THRIVEON
INFORMATION & TECHNOLOGY

Cybersecurity Essentials for Sustainable Success

For SMB Executive Leaders

About Thriveon

Sam Bloedow

CEO, Thriveon

@sambloedow

When founder and CEO Sam Bloedow started Thriveon in 2002, it was born from a love of technology and the needs of small-to-midsize businesses (SMBs) that weren't being met by their current IT service. Fascinated by how companies could leverage technology to enable growth, Sam founded Thriveon on the philosophy of helping other businesses find success the same way.

As technology continues to evolve, so does the need for strategic guidance. That's why, for the last 20+ years, Thriveon has deployed an approach that proactively eliminates IT risk and supports business growth.

Connect with us

info@thriveon.net
855-767-2571

Contents

1 Introduction

2 The Need for Cybersecurity

3 Understanding Cyber Threats

4 Navigating the Web Safely

5 Securing a Safe Workplace

6 Incident Response Planning

7 Securing Mobile Devices

8 Compliance and Regulations

9 Keys to Sustained Cybersecurity

10 Let's Get Started

CHAPTER 1

Introduction

The Importance of Cybersecurity Awareness in Business

Introduction

In an age where technology intertwines with every aspect of our lives, cybersecurity has become a paramount concern for businesses of all shapes and sizes.

Whether you're browsing the internet, sending emails or managing sensitive data in the office, the threat of cyber attacks looms large; no individual or organization is immune to cyber threats.

Cybersecurity isn't only about protecting data; it's about safeguarding privacy, maintaining trust and preserving the integrity of systems. A single breach can have far-reaching consequences, leading to downtime, financial losses, reputational damage and legal repercussions.

- ✓ **Get help navigating** the complex landscape of cybersecurity
- ✓ Obtain practical guidelines and **tools to mitigate risks** and safeguard your company
- ✓ Implement **best practices for secure behavior for you and your employees** both in the office and online

Whether you're a tech-savvy individual, an SMB owner or an IT professional, this eBook caters to all levels of expertise, and we hope you find it useful.

CHAPTER 2

The Need for Cybersecurity

Why do Cybersecurity programs matter?

Why Do Cybersecurity Programs Matter?

When developing cybersecurity programs, many businesses focus on protecting their infrastructure perimeter and device endpoints. That's where cybercriminals usually first gain access and wreak havoc on a company's digital environment.

However, it's also important to consider what happens when a threat bypasses perimeter defenses and targets an employee, whether in the form of a malicious email, text or voicemail that prompts the employee to respond with confidential company information.

There's also the possibility of an offline attack from inside the office. Stronger cybersecurity has become a global priority as hackers penetrate IT infrastructures with increasing frequency and sophistication. Coupled with the growth of the Internet of Things (IoT), mobile devices and Bring Your Own Devices (BYOD), the threat landscape and potential for data leaks has significantly increased, too.

