## 

**ezAccount**

Improving network security in a tax accountant office

EXECUTIVE REPORT

Risk Management &

Network Security

Analysis

Yair **Levy •** Federico **Niccolini**

Emanuele **Urselli** **•** Gianmarco **Pastore** **•** Alessandro **Zanatta** **•** Sergio **Parigi** **•** Andrea **Vergori**

# 

# 

# **Table of contents**

[**1 Introduction**](#_hgdt3oi5iwhm) **3**

[**2 Recognize and define the problem**](#_aof5aoz14fez) **4**

[**3 Gather facts**](#_kak0wfew6xzu) **5**

[**4 Project scope, goals and objectives**](#_7oxr1kqcclgi) **6**

[**5 Proposed solution & action plan**](#_g22ht2ow0qdq) **7**

[5.1 Before network improvement](#_meenvsh36ix3) 8

[5.2 After network improvement](#_44o405rdylk9) 9

[5.3 Action Plan](#_ouard3xpwlpl) 10

[**6 Risk Management Analysis (RMA) outline**](#_n9ca9up2hxmr) **12**

[**7 Anticipated project results**](#_4jgujpuv7wx3) **13**

[**8 Proposed costs**](#_ahr87roiorf) **14**

[8.1 Nonrecurring costs](#_3ihmr6boxx7m) 14

[8.2 Recurring costs](#_ukyac2onn3sl) 15

[**9 Conclusions**](#_yiy7lhfed1az) **16**

[**References**](#_auhk0ouln1j5) **17**

# **1 Introduction**

This project is prompted in an effort to mitigate cybersecurity risks and improve the overall security of a tax accountant office owned by Jane Doe. She lives in Tampa (FL) and she is the mother of two teenagers.

The company is composed of 2 offices, one in Tampa, the other in S. Petersburg with a total of 5 employees. It handles financial, accounting and taxation needs so that customers can focus on growing their business. It also supports business operations through the preparation and filing of company tax declarations, maintaining the company accounts and providing treasury services.

EzAccount does not have an IRP nor a BCP, and has a naïve network architecture, which can be the source of many network vulnerabilities. With our intervention we intend to bring the safety level of this company above the average level of the other SME.

## 

# **2 Recognize and define the problem**

For accountants and tax firms, it is part of daily business to work with their customers’ highly sensitive data. The storage and processing of these data and documents has long been fully digital and performed on their own IT systems, as well as on those of specialized IT service providers. Even though much has been done to eliminate IT security vulnerabilities, it is impossible to be completely confident that the privacy is protected, and that customer data is not at grave risk, because every connection with the Internet and every email can pose a potential danger.

Accounting firms are often the victims of cyber-attacks when working with third parties that are not secure, when they have network vulnerabilities, from phishing scams, through social engineering, or having their business email compromised. Moreover, SMEs are at particularly high risk as these firms usually do not have the in-house skills and collective capacity to operate controls efficiently (Parkin et al., 2016, 1-2).

Cyber-attacks can force closing the firm for 2-6 weeks while recovering the data and getting the system back up and running. Moreover, threat actors are known for the complete shutdown of accounting firms, due to excessive economic loss.

​In the event of data loss, the owners violate their professional duty of confidentiality. Not only does this make them fully liable, but they also risk the reputation of their firm and their economic future (Fernandez De Arroyabe & Fernandez De Arroyabe, 2021, 1-4,23).

Of course, the loss of tax returns and financial data not only impacts the firm itself, but clients as well. They will not only have to deal with the cost of the breach by paying a cyber security company to recover and restore your information, but they will also miss on new business opportunities, they will not be able to work on existing business, and they will have to deal with the bad press caused by the data breach.

The IRS has recently issued a warning to taxpayers to beware of scammers calling and emailing them about the stimulus payments from the CARES Act, along with other schemes related to COVID-19, as they could lead to identity theft and tax frauds (*IRS Warns About COVID-19 Economic Impact Payment Fraud*, 2021). Moreover, researchers have found that the number of cyber-attacks has significantly increased during the COVID-19 pandemic. For instance, consider that phishing attacks grew by 600% in March 2020 and have been part of 86% of the total global attacks (Lallie et al., 2021, 3-11).

