verus

May 8, 2024

Hello Georgia,

Thank you for the opportunity to discuss the Bolinas Community Public Utility District's IT support needs.

Located in San Rafael, we are a comprehensive provider of IT services throughout the San Francisco Bay Area. Since 2001, Verus has provided services that include systems engineering, application integration, and in-house, custom software development. Our primary focus is to provide solutions to technology issues encountered by small to medium sized businesses and to become an integral part of client operations. We strive to collaborate with management, employees, and IT staff to establish and maintain a technology environment that fosters maximum productivity.

Verus offers comprehensive IT support services with a fixed monthly fee service arrangement called TotalCare. TotalCare allows clients the flexibility to focus on other aspects of business while maintaining confidence that all IT requirements are being comprehensively managed. Services that support the daily use of technology include remote monitoring, desktop and server management, equipment procurement, data backup, security management, end user support, and PC upgrades and replacement. TotalCare is priced at $150.00 per user per month. For projects that fall outside the scope of TotalCare, Verus offers an hourly rate.

Hourly IT support is an alternative option to TotalCare. Hourly work is billed at a rate of $200.00.

Bolinas Community Public Utility District **Project Description**	**Estimated Number of Hours**	**TOTAL**
Migration of Active Directory to the Cloud	7	$1,400.00
Migration of QuickBooks and Intedata to a Cloud-hosted environment, Infinitely Virtual	8	$1,600.00
Migration of 500GB flat files to Microsoft SharePoint	8	$1,600.00
TOTAL ESTIMATED HOURS:	**23**	**$4,600.00**

TotalCare:

- ✓ ***All inclusive, fixed-price managed service plan***
- ✓ ***Month- to-month agreements mean more flexibility with no long -term contracts***
- ✓ ***Comprehensive assessment and documentation of network ensures maximum security***
- ✓ ***No initial onboarding fees***
- ✓ ***Onsite support as necessary***

Verus Security Foundation:

As a security first IT provider, we implement a comprehensive suite of security tools and practices to reduce risks. The following security elements are required of all clients:

- ***Remote Management*:** Provides visibility into the configuration of all supported devices.
- ***Endpoint Security*:** SentinelOne identifies threats and removes malware.
- ***Security Awareness Training*:** Ongoing trainings and simulated phishing attacks.
- ***Password Management*:** Identifies weak passwords, credentials on Dark Web, and re-used passwords.
- ***Multi Factor Authentication*:** Protects access when credentials have been compromised.
- ***Firewall:*** All physical locations must have a modern, updated firewall in place.
- ***Cloud Backups*:** Critical data on servers, PCs, and email platforms must be protected.

14 Pillars of Modern Security:

As there are now a myriad of cybersecurity threats that didn't exist until recently, we have identified key tools and best practices to ensure a secure IT infrastructure. Please see the included whitepaper, The 14 Pillars of Modern Security.

Client Satisfaction:

The Verus team strives to consistently exceed client expectations. Across hundreds of client ratings, 99+% are classified as "great". We ask clients for their feedback on every interaction. The rating options are "Bad", "Ok", or "Great". Any interaction that does not receive a "Great" rating receives follow-up. Responsiveness is a top priority that minimizes client downtime while increasing productivity. Quarterly business reviews and client satisfaction meetings ensure the team is consistently communicating and delivering excellent service.

Client Testimonials:

"I have worked with Verus Technology for over three years, and I can honestly say that these are the best technology professionals I have encountered. Not only are they extremely knowledgeable of their field, but they are very professional, friendly and quick to respond when we need help. Their reliability, expertise and perseverance to solve our IT problems makes technology easy to manage for our small company. I highly recommend Verus Technology to anyone looking for a seamless technology solution." ***-Jackie K., Financial Services***

"We have been with Verus for all our IT needs for years and we've been more than happy with their services. They are knowledgeable, reliable and always available. From the smallest troubleshooting issues on a PC, to the purchase of a new server, we are very satisfied with Verus' level of professionalism and end-results." ***-Juliette R., Real Estate Services***

Bolinas Community Public Utility District's Desired Services:

- **Support 7 Employees:** Support and customer service are critical components to providing excellent service. We use a ticketing support system to track and prioritize requests in an orderly fashion and provide clients with a consistent ticketing experience. The systems support team is expected to create documentation for issues that are likely to be repeated, review client event logs, and create tickets for action as necessary.
- **CTO and Strategic IT Consulting:** Our team of engineers will help drive IT strategy and recommend better ways to use technology by providing efficiency and productivity gains. Our IT strategists have 20+

years of business technology experience and offer solutions that assist in the development of a strategic IT plan based on the organization's goals and objectives. The team is available for onsite visits to handle issues that require a physical presence (including issues with specific devices and the Internet and Wi-Fi network).