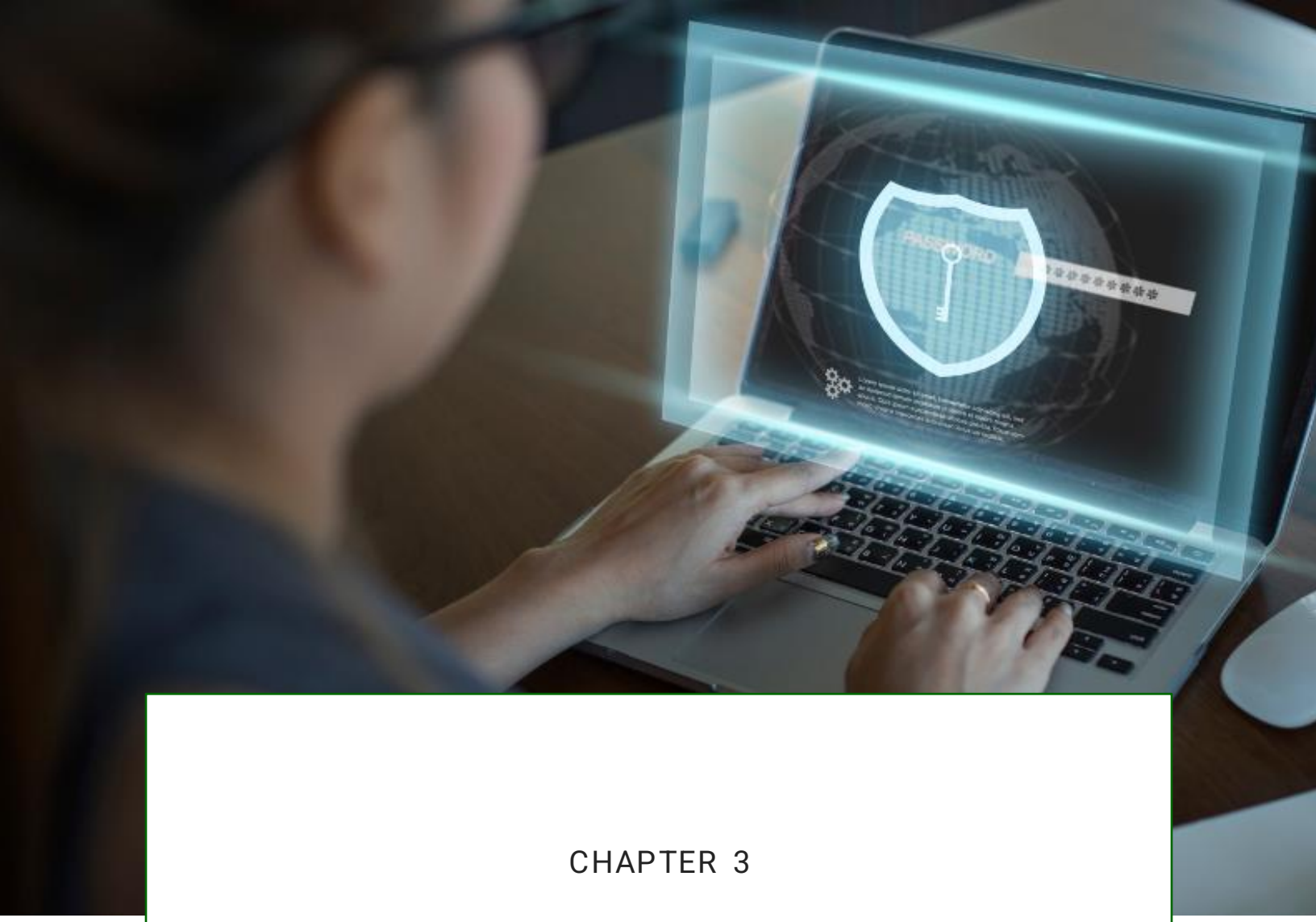
The Need to Educate Employees on Cybersecurity

The need for employees to practice strict and secure cybersecurity habits is not only to thwart digital attacks but also to prevent someone from walking by their desk, whether in the office or at home, and picking up something that contains sensitive information.

We can't stress enough the importance of security awareness training for employees. Educating them on what it takes to protect data is critical. Any leaks, intentional or unintentional, could hurt the business. Leaks can also hurt employees if their personal information is exposed.

60% of data breaches are caused by insider threats.

Plus, customers and business partners could be at risk, compromising the company's reputation for not properly protecting confidential information. It only takes one incident to completely destroy any goodwill you established and build with your customers and vendors.



CHAPTER 3

Understanding Cyber Threats

Types of Cyber Attacks and their Impact

Understanding Cyber Threats

Overview of Cyber Threats

The digital landscape is rife with a multitude of cyber threats, ranging from malicious software to sophisticated social engineering tactics. Understanding these threats is the first step toward building a robust defense strategy. Adopting a proactive approach and adhering to best practices can fortify your defenses and safeguard your company from the ever-evolving threat landscape.

Types of Cyber Attacks

1. Malware: Short for "malicious software," malware encompasses a wide range of harmful programs designed to infiltrate and damage systems. From viruses and worms to Trojans and spyware, malware poses a significant threat to businesses worldwide.

2. Ransomware: Ransomware is the most popular type of malware that encrypts files or locks users out of their systems, demanding a ransom payment (often bitcoin) in exchange for decryption keys or restored access.

3. Social engineering: Social engineering attacks exploit human psychology rather than technical vulnerabilities, relying on deception and manipulation to trick users into divulging confidential information and performing unauthorized actions.

4. Phishing: Phishing attacks are a common social engineering tactic that involves using fraudulent emails, text messages, social media or websites to trick users into revealing sensitive information like login credentials, financial details or personal data.

5. Insider threats: Insider threats involve malicious or negligent actions by individuals within an organization, including employees, contractors, partners and more. Whether intentional or accidental, insider threats pose significant risks to security.

Types of Cyber Attacks and their Impact

Understanding Cyber Threats

Impact of Cyber Attacks

The repercussions of a cyber attack can be far-reaching, affecting individuals, businesses and society as a whole. The consequences of a successful cyber attack can be devastating, from financial losses and reputational damage to legal liabilities and regulatory fines. Moreover, the erosion of trust and confidence in digital systems can have long-term implications for innovation, commerce and global security.

