A Year in Review

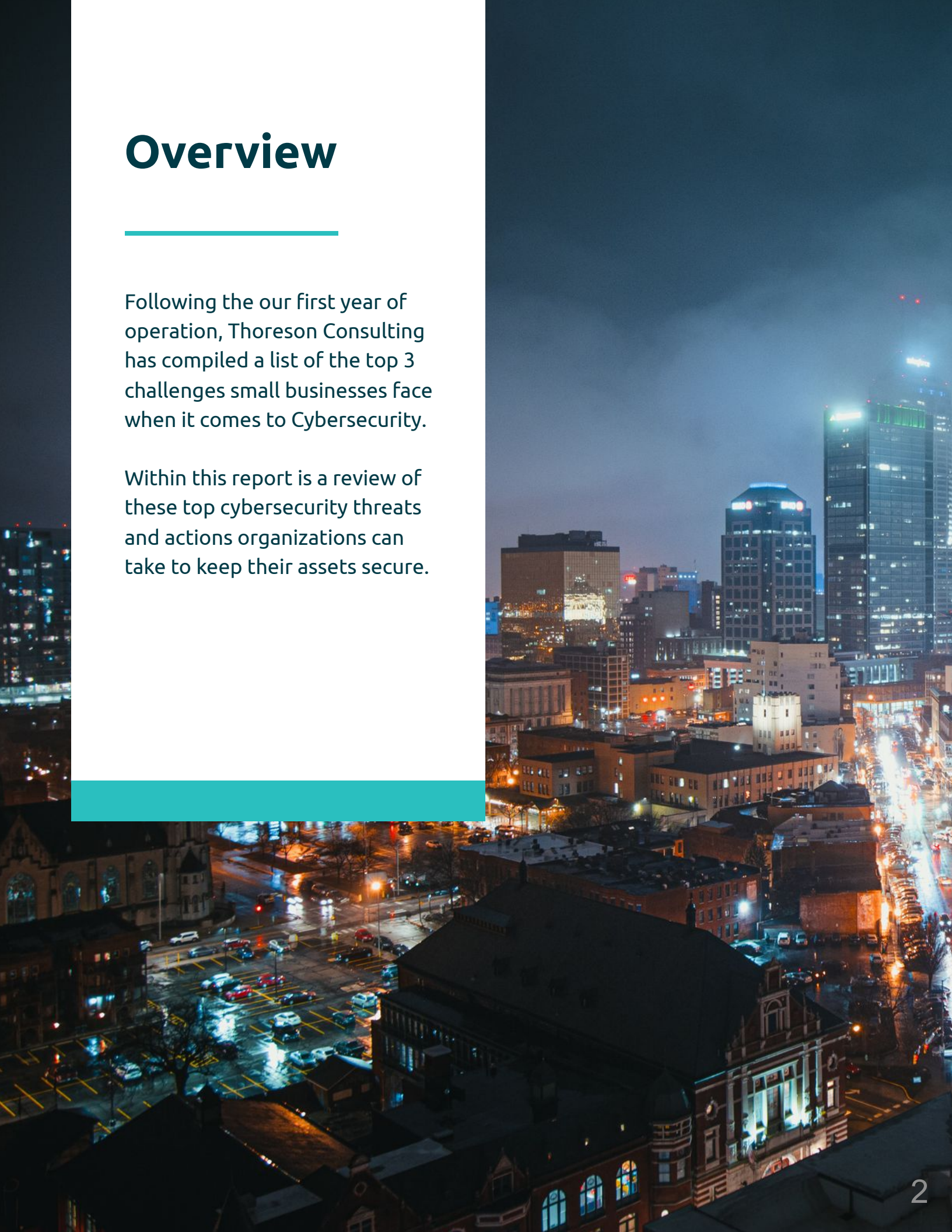
2022

Thoreson Consulting
Small Business Security Report

Overview

Following the our first year of operation, Thoreson Consulting has compiled a list of the top 3 challenges small businesses face when it comes to Cybersecurity.

Within this report is a review of these top cybersecurity threats and actions organizations can take to keep their assets secure.



Top Security Threats 2022

Throughout 2022 organizations of all sizes continued to face cybersecurity challenges. Small businesses often have an additional layer complexity when it comes to the allocation of limited time, money, and resources to security best practices.