- **Security:** Cybersecurity threats pose a larger risk to businesses than ever before. A layered approach must be used to reduce the risk of falling victim to a cyberattack. Verus recommends Breach Secure Now Security Awareness and Phishing Training, a platform that helps users become more aware of security threats that arise during normal usage of email and web browsing. It helps lower the chance that a virus or other threat is going to successfully get onto an end user's computer as the user will be more educated about threats and how to avoid them. Email simulations allow us to send fake phishing emails to users at a client, and see who clicks on them, so we can pinpoint specific users that require additional training.

Once you have reviewed this information, the next step would be to schedule a follow up meeting to address any specific questions.

Best regards,

Elizabeth Chekouras

Director of Sales and Marketing

The Pillars of Modern Business IT Security

verus

Verus Technology Solutions
1717 5th Avenue, San Rafael, CA 94901
415-945-7000
www.verustechnology.com

Updated September 28, 2022

Introduction

This whitepaper aims to provide current, relevant background about the IT security threats facing businesses today, and a summary of tools and best practices that can be employed to reduce this risk.

Small and medium-sized businesses are under attack by cyber criminals like never before. It is important to understand that cyber criminals treat the work that they do as their job. While many cyber criminals are based in Eastern European countries, the US now originates 40% of phishing attacks.

Like any other business, cyber criminals look to find the largest opportunities to profit from the work that they do. Increasingly, they target small to medium-sized business, because these companies generally have less money to spend on IT security, and thus are often more vulnerable.

In an examination of thousands of security incidents, Verizon found that almost all malware arrived on computers via email — 94% of cases. In 80% of cases, phishing is the mechanism used to convince users to install malware.

Security tool-provider Kaspersky says that its platform identified mote than 25 million “unique malicious objects" in 2019, and that nearly 20% of all Internet users were the subject of some kind of malware attack. But those attacks weren't necessarily distributed equally, and attackers are showing more savvy and going after potentially richer targets.

The ransomware business model has evolved to become the main way cyber criminals earn money. They are sophisticated enough that many accept credit cards for their fees, just like normal businesses do. Average ransom amounts have skyrocketed to more than $150,000 in 2020.

With all of these threats facing businesses, how do you protect yourself? The short answer is that a multi-faceted, layered approach must be taken to reduce the risk of any particular type of threat. The risk of being attacked by a cyber criminal cannot be eliminated, but it can be significantly reduced by implementing a series of tools and best practices, as outlined in the remainder of this whitepaper.

This whitepaper provides a high-level overview of the steps that should be taken to properly secure your technology infrastructure. Because of the complexity of the tools and techniques involved in providing proper protection from cyber security threats, we strongly recommend working with experienced IT professionals, like a Managed Service Provider (MSP), to protect your technology environment, including the implementation of all of the initiatives outlined here.

The Pillars of Modern Business IT Security

Security Assessment

Endpoint Detection and Response

Backups and Disaster Recovery

Email Security

Secure Remote Access

Password Management

Security Account Review

Cyber Insurance

Firewall

Multi-factor Authentication

Product Updates

Security Awareness Training

Security Operations Center

Encryption

Dark Web Research

Security Assessment

Putting together a comprehensive security plan for a business starts with conducting a thorough assessment of the current IT environment, to identify security measures and platforms already in place. Vulnerabilities in the current environment will be identified, and methods for remediating those liabilities will be offered. If vulnerabilities are found, they should be documented and prioritized in terms of degree of risk.

At the conclusion of a security assessment, the business should have clear documentation on what risks are present, and what steps need to be taken to remediate those risks.