To assess your risk for a cyber crime, consider the information your business uses and stores. Then, consider the damage that would result if you were the victim of a cyber attack. Take a look at these stats:

- Cyber attacks occur every 39 seconds (source)
- 43% of cyber attacks are on SMBs (source)
- But only 14% of SMBs are prepared to defend themselves (source)
- 60% of SMBs go out of business within six months of a cyber attack (source)

CHAPTER 4

Navigating the Web Safely

Guide to Secure Online Habits

Guide to Secure Online Habits

Navigating the Web Safely

Practicing secure online behavior is paramount. Whether you're browsing the web, accessing online accounts or communicating with others, adopting best practices for cybersecurity can help protect your personal information and safeguard against potential threats.

Create Strong Passwords

Passwords serve as the first line of defense against unauthorized access to your online accounts. However, not all passwords are created equal. To enhance security, follow these guidelines when creating and managing passwords:

- **Complexity:** Use a combination of lowercase and uppercase letters, numbers and special characters to create strong, unique passwords that are difficult to guess.
- **Length:** Aim for passwords that are at least 19 characters long to increase complexity and resilience against password-cracking techniques.
- **Avoid common phrases:** Avoid using easily guessable phrases, like "password123." You should also avoid personal information like your birthday, pet's name or nickname.
- **Never reuse:** Use different passwords for each online account to prevent a single breach from compromising multiple accounts. You should also change passwords at least annually.
- **Password manager:** Consider using a password manager tool to securely store and manage your passwords, reducing the risk of password reuse and simplifying the login process across your devices and platforms.

Recognize Phishing Attempts

Phishing attacks remain one of the most prevalent and effective tactics cyber criminals use to steal sensitive information.

To avoid falling victim to phishing scams, keep the following in mind:

- **Verify the sender:** Always verify the sender's email address and domain before responding to unsolicited emails, clicking on links or downloading attachments. Look for misspellings or inconsistencies that may indicate a fraudulent message.
- **Check the URL:** Hover your mouse over email hyperlinks to preview the destination URL before clicking. Beware of shortened URLs or deceptive links that redirect to malicious websites. Only visit reputable websites with the secure https:// protocol.
- **Exercise caution:** Exercise caution when asked to provide sensitive information or perform urgent actions, such as verifying account credentials or transferring funds, especially if the request seems suspicious or uncalled for.

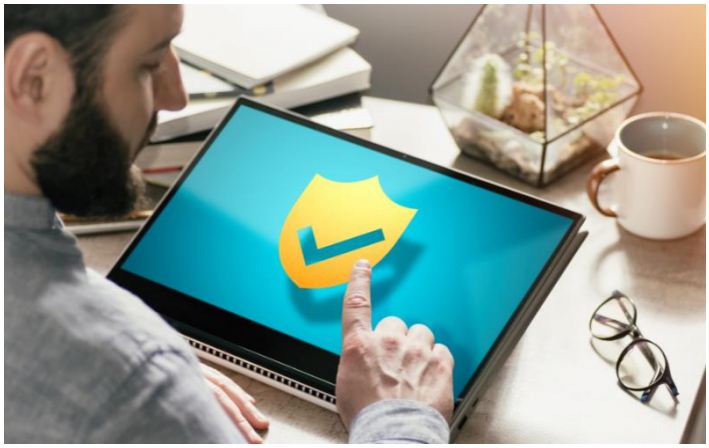
Keep your data safe! Never click, forward, or otherwise interact with a suspicious email.

Navigating the Web Safely

Use Public Wi-Fi Safely

Public Wi-Fi, while convenient, poses inherent security risks due to its open and unsecured nature. To mitigate these risks when using public Wi-Fi, consider the following precautions:

- **Use secure connections:** Whenever possible, use a virtual private network (VPN) to encrypt your internet traffic and protect your data from eavesdropping or interception.
- **Disable auto-connect:** Disable automatic connection to Wi-Fi networks on your device to prevent inadvertent exposure to untrusted networks.
- **Avoid sensitive activities:** Refrain from conducting sensitive activities, such as online banking or accessing confidential accounts, while connected to public Wi-Fi networks.
- **Enable firewall:** Enable the firewall on your device to monitor and filter incoming and outgoing network traffic, adding an extra layer of defense against unauthorized access.



Make Regular Updates

Regular updates are essential for maintaining a secure digital environment. Updates often include critical security patches that protect against cyber threats by addressing known vulnerabilities. Updates should be for software, operating systems and applications, including antimalware and antivirus.

