.

3.5 Key Finding #4 (IA Policies & Procedures)

3.5.1 This key finding is the absence of an information security management system within the association. Without this, there is no ownership of responsibility and no policies and procedures to define IA.

3.5.2 Section 4, within the association rules provides a statement on the protection of personal data which is in line with GDPR and all members sign a GDPR declaration on joining the association which permits the association to keep and maintain their personal data along with defining their rights. However, this does not preclude or absolve the association from its responsibility to keep personal information secure as far as is reasonably practical. Until a hierarchy of ownership and responsibilities are defined, agreed and implemented, then a critical risk against the association has been assessed.

3.6 Key Finding #5 (Resilience)

3.6.1 This refers to the absence of any resilience within the association to cope with the loss of data in the event of an accidental or 3rd party intrusion. The finding shows that key individuals in the association and in AGs conduct their day-to-day business on their PEDs. For example; this can be meeting agenda, minutes, actions, event schedules, programmes, bookings, list of attendees, emails and the list goes on. It has been described earlier just how vulnerable PEDs can be to 3rd part intrusion, but even the accidental loss of the data, or broken PC can have a detrimental effect on the organisation.

A live example is the planning and coordination of the Association Summer Cruise 2023 (ASC23), all of which is held on the organiser's PC. In this live example, the organiser has protected this information by copying it to his personal cloud storage as well as the hard drive on his computer. A failure of his computer will barely interrupt his ability to continue with ASC23 planning as he can download the data from the cloud to a spare PC, but in the event of the organiser becoming incapacitated through accident or illness, all the data will not be accessible without his username and password and therefore it is effectively lost to the association.

3.6.2 The solution to this problem is a small investment into a secure cloud file sharing site such as SharePoint, Google Drive and Dropbox etc where documents, files, media and data can be shared securely by named individuals using unique usernames and passwords. It will be important that each AG and the association have their own securely partitioned area which only they will have access to but there will be shared areas where AGs and the association can access to Read Only or Edit according to the permission granted to the individual. In this manner, the ASC23 organiser can save all the information to a shared location where other named individuals can have access privileges. Some such sites also provide change control to documents which only permits one person to edit the document at a time.

3.6.3 This solution will also mitigate the risk of BYOD in that all personal data can be accessed through the secure site rather than keeping it on PEDS.

3.6.4 Some research will be needed to find the ideal file sharing site which is both cost effective and enduring.

4. CONCLUSION

4.1 General Conclusions

4.1.1 It is concluded that the absence of an information security management system within the association is a critical risk. This is solely due to the absence of a hierarchy in the association that takes ownership and the responsibility for Information Assurance from which the policies and procedures should flow down to enable an effective information security management system to be implemented throughout the association and the AGs. This can be achieved internally without the need for outside consultants and will be the enabler to mitigate all the associated risks.

4.2 Takeaways

- Takeaway #1; without the policies and procedures highlighted above, personal data and the breach of GDPR is a critical risk.
- Takeaway #2; the association must implement a hierarchical structure which accepts the ownership and responsibilities for IA which conforms to best practice for a small volunteer organisation which the association is. Best practice is defined in BS EN ISO-IEC 27001-2022.
- Takeaway #3; key findings and risk assessment show critical risks to personal data breaches with a severity which the association may struggle to cope with. These risks will be mitigated by the implementation of a hierarchical structure for IA, from which an effective information security management system can evolve.
- Takeaway #4; there is no resilience in the association to recover from a catastrophic data loss or Denial of Service. This risk can be mitigated with the introduction of an appropriate file sharing site.
- Takeaway #5; the introduction of a secure file sharing site will also mitigate the risk associated with BYOD.
- Takeaway #6; the existence of the Yearbook in its current format invalidates all the digital security measures we may implement. From 2024 onwards, personal data in the Yearbook should be reduced to the members name and the name of their yacht.

- Takeaway #7; The removal of personal data from the Yearbook can be compensated by the secure private messaging function in the association's web site. This does not expose any contact details between individuals.

5. RECOMMENDATIONS

6.1 It is recommended that:

- The association should introduce a hierarchy to take ownership and responsibility for IA.
- Mitigate each of the Critical Risks with the development and implementation of policies and procedures for an information security management system.
- Establish a secure data file sharing site to:
  - Ensure the association and the AGs are resilient to and can recover from a catastrophic loss of data or a denial of service attack.
  - Personal data can be processed and stored securely rather than in PEDS/BYOD.
- Each solution should be commensurate with the association size and voluntary nature of it.
- The 2024 Yearbook onwards should only publish the following:
  - Members name
  - Name of their yacht.
  - Class of yacht.
  - Mooring location
  - Area Group(s).name and name of their yacht.
- Improve the visibility, utility and awareness of the private messaging system.
- The development of a bespoke app for members to track each other using AIS with short cuts to communicate with each other. Potential for IP ownership.