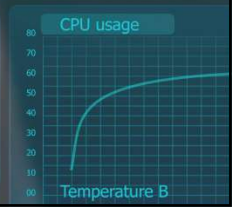
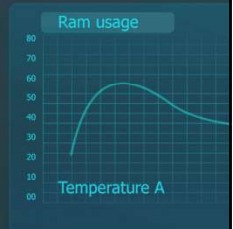
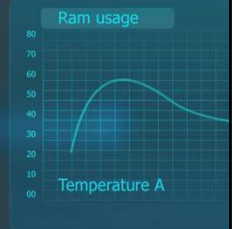


# Seven Tips To Protect Your Business in 2019

Atlas Cybersecurity

Login

- File
- Edit
- Object
- Search
- View
- Help



IP: 99.55.44.21  
Name: Name  
Age: 31  
Job: B...

IP: 10.55.12.57  
Name: Name  
Age: 47  
Job: Actor

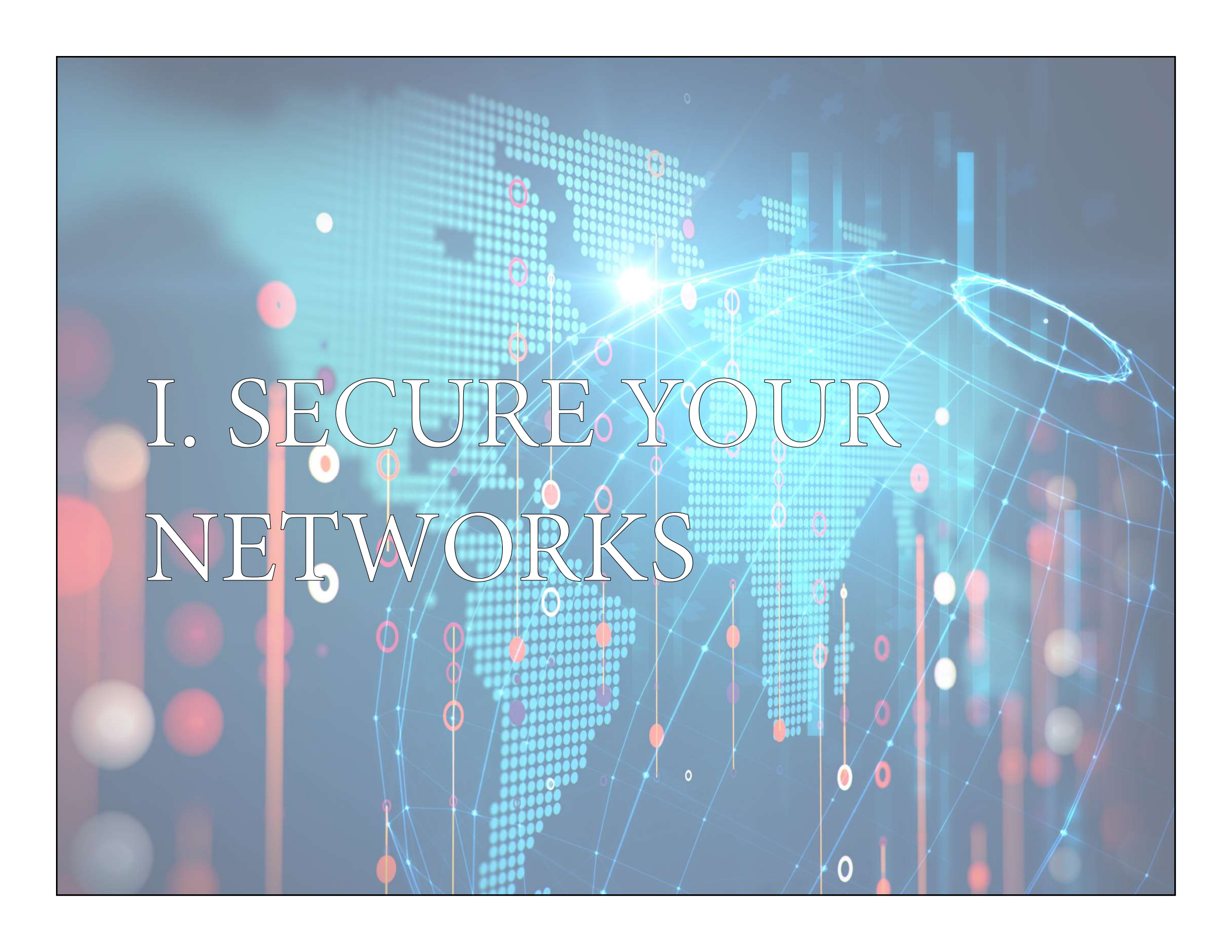
- HOME
- FILE
- SAVE
- BLOCK
- REPAIR
- LOCK