# **3 Gather facts**

The company represents a small accountancy firm, made up of 5 employees.

The organization consists of two offices that share a common network connection through the use of two suitably configured home routers. A Network Attached Storage (NAS) on each office allows you to perform tasks such as storage and backup.

The main application software used for tax accounting, tax returns and other daily activities is cloud-based.

The owner allows her two children and her customers to use the Wi-Fi connection of the offices and the password is pinned on the board of the meeting room, accessible to anyone.

In addition, the owner often works from home, using the office laptop and accesses the network using the standard VPN of the operating system.

Being a very small business, it does not have the advantage of IT consultancy. The company does not use a firewall to protect its internal, unsegmented network, and the mobile devices used currently do not use a secure VPN.

Unfortunately, the company does not have a business continuity, incident response and business recovery plan.

Corporate IT security risk is managed in an ad hoc manner coupled with a reactive risk management approach.

The overall cybersecurity position for the company is considered a level 1 within the implementation levels of the NIST cybersecurity framework.

# **4 Project scope, goals, and objectives**

Tax preparers, accountants, and auditors, like ezAccount, are working away from their offices as a result of the novel coronavirus pandemic and are at risk of falling prey to cybercriminals.

As a consequence, the scope of this document spans from managerial problems, such as cyber-hygiene and cyber-awareness, to technical aspects, such as network defense.

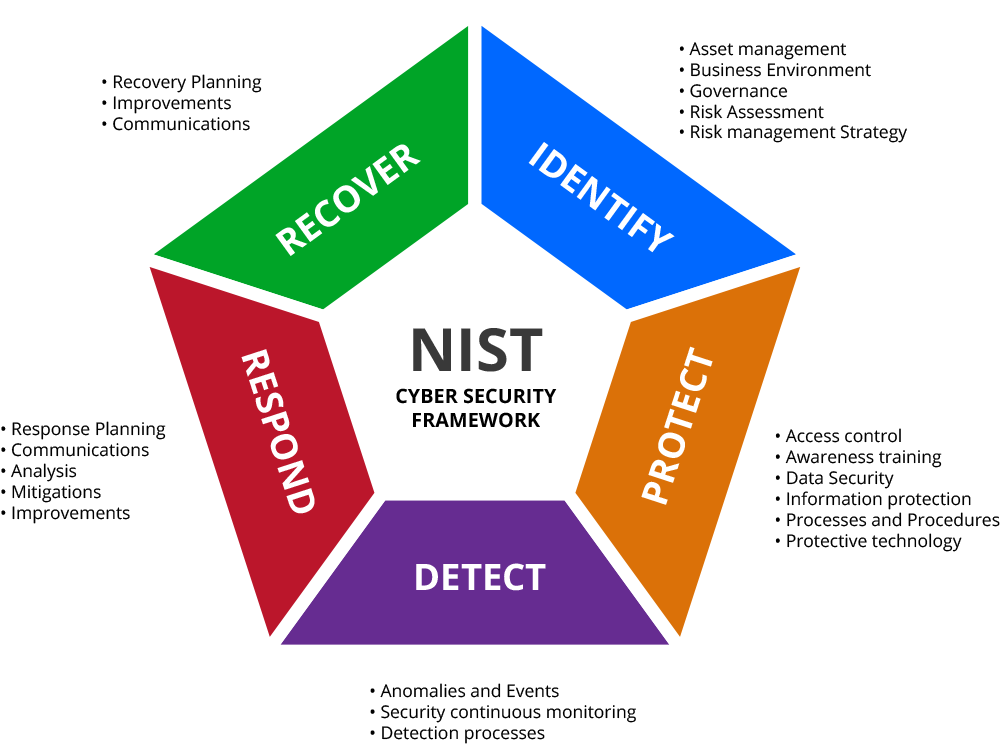
The overall goal is to improve the protection by implementing identity management and access control, to detect anomalies and events and perform a continuous monitoring of the network and the stored data. We will improve the awareness of the employees by means of training sessions. A duly maintenance plan and asset management will be implemented together with a recovery plan.

