Avast Business

White paper

5 Steps to protect businesses from ransomware

15 November 2023

Avast Business

Introduction

Ransomware is on the rise and shows no signs of slowing down. The global cost of damages due to ransomware attacks is predicted to reach $20 billion by the end of 2021, according to Cybersecurity Ventures.

It's not an exaggeration to say that ransomware presents an existential threat to the livelihood of U.S. and global businesses in sectors such as education, financial, government, healthcare, law enforcement, and telecommunications. Victims of ransomware — and the citizens, customers, investors, and patients that these organizations exist to serve — have much to lose.

In the first half of 2020, businesses, institutions of higher education, and local governments dedicated nearly $145 million to placate hackers and restore data and networks after being struck by major ransomware attacks. And paying ransom didn't — and doesn't — guarantee that such organizations get their data back. As if paying a ransom for your own data isn't demeaning and exhausting enough, the financial and other negative impacts of ransomware extend far beyond the ransom. Victims of ransomware also have to contend with added IT costs, lost productivity, mounting legal fees, the need for network modifications, and/or subscription fees for new credit monitoring services for employees or customers.

Fortunately, businesses can protect themselves from the threat of ransomware. One of the best ways they can do that is with an effective, and safeguarded, cloud backup and recovery solution — one that bypasses the ransomware event and returns an uninfected copy of their data. However, for those who do not have such a solution, there are other ways to counter the impact.

Below are several tips on how SMBs can mitigate ransomware. But, first, let's assess the larger landscape.

Avast Business

Why ransomware attacks are on the rise

New digital payment options that provide criminals with a high degree of anonymity, the growing ecosystem of ransomware hackers, and the disappearance of the enterprise network perimeter (amid an increasingly distributed workforce) have all contributed to the rise in ransomware. Bitcoin and other crypto currencies have made it possible, safe, and easy for cyberthieves to demand and receive payments and transfer money anonymously.

Adding fuel to the ransomware fire is the fact that it's not just well-financed, sophisticated criminal enterprises that are exploiting ransomware. State-backed and individual hackers, looking to cash in on what they perceive as easy money, are also launching ransomware attacks.

The pandemic also has helped feed ransomware's rise. Cybercriminals are actually leveraging the pandemic to their advantage, ramping up their attacks on organizations and individual consumers for financial and political gain.

The large increase in work-from-anywhere has more workers using their own devices — such as laptops, desktops, and mobile devices. Home networks are not nearly as secure as enterprise networks; IT departments have a lot less control over the security and settings on remote workers' devices and the infrastructure protecting those endpoints. Unfortunately, the bad actors know this as well, as we've seen an almost 400% growth in ransomware over the last two years as a result.

According to Infrascale, **43%** of SMBs surveyed said that they have paid **$10,000** to **$50,000** to ransomware attackers. The price tags were even higher for some others — **13% of SMBs doled out more than $100,000.**

Ransomware comes with a hefty price

Businesses of all sizes and industry sectors are subject to ransomware attacks. A recent Infrascale survey conducted with more than 500 C-level SMB executives revealed that 46% have been victims of ransomware.

Downtime is an enormous pain point for businesses, which lose time and money for every hour, minute, or second they don't have access to their critical data and other digital assets. That helps explain why nearly three-fourths (73%) of SMBs that have faced ransomware attacks shelled out their hard-earned money to pay the ransoms.

Paying a ransom can significantly eat into an organization's finances. According to Infrascale, 43% of SMBs surveyed said that they have paid $10,000 to $50,000 to ransomware attackers. The price tags were even higher for some others — 13% of SMBs doled out more than $100,000.

Avast Business

According to Coveware, the average amount paid for a ransomware attack in the fourth quarter of 2019 was $84,116. This is up from an average of $6,733 just 12 months prior. The Coveware study indicates that this amount is heavily skewed by Ryuk and Sodinokibi ransomware, pushing the median payment in the fourth quarter of 2019 to $41,198. Demands from both of those actors can typically reach six or even seven figures, making a single successful attack extremely lucrative. In June 2019, for example, Ryuk attackers extorted more than $1 million in ransom from two Florida cities in just one week. A single Sodinokibi affiliate appeared to snag $287,000 in three days.

The amount of money being funneled back to these criminals to fund future attacks is deeply troubling, and the size and quantity of ransoms being paid is causing insurance providers to raise their cyber insurance rates as much as 25%.

In most cases, however, the cost of the ransom is trivial compared to the cost of system downtime, missed sales, and lost credibility. Thus, in the hopes of quickly restoring their systems and getting their data back, ransomware victims often pay off anonymous blackmailers.

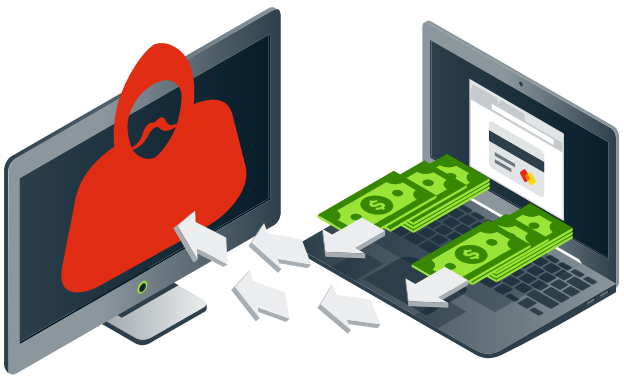
This is likely to be a continuing trend, as Infrascale research shows that more than a quarter (26%) of the SMBs that reported they have never paid a ransom said they would consider doing so. Of that group, 60% said they would pay a ransom to get their files back quickly, and 53% said they would pay a ransom to protect their company's public image around data protection and recovery efforts. Yet, 17% of the survey participants who paid ransoms to their ransomware attackers indicated they recovered only some of their organization's data back in return.