**ATLAS**  
CYBERSECURITY

In this e-book we provide you the top seven ways in which to protect yourself and your business from cyber threats in 2019. 2018 saw a remarkable rise in cyber incidents targeted towards small and mid-sized businesses with devastating effects. Nearly 60% of SMBs that were the victim of a successful cyber attack had to close operations within six months of the attack. These tips alone are not enough to fully protect your business, but they are a great first step to ensuring that you are not low hanging from the world's cyber criminals. If you don't want to worry about security, and you want an easy and streamlined process for locking down your business, call Atlas Cybersecurity today!



The background features a glowing blue globe with a grid of dots. Overlaid on the globe is a complex network of blue lines and nodes, some of which are highlighted with red and white circles. The overall aesthetic is high-tech and digital.

# I. SECURE YOUR NETWORKS

# SECURE YOUR NETWORKS

In today's world, the first step in securing yourself in cyberspace, starts by locking down your network. While a defined and secure perimeter cannot be relied on solely to provide security, it is the best place to start. By understanding the assets on your network, the way systems talk to each other, what applications are commonly used, and how your users browse the web, you can formulate a compelling network security posture using a standard next-gen unified threat management solution. When putting together your network security posture, ensure that you have the following elements included:

# SECURE YOUR NETWORKS

**Intrusion Detection/Prevention System:** Intrusion detection systems (IDS) and intrusion prevention systems (IPS) constantly watch your network, identifying possible incidents and logging information about them, stopping the incidents, and reporting them to security administrators. In addition, some networks use IDS/IPS for identifying problems with security policies and deterring individuals from violating security policies. IDS/IPS have become a necessary addition to the security infrastructure of most organizations, precisely because they can stop attackers while they are gathering information about your network. Three IDS detection methodologies are typically used to detect incidents: (1) Signature-Based Detection compares signatures against observed events to identify possible incidents. This is the simplest detection method because it compares only the current unit of activity (such as a packet or a log entry, to a list of signatures) using string comparison operations. (2) Anomaly-Based Detection compares definitions of what is considered normal activity with observed events in order to identify significant deviations. This detection method can be very effective at spotting previously unknown threats. (3) Stateful Protocol Analysis compares predetermined profiles of generally accepted definitions for benign protocol activity for each protocol state against observed events in order to identify deviations.

# SECURE YOUR NETWORKS

**Email Filtering**: A filtering solution applied to your email system uses a set of protocols to determine which of your incoming messages are spam and which are not. There are several different types of spam filters available:

- **Content filters** – review the content within a message to determine if it is spam or not
- **Header filters** – review the email header in search of falsified information
- **General blacklist filters** – stop all emails that come from a blacklisted file of known spammers
- **Rules-based filters** – use user-defined criteria – such as specific senders or specific wording in the subject line or body – to block spam
- **Permission filters** – require anyone sending a message to be pre-approved by the recipient
- **Challenge-response filters** – require anyone sending a message to enter a code in order to gain permission to send email

Spam filtering solutions are commonly deployed 3 different ways – hosted or in the “cloud”, on-premise using an appliance, and software installed on PCs that integrate with an email client such as Microsoft Outlook. Although no spam filtering solution is 100% effective, a business email system without spam filtering is virtually unusable and very susceptible to the most common type of cyber-attack: phishing. Many spam emails contain infected email attachments that contain viruses, phishing attacks, compromised web links and other malicious content. By preventing them from reaching your mailbox, your spam filter offers an additional layer of protection to your users.