Our goal is to bring the company to a good overall level of security, according to the NIST framework (Barrett, 2018, 23-44), improving its network architecture, training the employees, and establishing plans for responding and recovering after attacks.

There are three important objectives in our project. The first one is to implement an efficient and safe network architecture by adopting firewalls, VPN, centralized antivirus, IDs. The second is to mitigate many technical problems, like the lack of encryption or unsafe access control policies, in order to provide a mitigation to various common threats. The last one is to train company employees to make them aware of the most common threats and to establish IRP and BCP to improve the resilience of ezAccount.

# **5 Proposed solution & action plan**

We decided to apply the NIST Cybersecurity Framework guidance on how to mitigate cyber threats in order to adopt a comprehensive cybersecurity strategy.



We will implement **identification** in assets both software, hardware, and data flow.

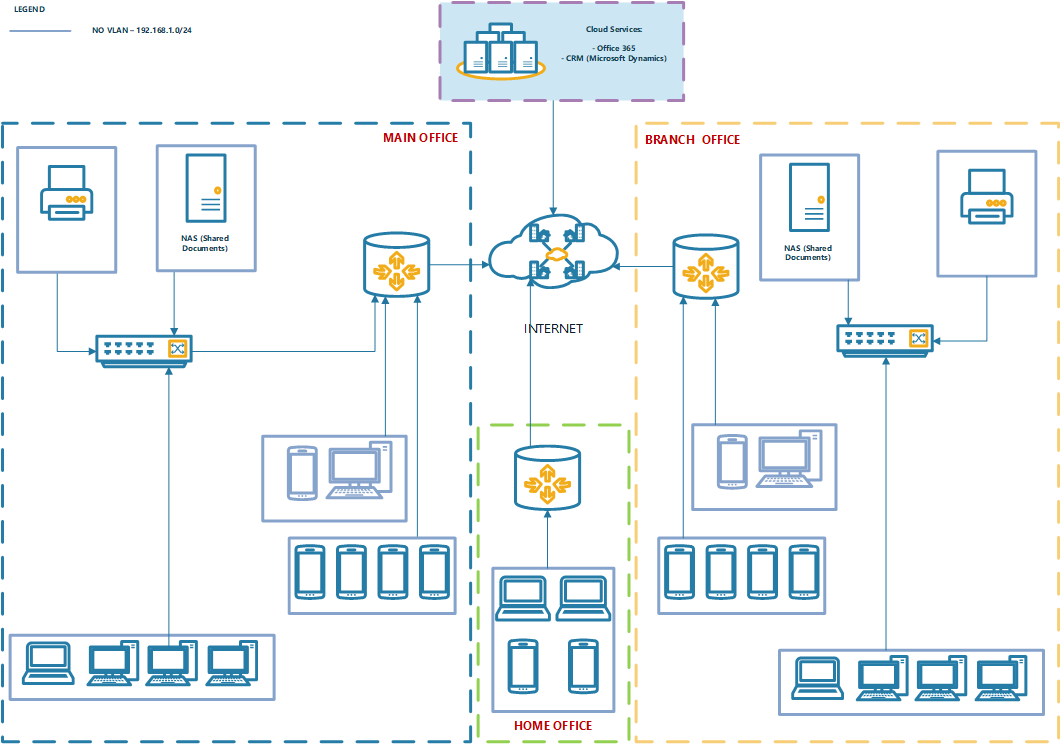
We will **protect** the company by installing devices that allow it to execute Identity Management and Access Control, we will perform training for employees and managers, and we will enforce data security.

We will implement a way to **detect** potential anomalies and events and we will set up a system for continuous monitoring.