Firewall

A network firewall is a physical device on your office network that controls all data flowing between the devices on the network and the Internet. Firewalls provide three critical functions to protect your network from threats on the Internet.

Because a firewall controls the flow of all information between devices on the internal network and the Internet, it has the ability to inspect this information, and prevent access to websites or other resources that are determined to be potentially harmful. Modern firewalls use "sandbox" technology to assess potential threats in a safe, controlled environment, and only allow delivery of information once the content has been concluded to be safe.

Firewalls also provide secure, encrypted remote access to resources inside the network for specific users, using virtual private network (VPN) technology. With a VPN, users who are remote start a small application on their device, and authenticate using their regular network credentials. Once the user is authenticated, they can then access resources on the internal network, just as if there were in the office. VPN technology is often used to securely provide remote access to key files and applications.

As many business have migrated to utilizing Cloud-based services for key functions like email, file sharing, and application access, the need to share an internal resource to the Internet is not as common as it once was. However, in some environments there is a need to provide access to servers or other resources inside your network to the general Internet. In these cases, the firewall controls what specific server can be accessed, and logs what access has taken place for review if needed.

Endpoint Detection and Response

Endpoint Protection and Response (EDR) is the modern evolution of what many people think of as anti-virus or anti-spyware tools. EDR platforms work by installing a small "agent" piece of software on each computer (PCs and servers) in the business, including devices in home offices or other remote locations. The agent then watches all activity on the computer, and can stop applications and processes that appear to be malicious.

Traditionally, EDR platforms worked by having essentially a large database of known threats, and then comparing all files and applications on each computer against the list of threats. Because threats have gotten more sophisticated and are introduced in very large volumes, a database can no longer be updated fast enough to effectively catch new threats.

Thus, modern EDRs utilize new detection mechanisms, including the use of artificial intelligence (AI), to detect and eliminate threats. The technology has evolved to a level of sophistication that leading vendors now offer a warranty to customers, in the event that a threat gets past their defenses.

Multi-factor Authentication

In the modern IT world with many Cloud-based applications and services, everyone has to use username and password credentials for access. However, there have been many historical security breaches at large companies (see *Dark Web Research* below), which has caused millions of passwords to be exposed to hackers on the Internet. Hackers can also attempt to log into websites using a collection of often-used passwords, in what is known as a "brute force attack".

The most common way to address the inherent insecurity of the username/password system is by enabling multi-factor authentication (MFA). MFA involves using both "something you know" (your username and password), as well as "something you have" (usually your mobile phone). Most modern applications can be configured to force MFA, where a temporary, unique code is sent to the user's mobile device, as an additional form of authentication before allowing application/website access.

In addition to all key applications, MFA should be enabled for logging into individual computers, which can be implemented using 3rd party solutions that integrate with Windows and MacOS. MFA should also be implemented if a VPN is used for remote access to any network resouces.

Some applications perform MFA by sending a code to the user's mobile phone via text message (SMS). If possible, this method should be avoided, because the SMS system is inherently not completely secure — the SIM cards used in mobile phones can be "spoofed", so that a different phone receives the SMS message. An authenticator application like Google Authenticator or Microsoft Authenticator should be used instead, as these applications use a secure Internet connection to receive the unique codes.

Backups and Disaster Recovery

In the event security is compromised, it is critically important that all data on your computer and network be protected with good, validated backups, to ensure that the data can be restored if needed.

The "golden rule" in data backup overall is the 3-2-1 rule. There should be "3" copies of all critical data: one in production, and two backup copies. The "2" backup copies should be on different media, and "1" of the backups should be offsite (in today's world, often this means stored in the Cloud).

When determining what data needs to be protected with backups, it is important to include data that is stored in various Cloud services. The most common of these is email (and related data) stored with a provider like Microsoft 365. This kind of data is also vulnerable to attacks by cyber criminals, and thus must be protected with a data backup strategy like all other business data.

Product Updates

All computers utilize an array of software to perform critical functions. Starting with the operating system, like Microsoft Windows and Apple MacOS, and including common applications like Microsoft Office, Google Chrome, and Adobe Acrobat, these platforms are very large, complex pieces of software.