# SECURE YOUR NETWORKS

**URL Filtering**: Users spend increasing time on the web, surfing their favorite sites, clicking on email links, or utilizing a variety of web-based SaaS applications for both personal and business use. While incredibly useful to drive business productivity, this kind of unfettered web activity exposes organizations to a range of security and business risks, such as propagation of threats, possible data loss, and potential lack of compliance. Traditionally, companies have used URL filtering as a tool to prevent employees from accessing unproductive sites. With today's URL filtering, firms enable secure web access and protection from increasingly sophisticated threats, including malware and phishing sites. URL filtering technology compares all web traffic against a URL filtering database, permitting or denying access based on information contained therein. Each website defined in the database is assigned to a URL category, or group, that firms can utilize in one of two ways: (1) Block or allow traffic based on URL category. Create a URL Filtering profile that specifies an action for each URL category and attach the profile to a policy. This includes categories for malware or phishing sites. (2) Match traffic based on URL category for policy enforcement. If the goal is for a specific policy rule to apply only to specific web traffic categories, add the category as match criteria when creating the policy rule. URL filtering is enabled through local database lookups, or by querying a master cloud-based database. Local lookups on a limited, but frequently accessed, number of websites ensure maximum in-line performance and minimal latency for the most frequently accessed URLs, while cloud lookups provide coverage for the latest sites. To account for firms' unique traffic patterns, on-device caches store the most recently accessed URLs, with the ability to also query a master database in the cloud for URL category information when an on-device URL is not found.

# SECURE YOUR NETWORKS

**Sandboxing**: Organizations of all sizes understand that sophisticated cyberattacks can use unknown malware to evade traditional gateway and endpoint protection. These advanced persistent threats, or APTs, use custom-developed targeted attacks to gain access to a network and remain undetected for long periods of time. The success of APTs depends on staying under the radar as long as possible, using evasive coding techniques to slip past traditional security barriers and steal sensitive data. One technology used to defend against these types of threats is a Sandbox. A sandbox is an isolated, safe environment, which imitates an entire computer system. In the sandbox, suspicious programs can be executed to monitor their behavior and understand their intended purpose, without endangering an organization's network. A sandbox provides a dedicated environment to analyze, understand and take action on the threats to your organization that haven't been detected by conventional security measures. Sophisticated, targeted malware, designed to evade detection, will be detected and blocked when detonated in your sandbox.



The background features a stylized globe with a network of glowing blue and cyan lines connecting various points, symbolizing global connectivity and data flow. A semi-transparent padlock icon is positioned on the right side of the globe, indicating security or encryption. The overall color palette is dominated by blues, cyans, and purples, with some warmer tones like orange and red visible in the background.

II. ENCRYPT ALL  
DATA AT REST AND  
IN-TRANSIT

# ENCRYPTION

Full disk encryption is a cryptographic method that applies encryption to the entire hard drive including data, files, the operating system and software programs. This form of encryption is comparable to the protection of your home. Just as locking all exterior entrances is an efficient way of ensuring that no unwanted visitors enter the interior living spaces of your home, full disk encryption places an exterior guard on the internal contents of the device. Unlike past iterations of full disk encryption, the process to encrypt hard drives has become quite simple and is supported by all the major vendors. For example, Apple offers built-in encryption for both the mobile IOS and the desktop OS X systems, Microsoft Windows offers its own native encryption software through BitLocker, and Android also supports encryption out of the box. However, because BitLocker is only available for higher-end versions of Windows, lower-tiered versions of Windows can utilize third-party encryption programs such as VeraCrypt. Mobile devices such as work phones, tablets and laptops have the unfortunate propensity of being lost or stolen. This can be disastrous for a company if a device is lost or stolen while containing sensitive information such as personally identifiable information (PII) or proprietary information. According to Verizon's 2015 Data Breach Investigation, 45 percent of healthcare breaches occurred due to stolen laptops. Furthermore, according to Bitglass's Financial Services Report 2016, one in four breaches that occurred in the U.S. financial sector over recent years was the result of lost or stolen devices.