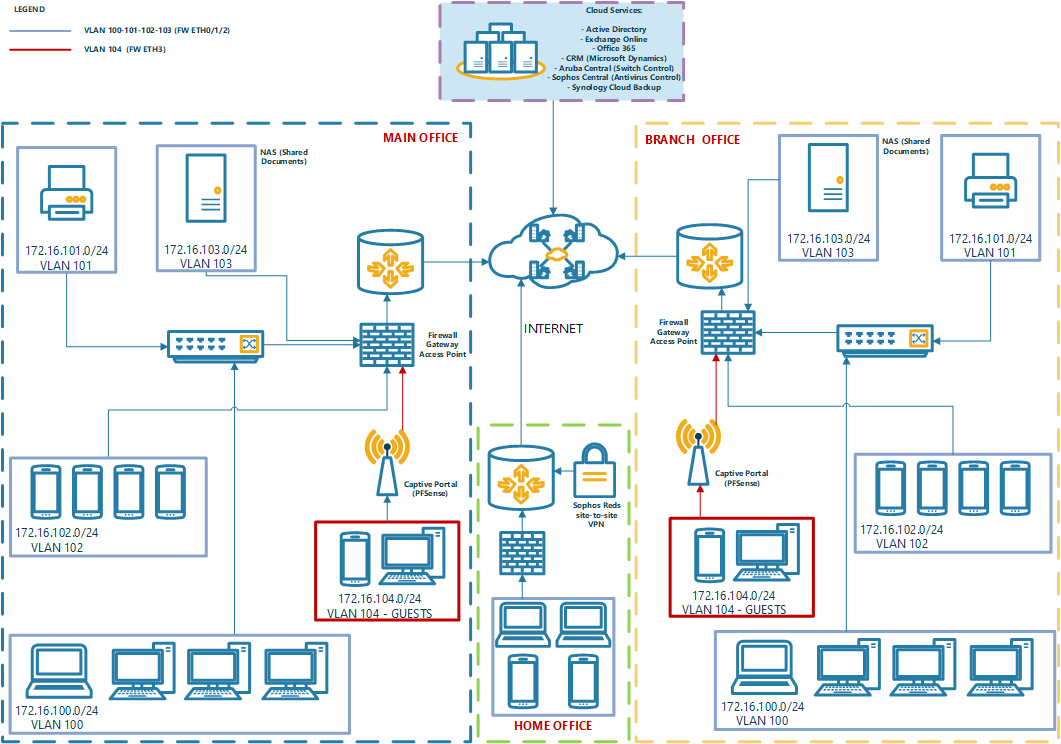
We will also set up a detailed and unambiguous **response** plan in case of attacks.

Finally, a disaster **recovery** and business continuity plan will be designed in order to minimize disruption in company operations.

## **5.1 Before network improvement**



## **5.2 After network improvement**



## **5.3 Action Plan**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ACT\_#** | **Item** | **Description** | **Type** | **NIST Category** |
| ACT-1 | Firewall Installation for both offices, proxy configuration for web site access segmentation, Adoption of VPN with strong encryption. Intrusion detection system (IDS) activation | * Buy two (Sophos UTM9 Firewall). Implement the following features: * Configure Firewall Policies * Configure Navigation Proxy used by company users * Configure the PDS (Proactive Detecting System) * Configure VPN and install VPN client to all devices * Buy one (Sophos RED) for home security connected to Office Firewalls using a fixed VPN connection * Buy one Bitdefender Box Firewall (@ CEO Home) * Buy an HPE Managed Switch (24 ports) * Configure different VLAN for every type of device (wireless, printers, PC and NAS, captive portal) * Install Servers/Network Secure Cabinet * Buy two enterprise level NAS (Synology RS Series) and configure it in cluster mode. The NAS will be installed in the primary office.   Home and branch office can reach the NAS data using fixed VPN   * All NAS data will be saved on cloud using Synology C2 Storage/Backup or a third part service * Buy a BYOD cloud system (Cisco Meraki) | Technical | **PR-AC** |
| * Configure the IDS (Intrusion Detection System) | Technical | **DE.AE** |
| * Buy a (Sophos) Central Antivirus for every device of the organization | Technical | **DE.CM** |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ACT\_#** | **Item** | **Description** | **Type** | **NIST Category** |
| ACT-2 | Employee training about cyber-hygiene and cyber-awareness | * Manager training * Employee training | Managerial | **PR.AT** |
| ACT-3 | Create Business Continuity (BC) and Incident Response (IR) Plan | * Define recovery procedure * Setup Emergency Contact list * Employee Training * Configure automatic security updates | Managerial  Technical | **RC.RP** |
| * Implements a Maintenance Program (update/security fix) | Technical | **PR.MA** |
| * Define Response procedure | Managerial | **RS.CO** |
| * Detailed assets of hardware & software and business data flow | Managerial | **ID.AM** |
| ACT-4 | Use of data encryption on every asset, data synchronization on the cloud. Enroll all mobile devices to BYOD manager.  Least privilege configuration, implementation of role-based access control (RBAC), zero-trust authentication and/or 2FA | * Configure data encryption on each device * Implement backup strategies on BYOD * Configure 2 factor authentication * Configure Role Based Access Control on NAS | Technical | **PR-DS** |