Threat actors are becoming more efficient in their operations resulting in quicker and more complex attacks against organizations.

Here were the top three threats observed by Thoreson Consulting throughout 2022:

Rank 1

Business Email Compromise

Compromised accounts are leveraged to intercept funds

Rank 2

Ransomware

Attackers encrypt corporate files and demand payment for their return

Rank 3

Security Misconfigurations

Failure to deploy digital assets correctly may result in excessive permissions or unauthorized access

1 Business Email Compromise

Threat Profile:

Business Email Compromise (BEC) occurs when compromised email accounts are used to engage in fraudulent business transactions.

Often times businesses are engaged by a legitimate but compromised third party account where the attacker attempts to redirect payments or gain insider knowledge about the organization.

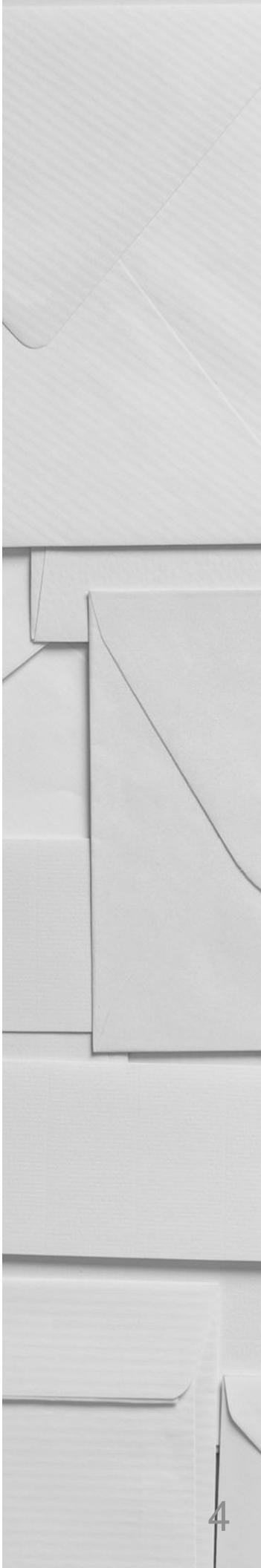
A Growing Concern:

- According to the FBI, BEC has resulted in losses of over $2.4 billion dollars throughout 2021 - up from $360 million in 2016.
- The FBI expects losses to increase as BEC attacks develop in efficiency.
- BEC is becoming extremely common, especially in small to medium size businesses where security controls may not be as developed.

Methodology

Thoreson Consulting observed instances where client organizations had trusted third parties compromised leading to potential BEC incidents:

1. Attacker compromises an e-mail account
2. Attacker monitors the account for sales and transactions between clients & third-parties
3. When services are rendered, the attacker messages the clients requesting that the ACH information is updated to their information in an effort to steal the funds.



Preventing Business Email Compromise

Preventing BEC requires both strong **technical** and **procedural** controls. Technical controls should aim to assist the policies and procedures in place at the organization.

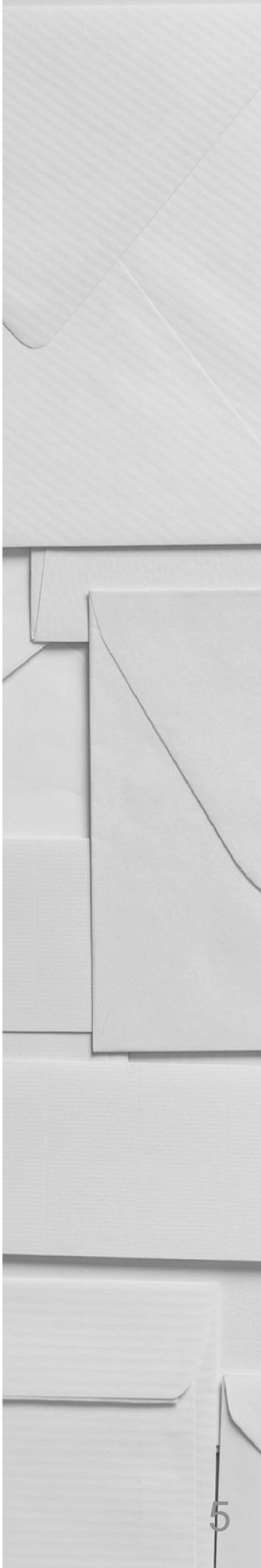
Often times the accounts and email addresses used in BEC attacks are real and are more difficult to identify than typical phishing emails.