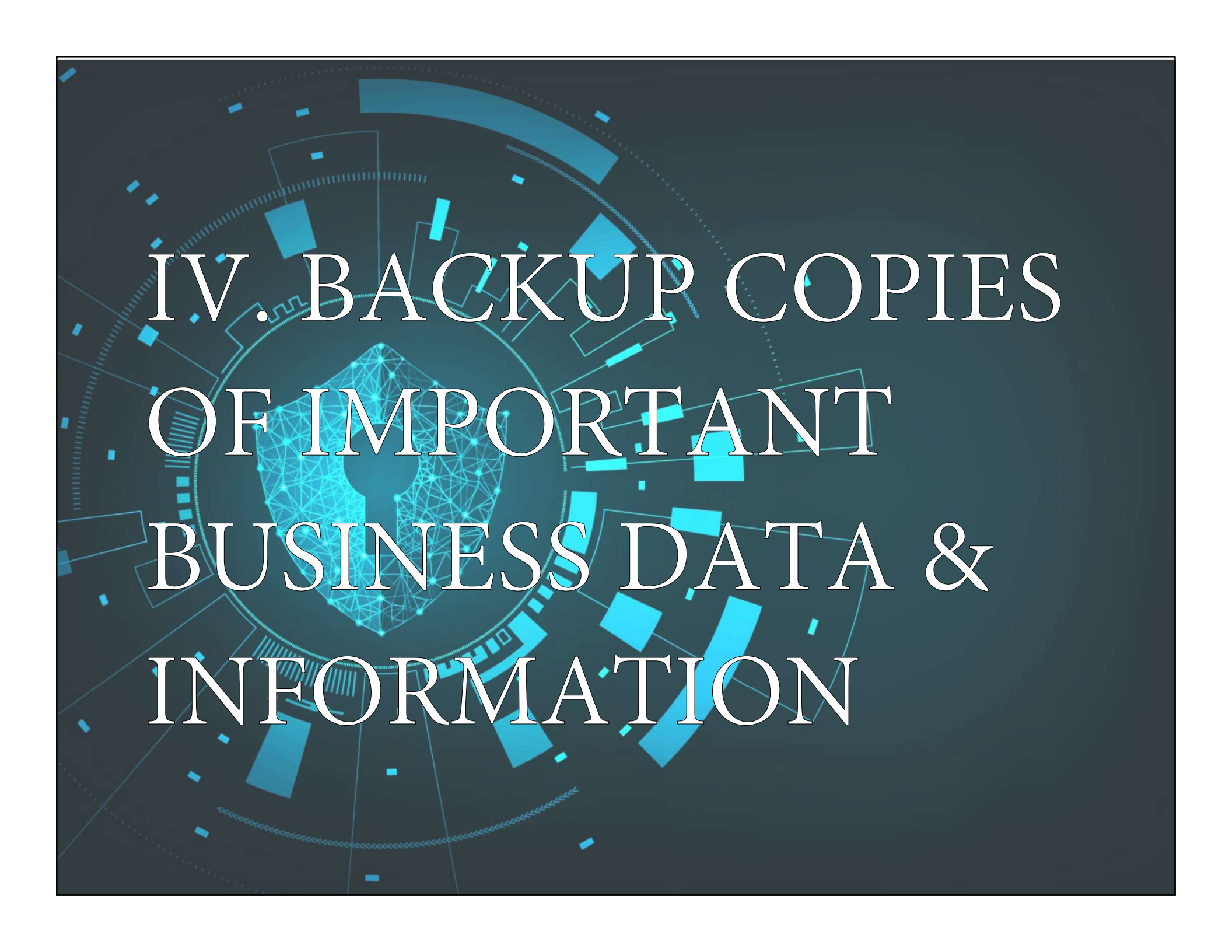


The background features a vertical gradient from orange at the top to dark blue at the bottom. It is filled with vertical columns of binary code (0s and 1s) in white and light blue. Several padlock icons are scattered throughout, some in light blue and some in a darker blue, appearing to be part of the digital data stream.