## 

# **6 Risk Management Analysis (RMA) outline**

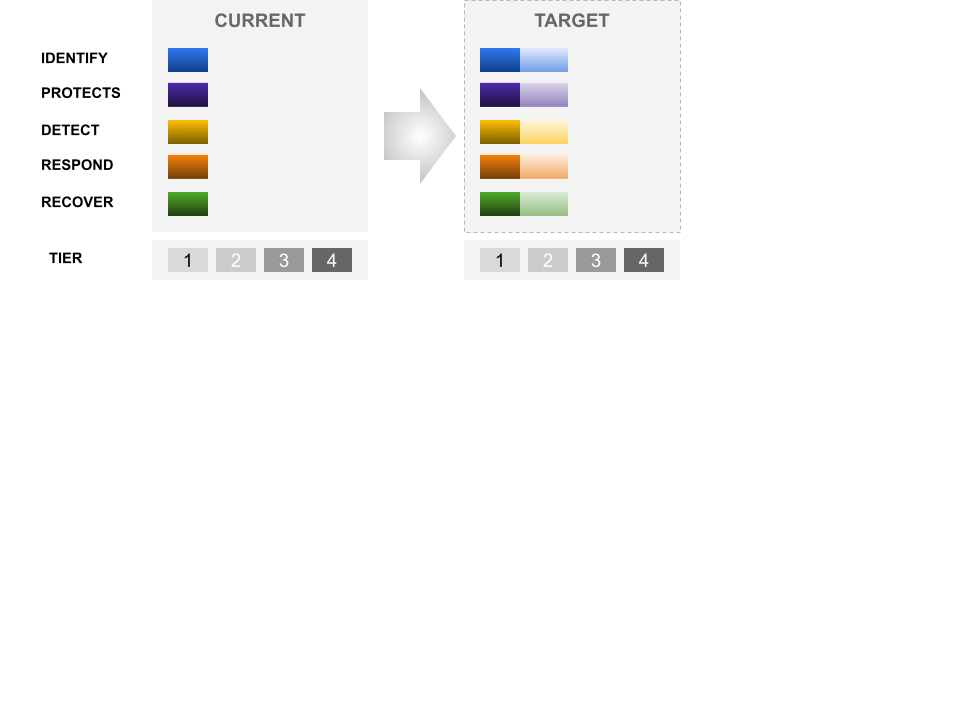
Next, we have the Risk Management Analysis table containing the ranked risks.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Risk rank** | **Threat type** | **Risk description** | **Likelihood of occurrence** | **Impact on organization** | **Mitigation strategy** | **ACT\_ #** |
| 1 | Data breach | Unauthorized disclosure of sensitive customer data, due to data breach | **HIGH** | **HIGH** | Firewall Installation for both offices, proxy configuration for web site access segmentation, Adoption of VPN with strong encryption. Intrusion detection system (IDS) activation | ACT-1 |
| 2 | Ransomware | Network modification, loss of productivity, files and financial loss as a result of revenue generating operations being shut down or/and paying ransom | **HIGH** | **HIGH** | Employee training about cyber-hygiene and cyber-awareness, use of RAID 5, antivirus, disable macro scripts, use of server proxy for internet access | ACT-2 |
| 3 | Data leakage | Loss of data confidentiality, communication confidentiality due to data leakage | **MEDIUM** | **HIGH** | Adoption of VPN with strong encryption | ACT-1 |
| 4 | Unauthorized Remote Access | Loss of confidentiality, integrity and availability. due to unauthorized remote access | **MEDIUM** | **HIGH** | Least privilege configuration, implementation of role-based access control (RBAC), zero-trust authentication and/or 2FA | ACT-4 |
| 5 | Network breach | Loss of confidentiality due to network breach | **MEDIUM** | **HIGH** | VLAN adoption, installation of a captive portal on demilitarized zone (DMZ) | ACT-1 |
| 6 | Business Operation continuity/ recovery risk | Business operation disruption and potentially bankruptcy due to the lack of business continuity plan / Incident Response Plan | **LOW** | **HIGH** | Create Business Continuity (BC) and Incident Response (IR) Plan | ACT-3 |
| 7 | Physical access | Loss of backup data files due to theft of hardware or sabotage | **LOW** | **HIGH** | Use of data encryption on every asset, data synchronization on the cloud. Enroll all mobile devices to BYOD manager | ACT-4 |