Because of their inherent complexity, these pieces of software contain security liabilities that are identified by the manufacturer over time. When this happens, the manufacturer will produce an update, sometimes called a "patch", to fix security problems that have been found. Malicious software, including viruses and other forms of malware, will attempt to exploit documented liabilities in unpatched software.

It is thus very important that these software platforms be kept up-to-date with patches, especially for the operating system. IT professionals need to carefully monitor all systems to ensure that updates are being applied consistently, in order to prevent security liabilities from being exploited. Research shows that 60% of security breaches involved vulnerabilities for which a patch was available but not applied.

The same concept applies to important hardware devices on a network, like firewalls. These devices also run software within them, and the providers of this equipment will issue "firmware" or similar updates which should be applied on a consistent basis.

Finally, all major software and hardware manufacturers define an "end-of-life" for their products, after which they no longer provide security updates. For example, Microsoft defined January 14, 2020 as the end-of-life for their popular Windows 7 operating system. In order to not have security liabilities exploited, it is important to identify computers running end-of-life software, and to upgrade that software to a supported version.

Email Security

Because email is used so ubiquitously in business, it is the mechanism most often used by cyber criminals to attempt to deliver malicious material to unsuspecting users. Thus, it is essential to employ an email security platform that protects against these threats.

Email security starts with preventing spam (unwanted email) from being delivered to the user's mailbox. While strictly speaking this is not a security threat, spam can significantly affect an employee's productivity. Modern email security platforms utilize artificial intelligence to identify spam with a high degree of accuracy.

Phishing attacks are used by many cyber criminals, sending emails that look like legitimate messages, but instead have either attachments or links that contain malicious content. These messages can look like they are from common vendors like amazon.com or Wells Fargo, or they can appears to be from people you commonly communicate with—fellow employees or vendors. Email security platforms identify and quarantine phishing emails to prevent these messages from arriving in the user's mailbox.

Finally, often users need to send sensitive information, like passwords or social security numbers, via email as part of their regular job functions. Because email on the Internet is inherently unencrypted, this information can be potentially seen by cyber criminals. Email security tools can offer an easy ability to encrypt this sensitive information, and thus protect it from being accessible to cyber criminals.

Security Awareness Training

The largest security threat to businesses lies in the actions employees take when doing their regular work, including accessing malicious websites, and accessing emails with bad attachments or links. As a result, training users to be more security aware is important to the business's overall security posture.

Security awareness training generally comes with two components. First are a series of modules that can be send to all employees on a consistent basis (often monthly) to teach them key aspects of remaining secure while working online.

Because so many threats come in the form of phishing emails, simulated malicious emails can be sent to all users. The responses to these emails are then tracked, so that users can be identified who selected items in the fake phishing email. These users can then be provided with additional training, so that they better understand what malicious content looks like. Research shows that consistent training, combined with phishing attack simulations, can reduce infections by up to 72%.

Secure Remote Access

Remote access to internal resources from outside the office is often an important part of employee productivity, especially in the age of Covid where many companies have switched to partial, or even entire, remote work environments.

There are different mechanisms that support remote access to internal resources, and it is important to take appropriate security measures for each. If a VPN is in use (see the *Firewall* section above), it should be configured with multi-factor authentication (see *Multi-factor Authentication* above), to prevent unwanted access using stolen credentials.

There are different technologies that allow a user to control their in-office PC from a remote location, including popular services like GotoMyPC and TeamViewer. If these tools are in use, they also should be configured to enforce multi-factor authentication.

Microsoft has a core remote control technology known as Remote Desktop (RDP or RDS for short) that is built into their desktop and server Windows platforms. Because Windows is so commonly used in business, this remote access technology is especially vulnerable to attack by cyber criminals. If this is in use, it should only be allowed while protected by a VPN connection—in other words, it should not be used across an open, unencrypted Internet connection.

Finally, some users work from multiple remote locations, like coffee shops and airports, in addition to their home office. These remote environments have an additional risk that cyber criminals can be in the same environment and can work to steal information, like credentials, as it is being transmitted on the local network, before going to the Internet. As a result, a personal VPN platform should used in these environments, to ensure that all information being sent to and from the computer is encrypted, and thus cannot be accessed by others.