Establish Secure Processes

- When handling sensitive information, require use of additional communication channels (i.e. phone, secure file sharing)
- Establish parties authorized to make adjustments to financial processes
- Changing of ACH information should NEVER be done entirely through e-mail or by one person

Support Process with Technology

- Data Loss Prevention (DLP) tools can be used to detect sensitive information in email
- Deploy multi-factor authentication on e-mail to prevent unauthorized access to mailboxes



2 Ransomware

Threat Profile:

Criminal groups leverage malware that spreads throughout the victim organization encrypting all computer files. In order to decrypt the files, ransomware groups demand payment.

In recent times, ransomware groups will employ a 'double extortion' method in which data is exfiltrated and threatened to be leaked publicly should the victim organization not pay or seek external assistance.

Quick Deployment

- As ransomware evolves, the duration from an attacker's initial access to a victim network to the deployment of ransomware has drastically been reduced.
- Ransomware groups that target small businesses often leverage automated scripts to quickly take over a network and deploy ransomware within hours of the initial breach.

Tailored Ransoms

- It is becoming more common for ransomware groups to research their victims before determining a ransom amount.
- Ransom amount increases depending on company size, profits, criticality.
- Ransomware groups favor organizations with cyber insurance due to the potential for a quick turn around in payment.

Preventing Ransomware

Becoming resilient to ransomware is becoming more imperative as ransomware continues to increase in prevalence and efficiency. Security Awareness Training, Threat Management, and Business Continuity planning are critical in mitigating ransomware risk.

Security Awareness Training

- Ransomware attacks often begin with phishing campaigns seeking to steal credentials or distribute malware
- Teaching employees how to recognize suspicious activity can prevent unauthorized access to company assets

Threat Management

- Ensure digital company assets are patched and up to date with latest software releases
- Deploy endpoint protections and follow network best practices such as antivirus and segmentation

Business Continuity Planning

- Develop a strategy to perform backups and restorations of critical company data and applications
- Ensure documentation is in place to identify critical assets with steps to restore to production following an outage or disruption

3 Security Misconfigurations

Threat Profile

Small businesses often have limited resources when it comes to the deployment of security controls. As the company grows, quick and easy solutions to VPNs, File Sharing, and Identity Management often overlook security.

These holes often leave an opportunity for an attacker to gain access to company assets. Below are the top security configuration challenges small businesses face:

Lack of Multi-Factor Authentication (MFA)

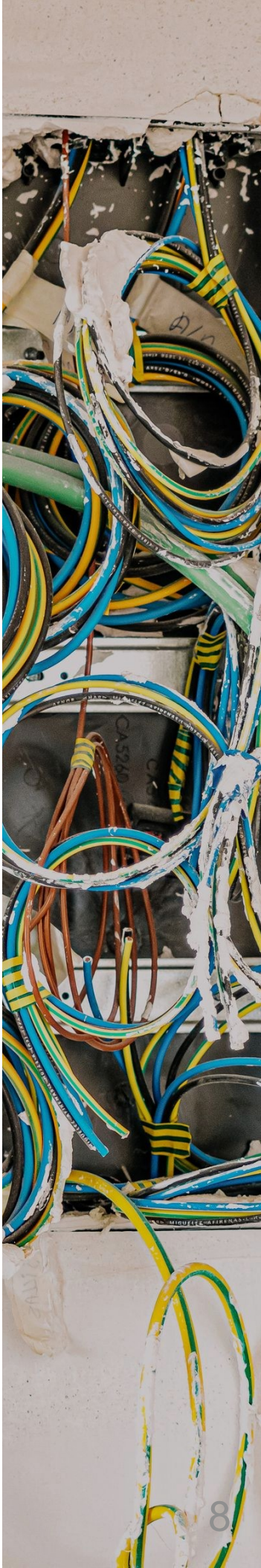
MFA is often overlooked as businesses grow and begin to set up their digital ecosystem. This can lead to severe consequences should an account password become compromised.