For every risk, we have devised that the impact on the organization is high as a successful cyber-attack would result in a catastrophic economic and image damage.

# **7 Anticipated project results**

The expected result of this project allows to considerably increase the level of cybersecurity of the company. Using NIST's cybersecurity framework, it will offer the company an effective and efficient way to comply with it and achieve its intended results. If accepted and implemented correctly by a cybersecurity consultant, the improvement in cybersecurity will be almost immediate. Furthermore, to simplify the aforementioned improvement process, training hours are provided for all company personnel. At the end of the implementation, the company will be able to cope with and / or avoid data breaches, ransomware and malware, data leakage, unauthorized remote accesses and consequent losses of confidentiality, integrity and availability of the data and the service offered, aligning all with a new business continuity, incident response and recovery plan.



As shown in the figure we intend to bring EzAccount, according to the NIST framework, from tier 1 to tier 2, even reaching tier 3 as regards the protection. This is a noticeable improvement that allows the company to resist the most common threats and to recover after attacks.

# **8 Proposed costs**

## **8.1 Nonrecurring costs**

**Activity list**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Action** | **ACT-REF** | **Hours** | **Cost/Hour** | **Price** |
| Configure Firewall Policies | ACT-1 | 4 | € 100 | € 400 |
| Configure Navigation Proxy used by company users | ACT-1 | 4 | € 100 | € 400 |
| Configure the Intrusion Detection System (IDS) | ACT-1 | 4 | € 100 | € 400 |
| Install and configure VPN client to all devices | ACT-1 | 6 | € 100 | € 600 |
| Configure different VLAN for every device | ACT-1 | 2 | € 100 | € 200 |
| Configure NAS on cluster mode | ACT-1 | 4 | € 100 | € 400 |
| Manager and employee training | ACT-2 | 4 | € 100 | € 400 |
| Define recovery procedure | ATC-3 | 4 | € 100 | € 400 |
| Setup Emergency Contact list | ATC-3 | 2 | € 100 | € 200 |
| Configure automatic security updates | ATC-3 | 2 | € 100 | € 200 |
| Implements a Maintenance Program | ATC-3 | 4 | € 100 | € 400 |
| Configure data encryption on each device | ATC-4 | 8 | € 100 | € 800 |
| Implement backup strategies on BYOD | ATC-4 | 4 | € 100 | € 400 |
| Configure 2 factor authentication | ATC-4 | 4 | € 100 | € 800 |
| Configure Role Based Access Control on NAS | ATC-4 | 6 | € 100 | € 600 |
|  |  |  |  |  |
| **TOTAL ACTIVITIES** | | **€ 6.600** | | |