If you don't think you'll remember to manually update, enable automatic updates to ensure timely installation; delaying updates increases the window of opportunity for attackers to compromise systems.

Implement Two-Factor Authentication

Two-factor authentication (2FA) is a way to confirm a user's identity before logging them into their account.

With two-factor authentication in place, it helps prevent hackers from gaining access, even if they do have the password.

CHAPTER 5

Securing a Safe Workplace

Guide to Secure Office Habits

Guide to Secure Office Habits

Securing a Safe Workplace

As the backbone of modern business operations, offices are prime targets for cyber attacks. From sensitive client information to proprietary data, organizations must prioritize cybersecurity and implement secure office behaviors to safeguard their assets and maintain trust with stakeholders.

In-Person Desk Precautions

If your employees work in person, start their secure behavior with a clean, clear desk area. Cluttered desk areas can leave USB devices, smartphones and other devices vulnerable to theft. Lock up and secure devices and documents with sensitive information.

Employees should never leave notes or post-it notes with login credentials and other sensitive information written on them. If an employee needs to get rid of something that contains sensitive information, they should use a shredder to ensure it's properly destroyed.

Secure Network Practices

Firewalls: Install and configure firewalls to monitor incoming and outgoing network traffic, filtering out potentially harmful connections and blocking unauthorized access to your network.

Secure Wi-Fi network: Use strong encryption protocols to secure your office Wi-Fi network and prevent unauthorized users from intercepting or accessing your sensitive data.

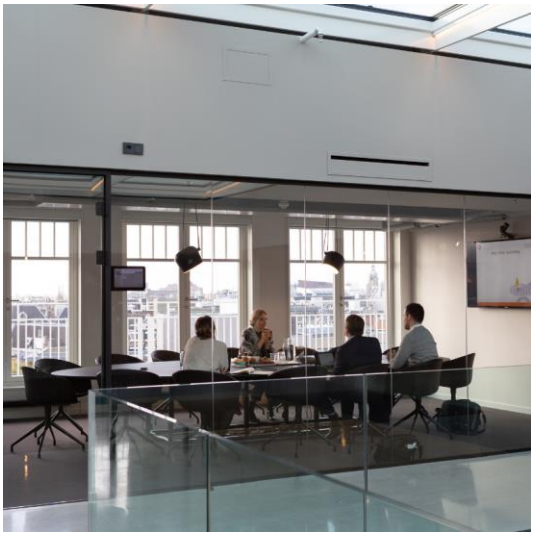
Network segmentation: Implement network segmentation to divide your office network into separate subnetworks, restricting access to sensitive information and minimizing the impact of security breaches.

Regular audits and updates: Conduct regular audits of your network infrastructure to identify vulnerabilities and ensure that software and firmware are updated with the latest security patches and updates.

Data Protection Measures

Utilize the following to safeguard company data:

- **Encryption:** Encrypt sensitive data both in transit and at rest using robust encryption algorithms to prevent unauthorized access or interception by malicious actors.
- **Data backups:** Implement regular data backup procedures to create copies of critical information and ensure rapid recovery in the event of data loss or security breach.
- **Access controls:** Enforce strict access controls and least privilege principles to limit employee access to confidential data based on their job roles and responsibilities, reducing the risk of insider threats and unauthorized disclosure.
- **Data display:** Establish protocols for securely disposing of outdated sensitive data, including physical destruction of storage media and secure wiping of digital files to prevent data leakage or unauthorized retrieval.



