bis Getting IT done.

THE ULTIMATE SECURITY GUIDE FOR BUSINESSES

TO SAFEGUARD AGAINST **RANSOMWARE**

Reduce the threat of a ransomware security breach

Business Information Solutions, Inc. | www.askbis.com | Phone: 251.410.7601

UNDERSTANDING RANSOMWARE

Do you remember ransomware, the malicious software that blocks computer access until a ransom demand is paid? In the past, the threat was huge and dominated headlines, but it seems to have slowed down in recent months.

Could the decline in publications citing ransomware as the cause of data breaches indicate that cybercriminals have given up on dishing out the malware? The answer is no, not even close!

Although the chatter around the malicious software may have quieted down, the threat is very much alive and working hard to hand out ultimatums to its victims – pay up to unlock your data or lose it indefinitely.

Cybercriminals are continuously improving their techniques and attack methods, a large contributor to the fact that we're hearing less about ransomware than many other attacks that have recently risen in popularity. Aside from the growing threats in the news, such as targeted phishing attacks and Business Email Compromise (BEC) scams, the de-emphasis on ransomware in large part comes from cybercriminals finding new ways to infiltrate a user's system in a more targeted, harder to measure approach.

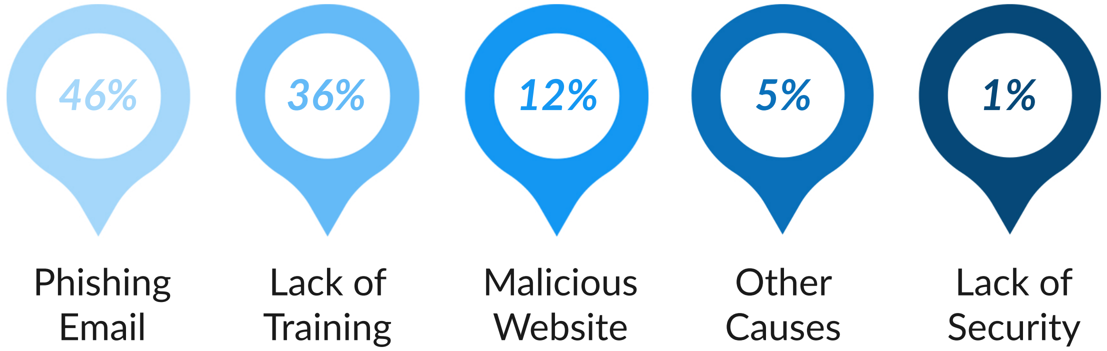
WARNING
Your file have been encrypted!!
WARNING
Your file have been encrypted!!

HOW RANSOMWARE IS DISTRIBUTED

The most common way for ransomware to be distributed is via a phishing email containing malicious attachments. The malware may be directly inside the attachment or may include a link to a website hosting the malicious software. Another common method for dispersing malware is by using an exploit kit to search for vulnerabilities in outdated software and then exploiting those vulnerabilities.

Vulnerable servers are also an open door for cybercriminals to distribute ransomware. Once a hacker gains access to a server, they can do serious damage, some of which may involve using administrative rights (which can also be obtained relatively easy with the right tools) to turn off certain protections that may alert administrators of the threat.

Causes of Ransomware



WHO IS A TARGET?

Everyone can be a target for ransomware. While cybercriminals do have industries they favor and target, such as the healthcare and financial industries, everyone is susceptible to a ransomware attack if the proper training and security measures aren't in place. Whether an individual user, small business, or large enterprise, everyone is fair game to a cybercriminal looking to make money via ransomware.

With that said, cybercriminals may be doing more research these days to choose their victims. Many believe that hackers are targeting fewer victims through ransomware, however, the truth is that they are just choosing the right victims. What does that mean? Cybercriminals are choosing targets who they believe CAN afford to pay large ransoms and CANNOT afford to lose their data – resulting in fewer attacks but more success for the attacker.

A company is infected with ransomware every 40 seconds

Kapersky

22% of victims had to stop business operations after being infected with ransomware

Malwarebytes

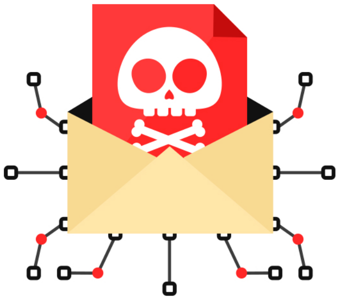
70% of companies end up paying the fine after falling victim to ransomware

Systemize

10x The cost of downtime from ransomware is 10x higher than the ransom demanded per incident