**Start-up material list**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Item** | **ACT-REF** | **Qty** | **Unit Price** | **Price** |
| Sophos XGS Firewall | ACT-1 | 2 | € 300 | € 600 |
| Bitdefender box firewall | ACT-1 | 1 | € 250 | € 250 |
| Sophos RED | ACT-1 | 1 | € 350 | € 350 |
| HPE Aruba 2930F | ACT-1 | 2 | € 2.250 | € 4.500 |
| Servers/Network Secure Cabinet | ACT-1 | 2 | € 200 | € 400 |
| (Sophos) Central Antivirus | ACT-1 | 1 | € 100 | € 100 |
| Synology RS 819 + DISKS | ACT-1 | 2 | € 1.650 | € 3.300 |
|  |  |  |  |  |
| **TOTAL MATERIALS** | | **€ 9.500** | | |

|  |  |
| --- | --- |
| **TOTAL COST** | **€ 16.100** |

## **8.2 Recurring costs**

**Activity Maintenance List**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Action** | **ACT-REF** | **Hours** | **Cost/Hour** | **Price** |
| Configure Firewall Policies | ACT-1 | 1 | € 100 | € 100 |
| Configure Navigation Proxy used by company users | ACT-1 | 1 | € 100 | € 100 |
| Configure the IDS (Intrusion Detection System) | ACT-1 | 1 | € 100 | € 100 |
| Maintenance of the recovery procedure | ATC-3 | 4 | € 100 | € 400 |
| Setup Emergency Contact list | ATC-3 | 1 | € 100 | € 100 |
|  |  |  |  |  |
| **RECURRING ACTIVITIES (YEARLY)** | | **€ 800** | | |

**Recurring Cost (yearly) Material List**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Item** | **ACT-REF** | **Qty** | **Unit Price** | **Price** |
| Sophos FW annual maintenance | ACT-1 | 1 | € 1.000 | € 1.000 |
| Aruba Central (3 years subscription) | ACT-1 | 1 | € 200 | € 200 |
| (Sophos) Central Antivirus | ACT-1 | 1 | € 500 | € 500 |
| Synology Cloud C2 Backup | ACT-1 | 1 | € 99 | € 99 |
| Synology Cloud C2 Storage | ACT-1 | 1 | € 139 | € 139 |
|  |  |  |  |  |
| **RECURRING MATERIALS (YEAR)** | | **€ 1938** | | |

|  |  |
| --- | --- |
| **TOTAL COST** | **€ 2738** |

# **9 Conclusions**

Accountants' offices are locations that contain private information that could harm customers if it becomes public or lost. Changes to the cybersecurity location may allow for greater confidentiality and availability of these critical resources to authorized employees of the accounting firm. In this project, various areas are highlighted where the organization's cybersecurity can be improved. Improving cybersecurity in these areas will reduce the likelihood of the accounting firm experiencing cyberattacks and improve the firm's ability to respond to and recover from an incident. It is estimated that approximately 62 hours of consultancy by a cybersecurity specialist and an initial investment of

€ 16.100 will be required.

# **References**

Barrett, M. P. (2018). *Framework for Improving Critical Infrastructure Cybersecurity* (1.1). NIST Cybersecurity Framework. <https://doi.org/10.6028/NIST.CSWP.04162018>

Fernandez De Arroyabe, I., & Fernandez De Arroyabe, J. C. (2021). *The severity and effects of Cyber-breaches in SMEs: a machine learning approach*. Enterprise Information Systems. 10.1080/17517575.2021.1942997 To link to this article: <https://doi.org/10.1080/17517575.2021>.

*IRS warns about COVID-19 economic impact payment fraud*. (2021, June 4). Internal Revenue Service. Retrieved November 24, 2021, from <https://www.irs.gov/compliance/criminal-investigation/irs-warns-about-covid-19-economic-impact-payment-fraud>

Lallie, H. S., Shepherd, L. A., Nurse, J. R.C., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2021, June). Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *Computers & Security*, *105*(1), 102248. 10.1016/j.cose.2021.102248

Parkin, S., Fielder, A., & Ashby, A. (2016). *Pragmatic Security: Modelling IT Security Management Responsibilities for SME Archetypes*. 10.1145/2995959.2995967