Ransomware:

It's about customer trust

It does not take much for your business to be crippled by ransomware. An "innocent" click on a suspicious advertisement or a link in an email. Even a visit to a legitimate website can land you in trouble, if the site is infected with code installed to redirect users to a malicious website.

When that happens, all your company files are encrypted and there will be a request for ransom. After you've paid, you will get back your files—or you may not, as some companies found out during a recent ransomware attack.

Every 40 seconds, a business is hit globally and one in five SMBs do not get their data back even after they've paid the ransom.[1]

Ransomware is a type of malicious software that threatens to publish the victim's data or perpetually block access to the data unless a sum of money, or ransom, is paid. Some ransomware is even more vicious: Your data is destroyed even after you have paid.[2]

40%

of global businesses experienced a ransomware incident during 2015.[3]

60%

of global ransomware attacks demanded $1,000 or more.[3]

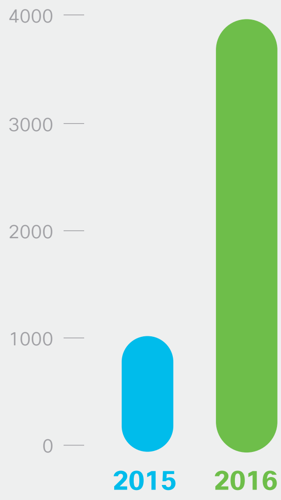
$ 1 billion

is the estimated amount cyberthieves made off with in 2016 alone.[4]

If you think your business is safe because it is too small to attract a cyberthief's attention, think again.

According to the U.S. Federal Bureau of Investigation (FBI) estimates, on average, there has been a 300% increase in daily ransomware attacks since 2015.[5]

Number of ransomware attacks per day



Results of the WannaCry ransomware attack in May 2017:[6]

150 countries hit	300,000 machines infected	200,000 companies victimized

The point is, ransomware respects neither you nor your company. No company is immune, but small and medium-sized businesses (SMBs) are more vulnerable because of budget constraints and smaller spend on IT infrastructure and security.

What can SMBs do to beef up their defenses against ransomware attacks?

Some experts have suggested that companies buy insurance against cyber attacks.[7] This may not be cheap, and does not prevent an attack in the first place. Also, while insurance can help recover costs related to the ransom payment and other IT expenditure caused by the fallout, there is no guarantee that you can recover your data.

For ransomware, prevention is the best cure.

Here are some steps your company can take to reduce its exposure to attacks:

01 Educate employees on the do's and don'ts of ransomware attacks. One simple reminder is to never click on any unsolicited links or email attachments.

02 Maintain a security protocol that can protect your employees while they are on the go and using mobile devices such as laptops.

03 Install a virtual security system that detects and contains. This system can continuously monitor your networks, identify malware exploit kits, and prevent malware code from executing. It will also block malicious command-and-control traffic, malicious files, and malicious URLs in emails.

04 Reduce infection risk by developing a proactive security plan that leverages on a multilayer defense, by having predictive intelligence to understand where attacks are staged on the Internet, while also continuously improving your network hygiene and evaluating your security posture.

05 Make sure you have a current business continuity plan. Back up all your critical data regularly. Test the integrity of the backups and ensure that the restoration process is always working. Backups should not be connected to your system networks and should be stored in the cloud or in offline physical storage.

06 Conduct an annual vulnerability assessment, which can include simulated cyber attacks.

07 Have a consistent and comprehensive patch management process in place.

08 Smaller businesses that cannot afford in-house IT teams can engage external security expertise and delegate control of IT systems to managed service providers (MSPs).

> Many SMBs list security as the highest priority when it comes to buying technology infrastructure for the company.
>
> –IDC study commissioned by Cisco[8]

SMBs globally are now more aware of the need to protect against ransomware and other cyber attacks.

The SMBs interviewed in the IDC study also said that they rely on solutions provided by established brands, which they find are more trustworthy and have enough built-in security.

Your business should not be left in the dark.

At Cisco, we know that customer data is the lifeblood of your company. Securing this information is non-negotiable. Ultimately, the best reason for an SMB to invest in a strong suite of cyber defense solutions is to secure customer trust. Learn how Cisco Start can help you do that.

Sources

1. *The Cost of Cryptomalware: SMBs at Gunpoint*, Kaspersky Lab, Sept. 7, 2016.
2. Robert Hackett, “Why You Shouldn’t Pay the Petya Ransomware,” Fortune, June 28, 2017.
3. “40 Percent of Enterprises Hit by Ransomware in the Last Year,” Security Magazine, Aug. 4, 2016.
4. David Fitzpatrick and Drew Griffin, “Cyber-extortion losses skyrocket, says FBI,” CNN Money, Apr. 15, 2016.
5. *How to Protect Your Networks from Ransomware*, Federal Bureau of Investigation.
6. “Stop Ransomware in Its Tracks,” Cisco Umbrella.
7. “Extreme cyber attack could cause $120bn in damage,” Lloyd’s, July 16, 2017.
8. Detailed findings of this study will be released soon.