CYBERATTACK SURVIVAL

Prevention is the best protection

	Yesterday's Attacks	Today's Attacks
What does an attack look like?	Hackers targeted enterprises to obtain high value data, such as financial records, that they could either sell or make openly accessible.	Hackers are still looking for high value data, but now take aim at SMBs with the same customer data, less budget for security, and more connections to enterprises.
How do they get in?	They got in by hacking into databases and internal systems via root kits, key loggers and Trojans, and botnet attacks.	Today, hackers use advanced social engineering techniques to trick unsuspecting users into handing over confidential or sensitive data.
Which data do they steal?	Information that can be bought and sold such as credit card numbers, bank account information, social security numbers, and more.	Using phishing, attackers attempt to install programs on company devices to mine cryptocurrency, and pose as trusted employees or businesses asking for money transfers via emails.

Can your business afford a cyberattack?

It can take *hours, weeks, months*, or even years to restore systems and operations

3in5

SMBs have experienced a cyberattack in the last 12 months

20%

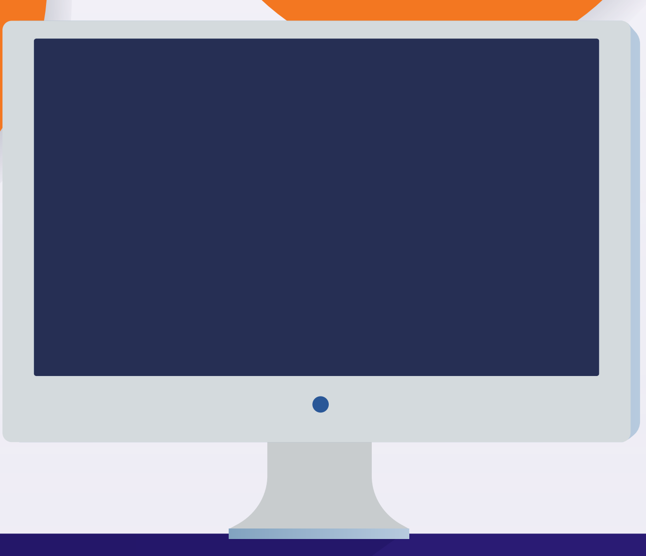
of those businesses attacked had to cease operations immediately

8hrs-1wk

The amount of time businesses spent wiping and restoring all the infected computers

40%

of infections spread to multiple devices throughout the network

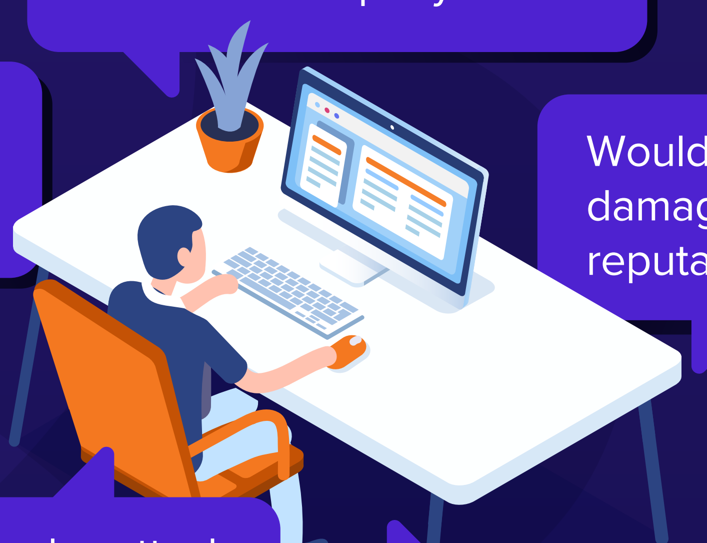


Ask yourself:

Can my business continue to operate if I don't have access to company files?

What would three days of downtime cost?

Would a cyberattack damage my business' reputation?



How would a cyberattack impact my business?

Can I afford to pay hundreds or even thousands of dollars to remediate a cyberattack?

Prevention is the best protection!

Learn how to protect your business with the **Good, Better, Best** prevention model

GOOD

ANTIVIRUS
One of the most important ways to defend devices in your business is by installing and monitoring antivirus software on all devices.

PATCH MANAGEMENT
Regular patching ensures software and applications are updated, providing a critical defense against software vulnerabilities that could lead to successful cyberattacks.

EMAIL SECURITY
End-to-end encryption of company emails so the content can only be read by the sender and the receiver.

SECURE REMOTE WORKING
To ensure remote employees have a secure connection to company data and applications, it is important to provide them with a VPN connection that encrypts all traffic.

BACKUP & DISASTER RECOVERY
Even the most sophisticated security measures are not enough in some cases. So it is important to have a solid backup and disaster recovery solution in place that can restore operations quickly and easily.

BETTER

WEB GATEWAY
Secure web and internet gateways filter unwanted and malicious web traffic to protect your network from a cyberattack. It usually incorporates URL filtering, SSL inspection, sandboxing of unknown files, and policy application

AUTHENTICATION
This starts with defining password policies for your business. It also helps to install a password manager that generates random, strong passwords for each login environment and allows for Single Sign On. Multi-factor authentication is another good option.

BEST

SECURITY POLICY
This involves defining business processes and security policies for the entire organization to follow.

DATA LOSS PREVENTION
A data loss prevention solution prevents end users from sharing sensitive data outside the company network by helping you regulate what data end users can transfer outside the network.

SERVER HARDENING
Web servers usually sit at the edge of the network making them more vulnerable to attacks. Proper hardening ensures default configurations are changed and that certain services are disabled.

SECURITY AWARENESS & TRAINING
It's crucial to educate your users on how to defend themselves, for example, by creating strong passwords and recognizing phishing emails. Knowledge is key when it comes to cybersecurity, so it is important to provide regular training.

Running your business should be your number one priority — let us focus on your security

Contact us today to learn more about business protection against cybercrime.

Sources:
http://bit.ly/2jLZq9a
http://bit.ly/2y4svWK
http://cnnmon.ie/2tGFWGv
http://cnet.co/2tYilvY
http://cnet.co/2f7hBYa

avast business