Securing a Safe Workplace

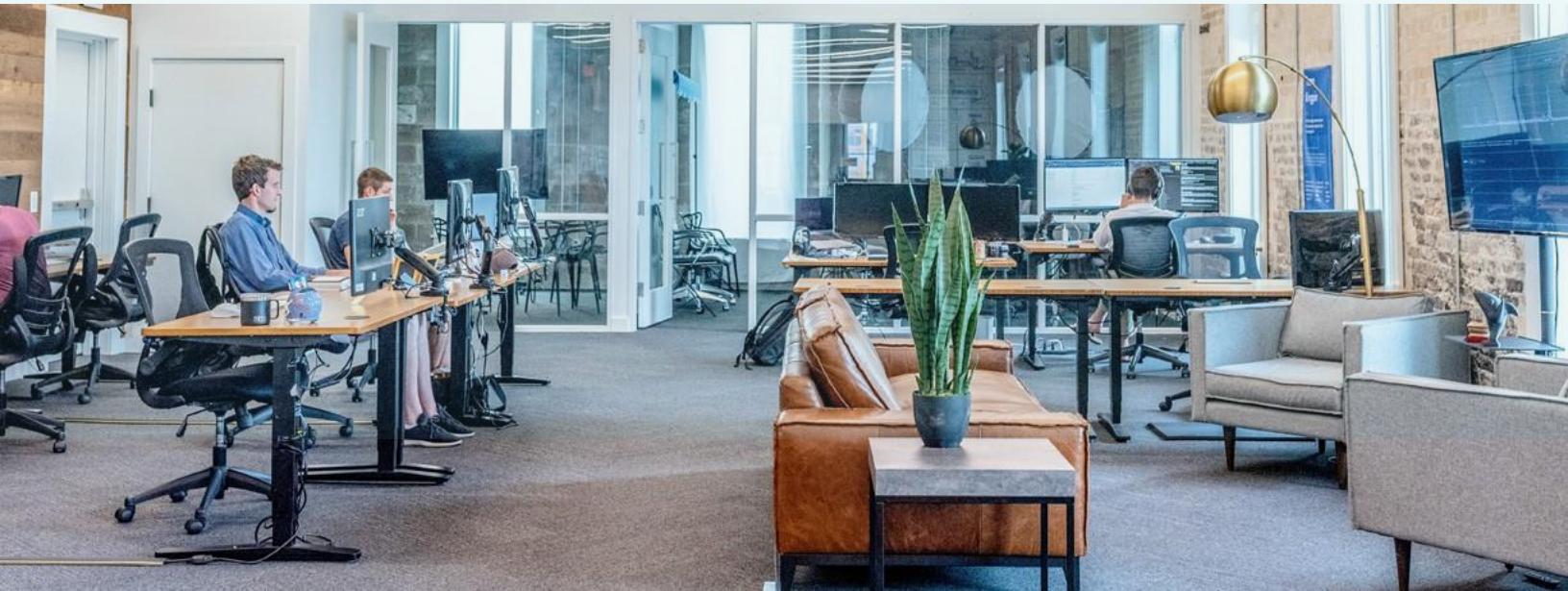
Employee Training and Awareness

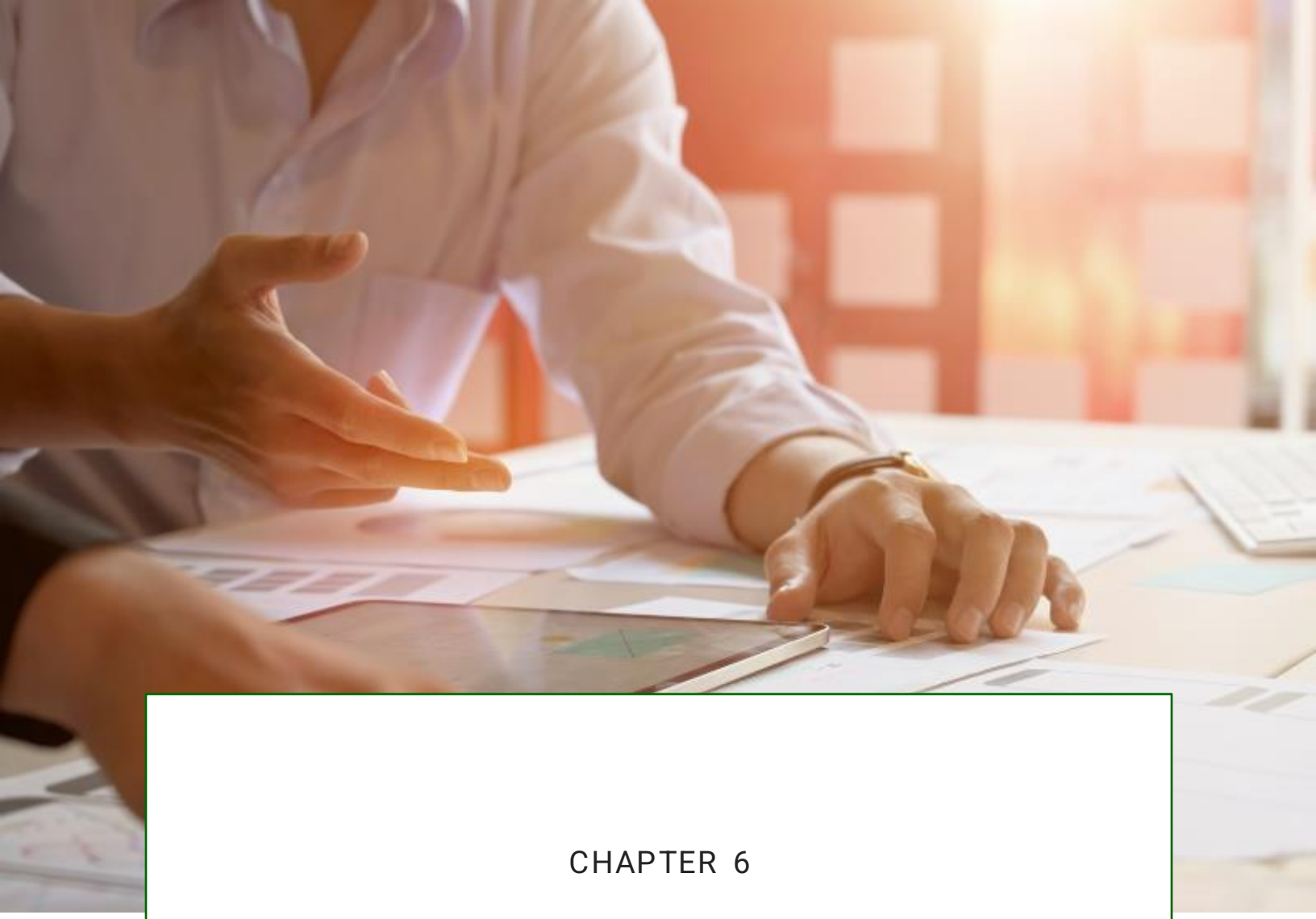
Employees are often the weakest link in the cybersecurity claim, inadvertently exposing organizations to cyber threats through human error or negligence. Invest in employee training and awareness programs to cultivate a culture of cybersecurity awareness and implement secure behaviors within the office.