Ransomware prevention deserves attention

Ransomware is not a threat that has just arrived on the scene. This problem has been around since 1989. Yet many businesses still have not prepared themselves for ransomware attacks.

Almost a fifth (19%) of the Infrascale survey respondents said they don't believe their businesses are adequately prepared to address and prevent unexpected downtime. That's interesting, considering that more than a third (37%) have lost customers and 17% have lost revenue due to downtime.

Downtime can cost businesses a pretty penny. Roughly half (48%) of the survey group reported that their per-hour downtime cost was in the $20,000 to $50,000 range.



The adage that time is money would seem to apply here, although perhaps in a different way than you might think. Infrascale research indicates that almost a third (32%) of SMBs have limited time to research ransomware mitigation solutions. The same share said that they don't have the proper IT resources in place to address ransomware threats. The point is that businesses that don't take the time to adequately prepare for a ransomware attack are likely to lose a lot of money —

possibly by paying the ransom, but certainly due to operational challenges, a loss in business, and a hit to their reputations. Given these challenges, here's a useful tip: Consider hiring a third-party expert, such as a managed service provider (MSP) or security professional, to assist with the heavy lifting around ransomware protection, education, implementation, and setup.

Educate staff on the importance of up-to-date antivirus software and phishing threats

Organizations that want to protect themselves from ransomware should educate staff members about this threat and its points of entry into an organization. This means education on proper email handling and making sure that employees' antivirus software is up to date. This may seem obvious, but it's often something that SMBs don't check on until it's too late.

Picking up on a potential attack in advance is ideal to prevent it from happening. Your IT department should check your network frequently to see what types of files are being sent and work to understand what types of computers are connecting to your network.

If something looks questionable, it usually is. Criminals are becoming increasingly sophisticated at making their attacks look legitimate. And during this time, when people are in search of information and answers, the public's fake-filters are at an all-time low.

Take these steps if your organization is compromised by ransomware

Cybersecurity is important, but it isn't foolproof. Chances are good you'll fall victim to ransomware at some point. Perhaps you've already experienced such a scenario.

Here are some helpful tips your organization can use to respond to a ransomware attack:

1 Capture the ransomware message

When your business is hit with an attack, your first impulse may be to take action. But don't forget to take a screenshot or photograph of the ransomware message. This captured image will serve as evidence for your own use and in case you report the ransomware event to law enforcement officials.

2 Don't automatically pay the ransom

As Tufts University professor Josephine Wolff wrote in this piece for The New York Times, paying ransomware attackers only serves to reinforce to the hacker community that ransomware is a "business model" that pays. If there's another way out of the situation, without risking life and limb, consider taking it. Don't reward the bad guys.

Avast Business

3 Conduct a cost-benefit analysis

This will help you decide on the best path forward. MIT professor Larry Susskind noted that if ransomware freezes critical business operations, an organization may not be able to collect revenues, provide vital services such as water or electricity, or conclude patient procedures. Ransomware certainly creates financial risk, but it can also be a life-and-death proposition. That said, it makes sense to look before you leap.

4 Understand whether the issue is encrypting ransomware or screen-locking ransomware

If you're dealing with screen-locking ransomware, the situation may be more easily remedied. Try closing the affected application using a Mac Activity Monitor or Windows Task Manager, restarting the device in safe mode, and employing malware removal technology. If you're lucky, this may help you overcome the screen-locking variety of ransomware.

5 Move quickly to limit the threat

Ransomware can spread like wildfire, so you'll want to contain it as soon as possible. One way you can do that is by physically disconnecting affected devices. Disable Bluetooth and Wi-Fi connections on those devices and put them in airplane mode. Unplug Ethernet cables and connections to external devices like cameras, hard drives, and phones. Organizations can also contain ransomware via microsegmentation. nd phones. Organizations can also contain ransomware via microsegmentation. This approach relies on network monitoring to detect anomalies and leverages automation to isolate devices that exhibit behaviors indicating they may have been infected.

Limit ransomware pain and stay up-and-running with Avast Business Cloud Backup

The risk that ransomware presents to your business decreases significantly if you employ a comprehensive, cloud-based endpoint backup and recovery solution such as Avast Business Cloud Backup, which is invaluable in the event of a ransomware attack. Our solution backs up critical data such as accounting files, Exchange data files, and SQL databases. The Avast Business direct-to-cloud backup solution protects a wide range of devices and endpoints, regardless of their location, which is important in our increasingly remote world.

As we're all aware, confronting a crisis is never fun. But contending with ransomware in this already challenging time can be a lot less painful, and you can get through it faster and with much less disruption if you already have good backup and disaster recovery in place. Businesses that have backup and disaster recovery strategies and solutions ready can restore their data and resume normal operations much more quickly after a cyberattack.

Avast Business

About Avast Business

Avast delivers all-in-one cybersecurity solutions for today's modern workplace, providing total peace of mind. Avast provides integrated, 100% cloud-based endpoint and network security solutions for businesses and IT service providers. Backed by the largest, most globally dispersed threat detection network, the Avast Business security portfolio makes it easy and affordable to secure, manage, and monitor complex networks. Our easy-to-deploy cloud security solutions are built to offer maximum protection businesses can count on. For more information about our cloud-based cybersecurity solutions, visit **www.avast.com/business**.