KnowBe4

61% of cyber victims were SMBs with less than 1,000 employees *cbia*



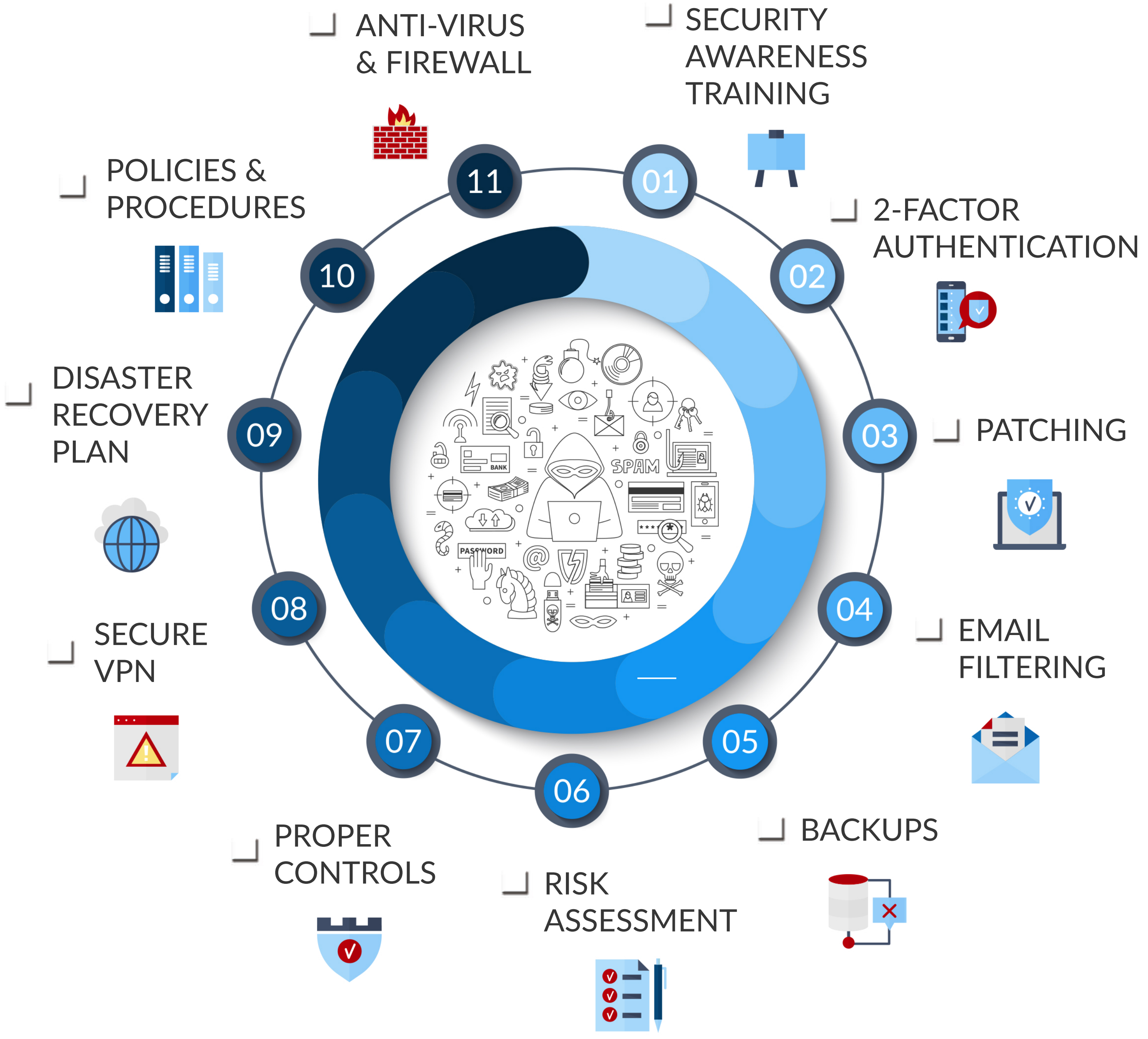
bis

BUSINESS INFORMATION SOLUTIONS

Getting IT done.

11 Tips to Help Protect Your Organization from Ransomware

The best defense against cyber threats is a strong offense. Organizations should proactively implement the following security protections to stay one-step ahead of hackers.



01 □ SECURITY AWARENESS TRAINING

02 □ 2-FACTOR AUTHENTICATION

03 □ PATCHING

04 □ EMAIL FILTERING

05 □ BACKUPS

06 □ RISK ASSESSMENT

07 □ PROPER CONTROLS

08 □ SECURE VPN

09 □ DISASTER RECOVERY PLAN

10 □ POLICIES & PROCEDURES

11 □ ANTI-VIRUS & FIREWALL

□ Security Awareness Training

Provide security awareness training routinely to educate employees on current threats and best practices.

□ Two-Factor Authentication

Utilize two-factor authentication as an added security metric for gaining access to your system and your company's sensitive data.

□ Patching

Keep your systems up-to-date and patch when necessary to prevent system vulnerabilities from being exploited.

□ Email Filtering

Email filters should be put in place to help identity and block known threats on incoming communications.

□ Backups

Confirm routine backups of your company's data are being performed.

□ Risk Assessment

Perform a yearly risk assessment to find vulnerabilities within your network.

□ Proper Controls

Ensure that proper controls are in place that only allows employees to access areas and information needed to perform their job function.

□ Secure VPN

If users are connecting remotely to your network, make sure it is done so securely through a VPN.

□ Disaster Recovery Plan

Have a disaster recovery plan in place to ensure that your organization knows how to respond a ransomware attack if one were to occur.

□ Policies & Procedures

Implement policies and procedures that outline your organization's rules and expectations such as password requirements.

□ Anti-Virus & Firewall

Make sure your organization is using reputable anti-virus software and firewall.

Get Your {FREE} Cybersecurity Training for Your Staff!

bis
BUSINESS INFORMATION SOLUTIONS
We Get *IT* Done!

A Special Offer Just for You...

Phillip Long,
CEO & CISSP

Training Videos
The content goes over cybersecurity best practices

Testing
Employees are required to take security tests

Admin Reporting
Administrators can view security reports & see testing scores

Reminders
Automated security reminders can be sent out to staff

BONUS: Complimentary network audit to find any vulnerabilities in your network

Get your FREE Security Training for Your Staff by calling 251-410-7601 or emailing security@askbis.com!

Business Information Solutions, Inc. | www.askbis.com | Phone: 251.410.7601