1. **Cybersecurity training programs**: Provide comprehensive training on cybersecurity best practices, covering topics such as phishing awareness, password hygiene and incident response procedures to empower employees with the knowledge and skills to identify and mitigate potential threats.

2. **Regular awareness campaigns:** Conduct regular awareness campaigns, workshops and simulated phishing exercises to reinforce cybersecurity principles and educate employees about emerging threats and attack vectors. Ensuring employees recognize and avoid cyber attacks is as important as having solid security measures.

3. **Reporting procedures:** Establish clear reporting procedures for employees to report suspicious activities, security incidents or potential vulnerabilities. This fosters a collaborative approach to cybersecurity and enables swift response and remediation.





CHAPTER 6

Incident Response Planning

What To Do When a Cyber Attack Strikes

When a Cyber Attack Strikes

Incident Response Planning

Despite best efforts to prevent cyber attacks, no company is immune to security incidents, and the vast majority of damage done during cyber attacks is due to the company's inability to respond because they don't have an incident response plan.

In the event of a breach or cybersecurity incident, having a well-defined incident response plan is essential for minimizing damage, restoring operations and mitigating the impact on business continuity, which is known as cyber resilience. It identifies the appropriate actions that should be taken when an incident occurs, and it can also instill confidence in your clients that you can protect their data.

An effective incident response plan is more than a document – it's a living, breathing process that requires regular review, refinement and rehearsal to ensure readiness and resilience in the face of evolving cyber threats. Here's how you can prepare an effective incident response plan:

Assess the Risks
Risks may include:

- Strategic: the failure to implement business decisions that align with the company's strategic goals
- Reputational: negative public opinion
- Operation: loss resulting from failed internal processes, people and systems
- Transactional: problems with service or product delivery
- Compliance: violations of laws, rules and regulations

Ask yourself:

1. **What data does your company use (intellectual data, operational data, client data)?**
2. **Who can access it?**
3. **What vulnerabilities does your company have?**
4. **What can you do to limit these vulnerabilities?**
5. **What risks does your company face? (unauthorized use, data leakage, unintentional exposure, data loss, service or productivity disruption)**
6. **What would the impact be if your company was threatened or lost the data?**

Establish Incident Response Teams

1. **Designate roles and responsibilities:** Identify key stakeholders and assign roles and responsibilities within the incident response team, including incident coordinators, technical experts, communication liaisons, legal counsel and executive leadership.
2. **Cross-functional collaboration:** foster collaboration between IT, security, legal, human resources and other relevant departments to ensure a coordinated response to security incidents, with clear lines of communication and escalation procedures.
3. **Training and drills:** Provide specialized training and conduct regular exercises and simulated incident response drills to familiarize team members with their roles and responsibilities to validate the effectiveness of the incident response plan.