Security Operations Center

In a business network with servers, firewalls, switches, and other equipment, it can be next to impossible to determine if a threat has infiltrated the network and is active. These threats are known as Advanced Persistent Threats (APTs), and as of 2020 statistics shows that over 76% of US-based small-to-medium sized businesses (SMBs) have a APT in their environment.

The solution to this challenge is to utilize a Security Operations Center (SOC). A SOC takes feeds of activity from key devices on a network, and then using a combination of both human and artificial intelligence (AI), identifies potential threats which can then be reviewed by an IT professional. SOC solutions can also monitor critical Cloud services, like Microsoft 365, to determine if those resources are threatened.

Aligned with utilizing a SOC is to run periodic network vulnerability tests. These tests examine all critical elements of a network infrastructure to identify security liabilities that need to be addressed.

Password Management

All users use passwords to access tools they utilize every day - applications, email, network resources, and more. Because of this, many users end up creating a small number of passwords that they re-use across different platforms, to make the process of remembering and entering these credentials easier. Research shows that 59% of all computer users use the same credentials for every website and application they access.

The risk in this practice is that hackers routinely identify and expose extensive lists of credentials from large companies whose security has been compromised (see *Dark Web Research* below). If a user is re-using passwords across different applications, those passwords may already be available to hackers to use.

A password manager allows a user to easily create and maintain a unique, complex password for all applications and sites where a password is required. Instead of the user having to type in their username and password, the password manager application will instead fill in these credentials for the user, after the user has established their identity with a “master password” (or similar authentication mechanism).

Over time, the password manager will store all credentials used by the user. This allows the platform to then identify potential security liabilities: 1) passwords that are re-used across sites; 2) passwords that are not complex, and thus could be guessed by a cyber criminal; and 3) passwords that have been found to be available on the Dark Web. The user can then change the passwords used in these situations, to help ensure that a complex, unique password is being used for all applications and sites.

Finally, password managers work across teams, for situations where common credentials are used by multiple employees to access an application or website. This way, when a shared password needs to be changed, it can be done by any user who has access, and the new password will be available to all related users.

Encryption

Laptop computers are a common target for thieves, and can also be lost during travel or other circumstances. When this happens, even if access to the computer is protected with a password, cyber criminals can attempt to access the data stored on the device by removing its storage device ("hard disk"), and then accessing the storage via another device.

To protect against this potential, the data stored on laptop computers needs to be encrypted. This is done using BitLocker technology on Windows devices, and with FileVault on MacOS devices. Both of these are integrated with the operating system, and simply need to be enabled and configured appropriately.

Security Account Review

All businesses create security accounts in different platforms for their employees. If you use internal network resources, there are likely Windows Active Directory accounts used to control access to files and other resources. Alternatively, there could be accounts inother platforms in use, such as a file sharing mechanism like Dropbox.

In any case, the accounts created in these platforms need to be consistently reviewed, to ensure that only current users have access, and that old users have been removed or disabled. This includes removing what are sometimes called service accounts, which are accounts used by different automated processes and services, rather than a specific user.

Dark Web Research

Hackers target businesses and other organizations to try and steal information. Some of this stolen information is used for other criminal activities, such as identity theft, online banking fraud, and social networking scams.

Often times, stolen information is sold on the Dark Web, a portion of the Internet frequented by cyber criminals. This information is used by other criminals to gain access to accounts or to conduct illegal activities. Dark Web Research involves using tools to scan the Dark Web to see if accounts associated with a business domain have been compromised in an external data breach.

An external data breach is one that has happened outside your company or organization. Some notable breaches include the Linked breach that compromised over 160 million accounts, and the Dropbox breach that compromised almost 70 million. While these data breaches are not the fault of your company or its employees, they could have potentially damaging consequences.

Often, hackers and cyber criminals will use the credentials from one breach, and try them on other websites. If your employees use the same email and password across multiple websites, they could be at risk of compromising their accounts.

The solution to this problem is to create unique, strong passwords for every account (see *Password Management*), and to use MFA (see *Multi-factor Authentication*) whenever possible. Credentials exposed on the Dark Web should be consistently reviewed, as new external breaches happen often.