Out of Date Virtual Private Networks (VPN)

Remote access to an office or server is common. However, VPNs often are deployed incorrectly, are out of date on security updates, or lack MFA (see above) putting the organization at risk.

Lack of Data Security

As small businesses grow, they often outpace a plan to keep data secure, available, and backed up. Without data backups, security incidents or outages become much more severe.



Preventing Security Misconfigurations

Keep in mind that it is far easier to implement security best practices as a company is growing rather than after the fact. When growing a business, factor in the additional security needs increased personnel, applications, and product offerings might include.

Follow Frameworks & Baselines

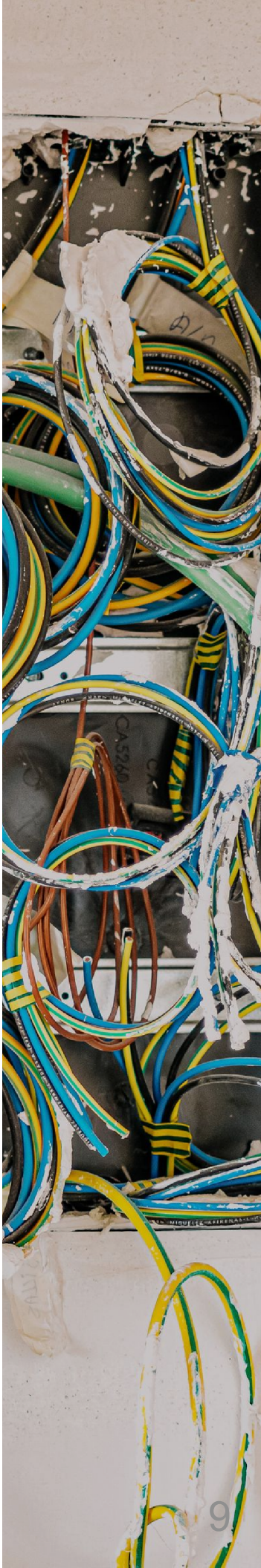
- Depending on the organization, there are a number of cybersecurity frameworks that exist as security checklists.
- Leverage industry approved baselines for the deployment of systems to ensure security is standardized across the organization.

Monitor Vendor Updates & End of Life

- Security is constantly evolving. Vendors may release updates or new software versions as systems go out of date over time.
- As systems reach their End-of-Life (EoL), they are no longer supported with security updates. Ensure EoL systems are secured and migrated to supported versions ASAP.

Perform Routine Audits

- As organizations grow, the addition of people and assets can lead to excessive permissions or residual access.
- Validate all assets have security solutions such as antivirus, encryption, and baseline configurations met.



How Small Businesses Combat Cybersecurity Risk

As small businesses continue to grow, security best practices should be baked into the company strategy. It is important to understand cybersecurity is never a one and done exercise, but an ongoing effort from executive leadership down to the employee.

Risk Assessments

Performing a cybersecurity risk assessment allows the organization to identify gaps in security controls and business processes.

Employee Training

Security Awareness training allows employees to become more familiar with social engineering tactics used by cyber criminals.

Security Culture

It is imperative that security starts with executive leadership to establish a culture of security at the organization. Cybersecurity should scale as the business scales, never taking a back seat.

MFA

The implementation of Multi-Factor Authentication considerably improves an organization's security posture and reduces the impact of a compromised user account password.

Thoreson Consulting Solutions Portfolio

Cybersecurity + Small Businesses

Thoreson Consulting aims to bring affordable and effective cybersecurity to businesses of all sizes. Through our solutions, small businesses can find value and improvements to their security posture.

Risk Assessments

Identify and prioritize the gaps in security that exist within your organization. Our risk assessments are designed to provide answers on where to start when seeking to secure your business.

Security Deployments & Configurations

Allow Thoreson Consulting to assist in the deployment of security solutions and validation of proper configurations. Whether cloud or on premises, we can assist in the security validation of your digital ecosystem.

Policy & Proceedure Development

Technical controls are only half of the equation. Thoreson Consulting can assist with the development of business policies and procedures to reduce human error and eliminate security risks.

Contact Thoreson Consulting

Free Consultation & Resources

- Visit ThoresonConsulting.com to connect for a free consultation session.
- Read the mini-series blog 'Building a Cybersecurity Strategy' for insights on how to improve the security practices at your organization.