When a Cyber Attack Strikes

Incident Response Planning

Create Response Plans for Different Scenarios

By proactively planning and preparing for security incidents, companies can minimize the impact of cyber attacks, mitigate financial losses and maintain trust and confidence with stakeholders.

1.Incident identification and assessment: Develop procedures for detecting and assessing security incidents, including incident triage, classification and initial containment to prevent further damage or unauthorized access to systems and data.

2.Evidence preservation: Define protocols for preserving digital evidence and maintaining chain of custody to support forensic analysis, legal proceedings and regulatory compliance requirements while minimizing disruption to ongoing operations.

3.Containment and mitigation: Implement strategies for containing and mitigating the impact of security incidents, such as isolating affected systems, disabling compromised accounts and deploying patches or security updates to remediate vulnerabilities.

4.Communication and notification: Establish communication protocols for notifying internal stakeholders, executive leadership, employees, customers, partners, regulators and law enforcement agencies about security incidents, including regular status updates and transparent disclosure of relevant information.

5.Recovery and restoration: Develop recovery plans and procedures for restoring affected systems, applications and data to operational status, including data recovery from backups, rebuilding infrastructure and implementing additional security controls to prevent future incidents. Monitor the system to ensure another incident doesn't occur.

6.Post-incident analysis: Conduct post-incident analysis and debriefings to identify root causes, lessons learned and areas for improvement with a focus on continuous process refinement and enhancing incident response capabilities for future incidents. Also use this information to train future incident response team members.

CHAPTER 7

Securing Mobile Devices

Ensuring Cybersecurity On the Go

Ensuring Cybersecurity On the Go

Securing Mobile Devices

In an increasingly mobile-centric world, smartphones, tablets and other mobile devices have become indispensable tools for work, communication and productivity. Mobile security has also increasingly become a concern as more companies adopt BYOD environments, allowing end users to connect to corporate networks through their own devices.

However, their portability and ubiquity also present security challenges, making them attractive targets for cyber criminals. With personal devices accessing corporate networks, businesses must protect endpoint devices that are not under their control, opening the company up to greater risk. Trying to gain control over personal devices also presents the challenge of ensuring the organization doesn't infringe on personal apps and information employees store on their devices.

To safeguard sensitive data and protect against mobile threats, follow these best practices and secure your mobile devices against mobile threats:

Mobile Security Best Practices

Device locking and biometric authentication: Enable device locking mechanisms, such as PIN codes, passwords or biometric authentication to prevent unauthorized access to your mobile device and sensitive information.

Remote locate tools: If your device becomes lost or stolen, software solutions can help find it through GPS and geofencing capabilities.

App permissions and updates: Regularly review and manage app permissions to limit access to sensitive data and functionality only to trusted applications. Keep your mobile operating system and apps updated with the latest security patches and updates to address known vulnerabilities and minimize the risk of exploitation.

App source verification: Download apps only from official app stores, such as the Apple App Store or Google Play Store, to minimize the risk of downloading malicious or counterfeit apps that may compromise your device's security or privacy.

Mobile Device Management (MDM)

Deploy mobile device management (MDM) solutions to centrally manage and secure company-owned mobile devices, enforce security policies and remotely monitor and control device usage to prevent unauthorized access or data leakage. MDM can also isolate personal apps from corporate ones so that personal information remains private, and when an employee leaves the company, only the corporate apps and data are deleted while the personal apps and data are left intact.

Configure remote wipe capabilities to remotely erase data from lost, misplaced or stolen devices to prevent unauthorized access to sensitive information. Additionally, enable device encryption to protect data stored on the device from unauthorized access, even if the device falls into the wrong hands.

CHAPTER 8

Compliance and Regulations

Understanding and Adhering to Cybersecurity Laws

Understanding and Adhering to Cybersecurity Laws

Compliance and Regulations

In today's regulatory landscape, compliance with data protection and cybersecurity regulations is not only a legal obligation but a critical component of maintaining trust and credibility with customers, partners and regulators. By prioritizing compliance with data protection and cybersecurity regulations, companies can mitigate legal and regulatory risks, protect sensitive data and foster stakeholder trust and confidence.