Cybersecurity Insurance

Cybersecurity insurance, also called cyber liability insurance or cyber insurance, is a contract that an entity can purchase to help reduce the financial risks associated with doing business online. In exchange for a monthly or quarterly fee, the insurance policy transfers some of the risk to the insurer.

The loss, compromise or theft of electronic data can have a significant negative impact on a business, including the loss of customers and revenue. Businesses may be liable for damages stemming from the theft of third-party data. Cyber liability coverage is important to protect businesses against the risk of cyber events, including those associated with terrorism. Cyber-risk coverage can also assist in the timely remediation of cyber attacks and incidents.

Cyber insurance policies help cover the financial losses that result from these cyber events and incidents. In addition, cyber-risk coverage helps with the costs associated with remediation, including payment for the legal assistance, investigators, crisis communicators, and customer credits or refunds.

Conclusion

Information security for small to medium-sized businesses is a complex, multi-faceted challenge. Cyber criminals use increasingly sophisticated techniques to carry out attacks, and businesses must stay continually abreast of current threats in order to reduce the risk that they succumb to an attack. Implementing the 14 recommendations in this whitepaper will significantly reduce the chance that cyber criminals will successfully attack your business.

We hope the content of this whitepaper has been helpful and educational. To learn more about these recommendations, and to discuss your business's approach to IT security, please contact us at:

Verus Technology Solutions
415-945-7000
clientservices@verustechnology.com
https://www.verustechnology.com

verus

Client Name : Bolinas Community Public Utility District

Date: 6/11/2024

Computers: 5 Employees: 7

Number of Servers: 1

Number of Email Accounts: 12

	$/User/ Month	$/Device/ Month	$/Hour	$/Mailbox/ Month	$/Year	$/Month	One Time Fee	Total Number of Users/Devices	Total Cost	
Endpoint Protection										
***SentinelOne* (Required)**		3.75						6	**$22.50**	*Per device
*Device antivirus that offers a ransomware warranty of up to $1,000 per endpoint affected by a breach.										
***ThreatLocker* (Optional)**		8.00						6	**$48.00**	*Per device
* An advanced platform that will not allow any new software to run on a device without review and approval										
Sonicwall Firewall TZ270										
*One time purchase that includes three years of Essental Protection annual support. Each additional year costs $446.25. Two firewalls are necessary (office and water treatment plant).							1,315.00	3	**$3,945.00**	*Monthly and One Time
Backups (Required)										
Veeam Local Backups		15.00						1	**$15.00**	*Per device
Microsoft 365 Backups				2.00				12	**$24.00**	*Per mailbox
PC and Mac Backups		7.00						5	**$35.00**	*Per device
Server Cloud Backups		60.00						1	**$60.00**	*Per device
Security Operations Center										
RocketCyber Security Operations Center		10.00						4	**$40.00**	*Per device
*A security service that monitors key devices for unusual network activity.										
Security Awareness Training (Required)										
Breach Secure Now Security Awareness Training + Phishing Simulation	2.50							7	**$17.50**	*Per user
*A platform that helps users become more aware of security threats that arise during normal usage of email, web browsing. etc. Recommended for all users.										
*10- user minumum										
Email Security (Augmentt Required)										
Mail Protector				1.50				12	**$18.00**	*Per mailbox
*A suite of services that offers overall email security.										
Bracket Option - Email encryption				4.00				2	**$8.00**	*Per mailbox
Augmentt Email MFA and security policy enforcement				1.00				12	**$12.00**	*Per mailbox
*Provides end-user visiblity that audits, detects, and protects against security threats.										
Azure Active Directory P2 license				9.00				1	**$9.00**	*Microsoft 365
*Provides advanced security configuration information for Microsoft 365 enviornments.										
Password Management (Required)										
LastPass Enterprise	6.00							7	**$42.00**	*Per user
*A password manager that stores encrypted passwords online.										
Email Hosting										
Microsoft 365 Exchange Online Plan 1	4.00							5	**$20.00**	*Per user
Microsoft 365 Business Basic	6.00							4	**$24.00**	*Per user
*Provides Desktop, web, and mobile versions of Word, Excel, Powerpoint, and Outlook.										
Microsoft 365 Business Standard	12.50							3	**$37.50**	*Per user
Cloud Application Hosting										
Infinitely Virtual	26.99							2	**$53.98**	*Per device
*QuickBooks Cloud Hosting that allows access from any connected device.										
Internet										
Starlink						140.00	600.00		**$140.00**	*Monthly and One Time
*One time dish purchase is required.										
TOTALCARE AND SUBSCRIPTION MONTHLY FEES TOTAL									**$626.48**	
ONE TIME FEE									**$4,545.00**	