# III. PATCH YOUR SYSTEMS AND SOFTWARE

# PATCHING

Full disk encryption is a cryptographic method that applies encryption to the entire hard drive including data, files, the operating system and software programs. This form of encryption is comparable to the protection of your home. Just as locking all exterior entrances is an efficient way of ensuring that no unwanted visitors enter the interior living spaces of your home, full disk encryption places an exterior guard on the internal contents of the device. Unlike past iterations of full disk encryption, the process to encrypt hard drives has become quite simple and is supported by all the major vendors. For example, Apple offers built-in encryption for both the mobile IOS and the desktop OS X systems, Microsoft Windows offers its own native encryption software through BitLocker, and Android also supports encryption out of the box. However, because BitLocker is only available for higher-end versions of Windows, lower-tiered versions of Windows can utilize third-party encryption programs such as VeraCrypt. Mobile devices such as work phones, tablets and laptops have the unfortunate propensity of being lost or stolen. This can be disastrous for a company if a device is lost or stolen while containing sensitive information such as personally identifiable information (PII) or proprietary information. According to Verizon's 2015 Data Breach Investigation, 45 percent of healthcare breaches occurred due to stolen laptops. Furthermore, according to Bitglass's Financial Services Report 2016, one in four breaches that occurred in the U.S. financial sector over recent years was the result of lost or stolen devices.




IV. BACKUP COPIES  
OF IMPORTANT  
BUSINESS DATA &  
INFORMATION



# BACKUPS

In a data-driven world where information is often a company's most valuable asset, protecting data is more important than it's ever been. In one of the most significant cyberattacks of 2017, the WannaCry outbreak caused massive damage—up to \$4 billion according to one estimate—to businesses around the world. The estimate doesn't just account for the lost data, but also from its related consequences like the loss of productivity and data restoration costs. Operating systems, software, and even hardware can be replaced, but data is not so easily recoverable or replaceable. While there are solutions that can completely or partially recover lost data, these are often neither inexpensive, nor do they work for every kind of circumstance. What companies need to understand is that the most effective solution to prevent data loss is also the most obvious one: backing up data. Why are backups important? Everyone who stores data on a device—whether it's consumer databases, employee files, medical records or even simple photographs of memorable events—should make it a point to back it up in one form or another. However, organizations are often the ones who have the most to lose when it comes to data loss, as this often results in consequences that can affect production and services. A large number of data loss incidents can be prevented—or at least mitigated—by the proper backup of data files. It is an aspect of security that organizations should prioritize given the importance of data in their operations. Every March 31, the world celebrates what is known as World Backup Day, which serves as a reminder of the importance of backing up to protect data. However, it should also be a reminder that backing up isn't something one only does on a single day of the year: backing up data should be performed on a regular basis as part of a company's culture of security.