Failure to comply with applicable laws and regulations can result in severe penalties, fines and reputational damage. Here's an overview of key regulatory frameworks and compliance requirements:

Overview of Regulatory Frameworks

- **PCI:** PCI compliance relies on implementing secure technologies, processes, and practices to protect payment data throughout its lifecycle. Systems, applications, and services must meet PCI Security Standards to safeguard transactions and validate compliance.
- **CMMC for Department of Defense:** CMMC, Cybersecurity Maturity Model Certification ensures that Department of Defense (DoD) contractors meet specific cybersecurity standards to protect sensitive information. The certification framework includes multiple levels of maturity, each with requirements for processes and practices to secure controlled unclassified information. Achieving CMMC compliance is mandatory for organizations working with the DoD to ensure a secure defense supply chain.
- **Health Insurance Portability and Accountability Act (HIPAA):** HIPAA is a U.S. federal law that sets standards for protecting sensitive health information, known as protected health information (PHI). Covered entities, such as healthcare providers, health plans and healthcare clearinghouses, must comply with HIPAA's privacy, security and breach notification requirements to ensure the privacy, confidentiality and integrity of PHI.
- **General Data Protection Regulation (GDPR):** The GDPR is a comprehensive data protection regulation enacted by the European Union to safeguard the privacy and personal data of EU citizens. It imposes strict requirements on organizations that process and handle personal data, including consent mechanisms, data minimization, transparency and accountability. It requires organizations to obtain explicit consent for data processing, implement robust security measures and adhere to stringent data protection practices.

Compliance Requirements

- **Data protection standards**: Implement robust data protection measures and security controls to ensure compliance with applicable data protection regulations, such as encryption, access controls and regular security assessment and audits.
- **Reporting and notification obligations:** Establish procedures for promptly reporting and notifying regulatory authorities, affected individuals and other relevant stakeholders in the event of data breaches or security incidents, as required by data protection regulations.
- **Record-keeping and documentation:** Maintain detailed records and documentation of data processing activities, security policies, risk assessments and compliance efforts to demonstrate accountability and compliance with regulatory requirements.

Best Practices for Compliance

- **Conduct regular compliance audits:** Conduct regular audits and assessments to evaluate compliance with data protection and cybersecurity regulations, identify gaps and vulnerabilities and implement remediation measures to address deficiencies.
- **Stay informed about regulatory updates:** Stay informed about changes and updates to data protection and cybersecurity regulations, including new laws, regulations, guidelines and enforcement actions, to ensure ongoing compliance and adaptability to evolving regulatory requirements.

CHAPTER 9

Conclusion

Keys to Sustained Cybersecurity Success

Conclusion

Keys to Sustained Cybersecurity Success

As your business begins its journey to enhance its cybersecurity posture, it starts with educating your employees and learning the basics. The tips provided within this eBook can go a long way in ensuring sensitive information doesn't fall into the wrong hands.

Businesses must take the necessary steps to protect their intellectual property, confidential information and reputations while safeguarding their employees, customers and business partners. Succeeding in applying the necessary cybersecurity measures is paramount to your long-term business success.

1. **Vigilance is key:** Cyber threats constantly evolve, requiring constant vigilance and proactive measures to stay ahead of potential adversaries. By staying informed, practicing secure behaviors and implementing robust security measures, you can reduce the risk of falling victim to cyber attacks.
2. **Education empowers**: Knowledge is your most potent weapon in the fight against cyber crime. By educating yourself and your employees about common cyber threats, best practices for cybersecurity and compliance requirements, you can empower your employees to make informed decisions and mitigate risks effectively.
3. **Collaboration is critical:** Cybersecurity is a shared responsibility that requires collaboration and cooperation among individuals, organizations, governments and the cybersecurity community. By sharing threat intelligence, best practices and resources, we can collectively strengthen our defenses and build a safer, more secure digital ecosystem.
4. **Continuous improvement:** Cybersecurity is not a one-and-done effort but an ongoing process of continuous improvement and adaptation to evolving threats and challenges. Regularly assess your security posture, conduct risk assessments and update your security policies and practices to address emerging threats and vulnerabilities effectively.
5. **Stay connected:** Stay connected with the cybersecurity community, subscribe to security alerts and updates and continue learning and evolving your cybersecurity knowledge and skills. Remember, cybersecurity is a journey, not a destination.

Let's Get Started

Whether you are at the initial stages of formulating a comprehensive cybersecurity and incident recovery plan, or seeking to optimize your existing IT framework, Thriveon is here to guide you.

Every Thriveon Managed IT client receives a dedicated Fractional Chief Information Officer (CIO) who is committed to providing strategic insights, aligning technology initiatives with your business goals, and ensuring that your IT investments contribute to the overall success and security of your organization. At Thriveon, we recognize the significance of a tailored IT strategy, and our dedicated CIO plays a pivotal role in navigating your business through the complexities of the digital landscape, fostering innovation, and driving sustainable growth.

GET STARTED

THRIVEON
INFORMATION & TECHNOLOGY

www.thriveon.net
info@thriveon.net
855-767-2571