Cibecs

IT MANAGER'S GUIDE

8 Steps to Protect Your Users From A RANSOMWARE ATTACK

MORE THAN 4,000 RANSOMWARE ATTACKS HAVE OCCURRED EVERY DAY SINCE THE BEGINNING OF 2016

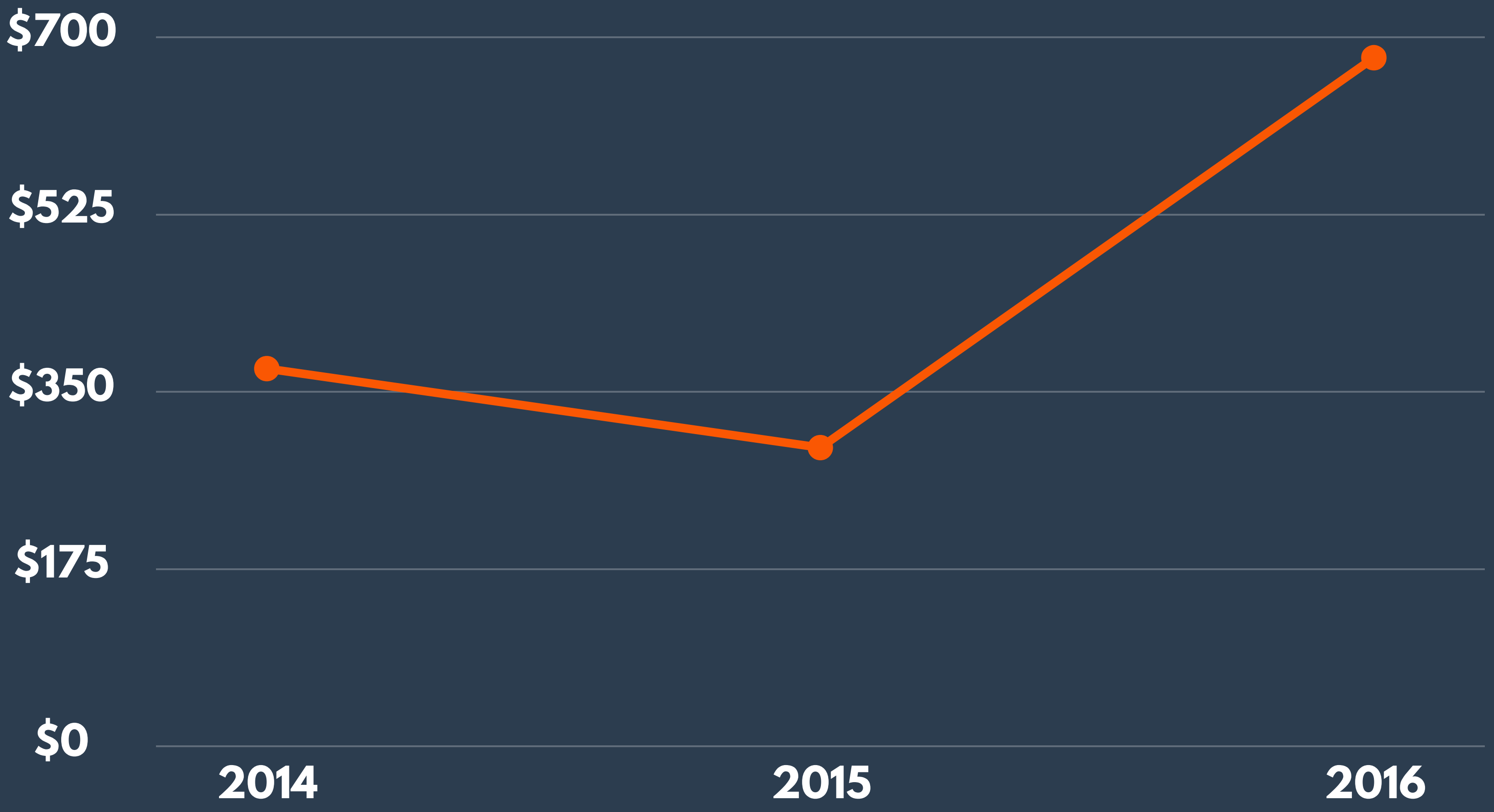
CCIPS RESEARCH

EVEN MORE FRIGHTENING, 41% OF BUSINESSES HAVE EXPERIENCED A RANSOMWARE ATTACK...

OSTERMAN RESEARCH

Cibecs

AND THE AVG. RANSOM DEMAND IS GROWING



SOURCE: SYMANTEC

Cibecs

DON'T LET IT BE YOU NEXT

HERE ARE OUR 8 STEPS FOR IT MANAGERS TO PROTECT USERS AGAINST RANSOMWARE ATTACKS

Cibecs

1. IMPLEMENT SECURE, AUTOMATED ENDPOINT BACKUPS

PROTECT THE DATA ON LAPTOPS & DESKTOPS

Ransomware targets data that is stored on endpoint devices, exploiting the fact that a huge number of users & companies do not have adequate backup policies and systems in place.

