

Ransomware Survival: Prevention is the best protection

The threat landscape has evolved

Legacy Attacks

Ransomware

What does
an attack
look like?



Hackers are looking for financial credentials or to steal large quantities of private data to sell or make openly accessible.

Data is held hostage or even deleted until you pay the ransom

How do they
get in?



Hacking into databases and internal systems via root kits, key loggers and Trojans, bot net attacks, etc.

Using advanced social engineering (sophisticated emails with a malicious file or link, website advertisements with malicious links)

Which data
do they steal?



Information that can be bought and sold (credit card numbers, bank accounts info, social security numbers, engineering plans and other intellectual property

Information of value to your business that you will pay to get back (operational data, documents, research, budget information etc.)

Can your business afford a ransomware attack?



Ransomware locks down the files required to run your business, there is no guarantee that you will get your files back, even if a ransom is paid.

Ask yourself:

Can I afford to pay hundreds or even thousands of dollars in ransom?

Can my business continue operating if files become encrypted?

What would three days of downtime cost?

How would an attack impact my customers?

Would a ransomware attack damage my business' reputation?

Prevention is the best protection!

Learn how to protect your (customers) business with the Good, Better, Best prevention model

GOOD

BETTER

BEST

Backup files to an external drive or secure cloud



Backup to an external hard drive

Backup in two formats and keep a copy offsite

Use bare metal backup and/or file and folder backup stored in the cloud

Educate employees and create policies



Boost Employee awareness

Implement mandatory ransomware training/testing for employees

Train employees and create internal policies for reporting and handling ransomware

Update all software to the latest version



Keep your operating system (OS) up to date

Keep your OS and applications up to date

Keep your OS and applications up to date in addition to removing toolbars and freeware

Use multi-level Antivirus Protection



Use antivirus

Use antivirus with anti-spam

Use antivirus with anti-spam and link scanning.