verus

Client Name : Bolinas Community Public Utility District

Date: 6/11/2024
Computers: 5 Employees: 7
Number of Servers: 1
Number of Email Accounts: 12

	$/User/ Month	$/Device/ Month	$/Hour	$/Mailbox/ Month	$/Year	$/Month	One Time Fee	Total Number of Users/Devices	Total Cost	
TotalCare	150.00							7	**$1,050.00**	*Per user
Onsite and Remote Support *Desktop and Server Management* *Remote Monitoring* *Equipment Procurement* *Contracts and Registrations* *Security Account Review and Assessment* *Inventory and Documentation* *Product Updates*										
Endpoint Protection										
***SentinelOne* (Required)**		3.75						6	**$22.50**	*Per device
*Device antivirus that offers a ransomware warranty of up to $1,000 per endpoint affected by a breach.										
***ThreatLocker* (Optional)**		8.00						6	**$48.00**	*Per device
* An advanced platform that will not allow any new software to run on a device without review and approval										
Sonicwall Firewall TZ270										
*One time purchase that includes three years of Essental Protection annual support. Each additional year costs $446.25. Two firewalls are necessary (office and water treatment plant).							1,315.00	3	**$3,945.00**	*Monthly and One Time
Backups (Required)										
Veeam Local Backups		15.00						1	**$15.00**	*Per device
Microsoft 365 Backups				2.00				12	**$24.00**	*Per mailbox
PC and Mac Backups		7.00						5	**$35.00**	*Per device
Server Cloud Backups		60.00						1	**$60.00**	*Per device
Security Operations Center										
RocketCyber Security Operations Center		10.00						4	**$40.00**	*Per device
*A security service that monitors key devices for unusual network activity.										
Security Awareness Training (Required)										
Breach Secure Now Security Awareness Training + Phishing Simulation	2.50							7	**$17.50**	*Per user
*A platform that helps users become more aware of security threats that arise during normal usage of email, web browsing. etc. Recommended for all users. *10- user minumum										
Email Security (Augmentt Required)										
Mail Protector				1.50				12	**$18.00**	*Per mailbox
*A suite of services that offers overall email security.										
Bracket Option - Email encryption				4.00				2	**$8.00**	*Per mailbox
Augmentt Email MFA and security policy enforcement				1.00				12	**$12.00**	*Per mailbox
*Provides end-user visiblity that audits, detects, and protects against security threats.										
Azure Active Directory P2 license				9.00				1	**$9.00**	*Microsoft 365
*Provides advanced security configuration information for Microsoft 365 enviornments.										
Password Management (Required)										
LastPass Enterprise	6.00							7	**$42.00**	*Per user
*A password manager that stores encrypted passwords online.										
Email Hosting										
Microsoft 365 Exchange Online Plan 1	4.00							5	**$20.00**	*Per user
Microsoft 365 Business Basic	6.00							4	**$24.00**	*Per user
*Provides Desktop, web, and mobile versions of Word, Excel, Powerpoint, and Outlook.										
Microsoft 365 Business Standard	12.50							3	**$37.50**	*Per user
Cloud Application Hosting										
Infinitely Virtual	26.99							2	**$53.98**	*Per device
*QuickBooks Cloud Hosting that allows access from any connected device.										
Internet										
Starlink						140.00	600.00		**$140.00**	*Monthly and One Time
*One time dish purchase is required.										
TOTALCARE AND SUBSCRIPTION MONTHLY FEES TOTAL									**$1,676.48**	
ONE TIME FEE									**$4,545.00**	