V. USE STRONG  
PASSWORDS AND  
TO CHANGE THEM  
OFTEN

# PASSWORDS

Creating strong passwords may seem like a daunting task, especially when the recommendation is to have a unique password for each site you visit. Anyone would be overwhelmed if they had to create and memorize multiple passwords like Wt4e-79P-B13^qS. As a result, you may be using one identical password even though you know it's unsafe and that if it gets compromised all of your web information is exposed. Or you use several passwords, but they are all short simple words or include numbers that relate to your life they are still too easy to guess. Or, if you made hard to remember passwords (probably because your business or a website forced you to) then you likely have a list of the passwords right next to your computer - even though you know this also compromises your safety if others use your computer. Passwords you can't remember are useless. But passwords that are too easy to remember can be easy to guess or to ascertain with a brute-force attack. With activities like personal banking and retirement increasingly migrating online, the stakes continue to rise. The key aspects of a strong password are length (the longer the better); a mix of letters (upper and lower case), numbers, and symbols, no ties to your personal information, and no dictionary words. The good news is you don't have to memorize awful strings of random letters numbers and symbols in order to incorporate all of these aspects into your passwords. The secret to creating a hard-to-crack password that's unique and easy to remember is to focus on making it memorable and making it hard to guess. Seems simple enough, right? By learning a few simple skills, you can easily create a strong and memorable password with minimal effort. Plus, creating them can actually be fun - and your payoff in increased safety is huge.



The image features a blue gradient background. In the center, there is a white login form with the text "Enter your login information:" at the top. Below this, there are two input fields: "User name:" and "Password:". The "Password:" field is filled with black dots. At the bottom of the form, there are two buttons: "OK" and "Cancel". A pair of glasses with a thin metal frame is positioned over the form, with the lenses resting on the "User name:" and "Password:" fields. The text "VI. TRAIN EMPLOYEES IN BASIC SECURITY PRINCIPLES" is overlaid on the image in a large, white, serif font, centered horizontally and vertically.

VI. TRAIN  
EMPLOYEES IN  
BASIC SECURITY  
PRINCIPLES

# TRAINING

Educating employees on security is more crucial than ever. Data from London-based advisory and solutions company Willis Towers Watson points to internal employees — whether through negligence or deliberate offense — as the cause of 66 percent of all cyber breaches. Figures like this are prompting security managers to put more resources into security awareness training. The Path to Effective Security Awareness Training When the Financial Services Information Sharing and Analysis Center (FS-ISAC) reached out to security managers about cyberdefense for its 2018 CISO Cybersecurity Trends report, 35 percent said they consider employee training a critically high priority for improving security posture. While awareness training is indeed not a new concept, gone are the days when merely giving employees a series of videos to watch was considered sufficient — especially in the absence of any follow-up measures. Security awareness training programs need to be interesting, engaging and memorable to be effective, said Lisa Plaggemier, director of security culture and client advocacy at CDK Global. Plaggemier believes the entire concept of awareness programs needs a revamp. (She even gave a talk on the subject, Let's Blow Up Security Awareness and Start Over, at the 2018 RSA Conference.)



A person is holding a smartphone, and a futuristic digital overlay is visible on the screen. The overlay features various data visualization elements such as bar charts, line graphs, and a circular gauge showing '2%'. The background is a blurred image of a person's hands holding the phone. The text 'VII. MOBILE DEVICES, SECURITY POLICIES AND USES' is overlaid in a white, serif font with a drop shadow effect.

VII. MOBILE  
DEVICES, SECURITY  
POLICIES AND USES

# MOBILITY

Mobile device management (MDM) is software that allows IT administrators to control, secure and enforce policies on smartphones, tablets and other endpoints. MDM is a core component of enterprise mobility management (EMM) which also includes mobile application management, identity and access management and enterprise file sync and share. The intent of MDM is to optimize the functionality and security of mobile devices within the enterprise while simultaneously protecting the corporate network.

## Sources

- <https://www.ltnow.com/email-spam-filters-work/>
- <https://www.paloaltonetworks.com/cyberpedia/what-is-url-filtering>
- <https://news.sophos.com/en-us/2016/04/13/what-is-a-sandbox-and-why-do-i-need-one-to-defend-against-advanced-threats/>
- <https://www.csoonline.com/article/3247707/encryption/full-disk-encryption-do-we-need-it.html>
- <https://www.idtheftcenter.org/what-are-security-patches-and-why-are-they-important/>
- <https://www.trendmicro.com/vinfo/us/security/news/virtualization-and-cloud/best-practices-backing-up-data>
- <https://securityintelligence.com/4-essentials-for-effective-security-awareness-training/>
- <https://www.juniper.net/us/en/products-services/what-is/ids-ips/>