# Don’t be held hostage by ransomware

November 2016

**According to new research from Kaspersky Lab, small and midsize businesses rank ransomware in the top 3 most concerning IT security problems. Survey findings also reveals that 20% of companies worldwide have been subjected to IT security incidents as a result of a cryptomalware-based attack and the average amount of damage caused by one attack may cost small and midsize businesses up to $99,000.**

File-encrypting malware is hardly new, but its ability to continuously evolve into new forms is what makes it so dangerous. The fight to secure your business is a never-ending battle. Ransomware is a particular strain of malware that quietly works in the background to encrypt user documents with a secret cryptographic key kept at a remote location and threatens to only release this key upon payment to the perpetrators.

This type of malware has mostly changed in its increasing sophistication and prevalence, as well as the use of schemes that offer little hope of undoing by the time its nefarious encrypting work is completed. According to Software Advice, businesses are taking note of the risks surrounding this malware. Sixty-seven percent of business decision-makers claim they'd never pay a ransom to regain access to infected files, yet only 23 percent say they're "very confident" their data is secure from ransomware attacks.

Fortunately, a bit of preparation can go a long way toward defending against this scourge. Follow these three simple steps to help combat this threat in your business:

**1. Defend against malware**

Since ransomware is just another type of malware, it shouldn't be surprising the best strategy to stop it in its tracks is to beef up your business's defenses against malware in general. Tried and tested strategies on this front include timely software updates and patching, the use of anti-malware on end-user devices, and security software gateways, such as email and proxy servers.

It's also important for IT to educate users about safe computing practices and common attack vectors used by hackers. While businesses can't realistically expect employees to stay immune in the face of each and every phishing or social engineering attempt,

user training helps raise the bar, so hackers searching for the lowest hanging fruit may decide to try their luck elsewhere.

**2. Set granular access rights**

An underutilized defense against ransomware is the establishment of suitably granular access rights, so the damage caused by an infestation is better contained. To start, try logging into a computer or device as an administrator to limit the damage only to that.

You can also limit the network resources able to be accessed by default. Some businesses tend to be guilty of excess mapping of network drives on various computers and servers to more easily access or transfer files across the local area network. Because many of these mappings are created with full write access to remote users, they end up serving as conduits the file-encrypting malware can leverage to cause more widespread damage. An infected workstation could easily end up encrypting the data files for the account's server, for example.

**3. Rely on multifaceted data backups**

Finally, the traditional defense against ransomware has always entailed having backups to replace the damaged originals. Unfortunately, it isn't altogether unknown for some victims to end up with the encrypted version of their files in backups, too. Though cloud storage services are an ideal defense against failed storage drives, files synchronized to the cloud are not true backups.

For a more sophisticated defense, you can embrace a multifaceted data backup approach that relies on the use of more than one form of backup. With proper backup software, for example, changes in files could be stored on an on-premise storage appliance. This could, in turn, be backed up onto an off-line media, such as a tape drive or via batch jobs to a secure cloud location.

Without question, ransomware attacks will continue to evolve as the cyber criminals behind them seek to infect as many users as they can. Regardless of what they do next, these three simple strategies should go a long way toward preventing, mitigating, and recovering from such attacks.