DON'T TRY USE A CLOUD FILE-SHARING SERVICE INSTEAD

This can't be substituted by employing a service like Dropbox. If you have your Dropbox folder mapped locally, the Ransomware can encrypt your Dropbox files as well.

IT NEEDS TO GIVE YOU COMPLETE CENTRAL CONTROL

The solution must give you central control over Backup Policies so that you can automate the daily backup of critical user data without needing any user intervention

Cibecs

2. THE SOLUTION MUST HAVE
BUILT-IN LOCAL FILE ENCRYPTION

Local data encryption protects data stored on laptops or desktops from being accessed by unauthorised users.

This is an essential part of your data protection strategy.

Local file encryption can also protect against Ransomware that threatens to leak your data such as Leakware or Doxware, reducing the risk of confidential or valuable data being leaked online.

Cibecs

3. MAKE SURE YOU CAN REMOTELY WIPE DATA

A user working remotely falls victim to a Ransomware attack. They call the IT Department.

NO PROBLEM

IT can forensically wipe the device regardless of where the user is. Once the computer is wiped, the safe and unencrypted backed up version of the user's data can be restored and the user can continue working.

NO RANSOM REQUIRED

Cibecs

4. DON'T GO IN BLIND
SHOW HIDDEN FILE EXTENSIONS

Ransomware frequently arrives as a disguised file, where the file is named with an extension such as ".PDF.EXE"

The Window's default behaviour is to hide known file-extensions. You can make disguised Ransomware files easier to detect by re-enabling the ability to see the full file-extension.

Cibecs

5. KEEP WITH IT
UPDATE YOUR SOFTWARE & OS

LIKE TAKING CANDY FROM A BABY

Malware relies on people or organisations running outdated operating systems and software with known vulnerabilities

DO YOUR UPDATES

By keeping your user's software and Operating System up to date you'll save yourself a lot of hassles

OR AUTOMATE THEM

Keep your user's anti-virus and anti-malware solutions set to automatically update and conduct regular scans

Cibecs

6. GET CRYPTIC

GIVE YOUR USERS STRONG PASSWORDS

PASS123 = A WAY IN

Ransomware attackers sometimes brute force weak passwords.

A strong, difficult to guess password is a vital first defence. Give your users strong, complex passwords to protect them.

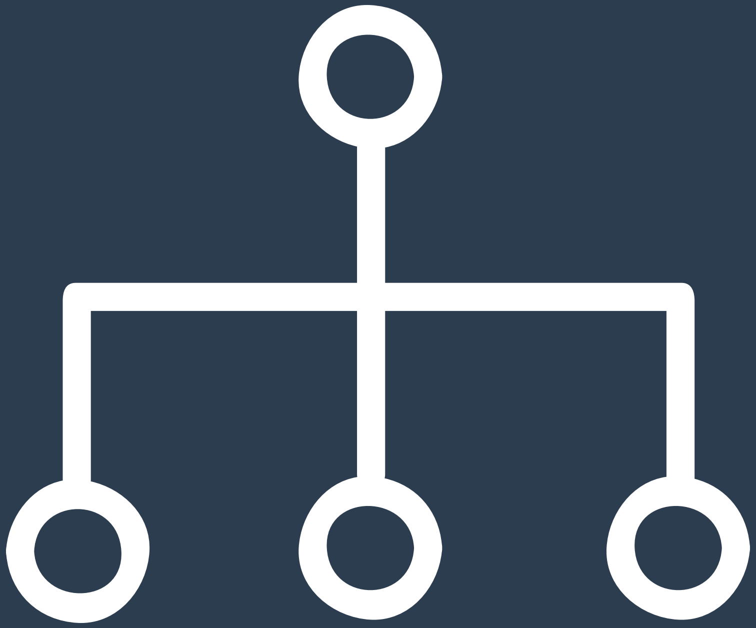
NO MORE MR NICE GUY

Cibecs

7. STOP IT FROM SPREADING BY DISABLING RDP

Malware often accesses target computers using Remote Desktop Protocol (RDP) which is a Windows utility that allows others, usually an IT administrator, to access the desktop remotely.

If you do not need RDP, you should disable it for all your users to stop Ransomware from spreading and to prevent RDP exploits.



Cibecs

8. EDUCATE YOUR USERS

GIVE THEM THE HEADS UP

Without understanding how Ransomware works and what to look out for, your users are sitting ducks.

DOWNLOAD OUR PRINTABLE GUIDE

Give your users our single page guide. It has a comprehensive summary that will help them understand what Ransomware is, the risks, and how to make sure you are Ransomware aware.

CLICK HERE

TO DOWNLOAD OUR FREE PRINTABLE PDF:
A USER'S GUIDE TO RANSOMWARE

THE NEXT STEP:

VISIT WWW.CIBECS.COM

DISCOVER THE BEST ENDPOINT DATA BACKUP & PROTECTION FOR BUSINESS

Click here to

Start your 30 Day Free Trial

Cibecs