
# THE BASICS OF RANSOMWARE ATTACKS AND HOW MIDDLE-MARKET COMPANIES CAN START TO BOLSTER THEIR NETWORKS

By **Holly Ridgeway** | Citizens Chief Security Officer

## Ransomware Attacks are a Growing Threat to Middle-Market Companies

High-profile attacks are now a weekly or even daily news event, reflecting how prevalent – and costly – these attacks have become for organizations. What's more, ransom values are steadily climbing as the attacks become more sophisticated. The average reported ransom was below $100,000 at the end of 2019, but spiked above $200,000 as of early 2021, according to incident response firm Coveware. Meanwhile, the total cost to businesses is even higher as they incur losses from halted operations, the steep expense of securing a network after an attack and business lost due to reputational damage.

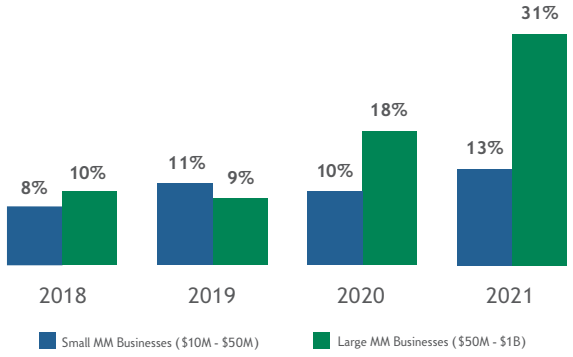
### The average ransom requested has grown exponentially since 2018


**Source:** Coveware, Inc.Q1 2021 Ransomware Report

Ransomware is a form of malware (malicious software) used by hackers to extort money from companies, government entities and other organizations. Typically, the malware enters an organization's network, encrypts data in the network to render it unusable, then holds the encrypted data for ransom. According to Coveware, about 75% of recent attacks included data exfiltration, which is when hackers threaten to publish or erase stolen data to bolster ransom negotiations.

Middle-market businesses are, unfortunately, a desirable target for ransomware. Their operations generate valuable data and depend on IT networks and they have the resources to pay more sizeable ransoms than small businesses. However, they may lack the robust security that much larger companies deploy. While middle-market firms of all sizes have reported increasing cyberattacks in recent years, the trend is hitting larger middle-market companies hardest. In the last year, 31% of firms with revenue of $50M to $1B reported a ransomware attack, compared to 13% of firms in the $10M to $50M market, according to a 2021 report from consulting firm RSM.

### The percent of middle-market businesses that experience a ransomware attack or demand is rising



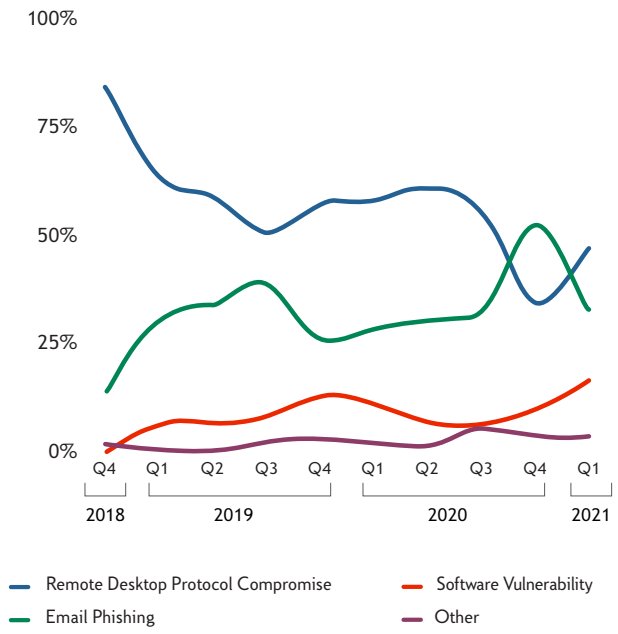

**Source:** RSM U.S. Middle-wMarket Business Index Cybersecurity Special Report, 2021

## Two Basic Types of Ransomware Attacks

Ransomware attacks come in two varieties. The first is sometimes referred to as "big game hunting." In this approach, hackers gain entry to a network and spend time quietly exploring and mapping it from within to identify the most sensitive or valuable data. This quiet mapping time, known as dwell time, can last for days or weeks. These attacks can be devastating in scope, shutting down operations completely – even disabling data backups. Accordingly, these attacks generate the highest ransoms. The Colonial Pipeline attack of 2021 was one of many such examples.

The second type of ransomware attack is more limited but can still be crippling for organizations. In these cases, hackers aim to seize or freeze data as soon as they enter a network, hoping to capture something sensitive in the process.

**Ransomware attack access points**




Source: Coveware, Inc. Q4 2020 Ransomware Report

## The Three Ways Malware Enters Networks

1. Enticing a network user to click on an email link is one of the simplest and most common ways that malware enters a network, according to Coveware. Email phishing has evolved from the early days of targeting naïve users with barely disguised fraudulent messages. Today, phishing often entails advanced social engineering, meaning that phishing messages come from domain addresses carefully crafted to look legitimate, and they often include deeply researched, personal information to trick recipients.

2. RDP compromise, or remote desktop protocol compromise, is another popular entry point. In this instance, hackers enter by guessing easy passwords or by using valid credentials that they purchased illicitly from a black market of credential-sellers – often for as little as $50, according to Coveware.

3. The third common entry point is a software vulnerability, such as an outdated version of software with known security gaps that has not yet been updated with available patches.

## The "Onion Layers" of Ransomware Prevention

Ransomware attacks are impossible to halt completely, but organizations have a chance to fend them off by instituting a defense strategy with multiple layers, like an onion. The key idea behind prevention is to make entry sufficiently difficult for hackers so that they will give up and move on to easier targets. Most of the defense layers are more about technological "hygiene" than they are about cutting-edge, high-cost technology.

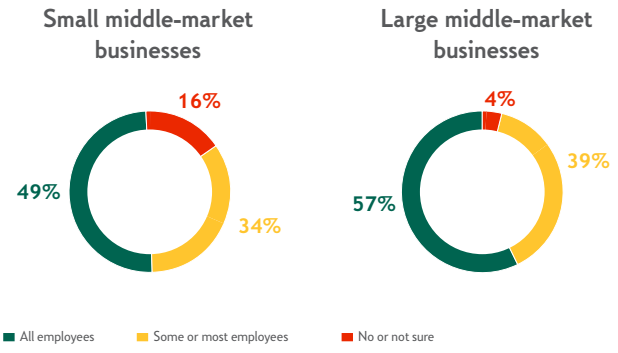
**Here are a few ways that middle-market companies can start to bolster their networks against ransomware:**

- **Conduct regular training sessions.** Educate employees at all levels of the organization about cybercrime and the increasing sophistication of phishing tactics. Unknowing network users are a vulnerability, but educated users become part of the defense team.

- **Be vigilant about passwords and other settings.** Easy-to-guess passwords continue to be one of the easiest ways for hackers to gain entry to networks. Encourage network users to use a password manager, which can ensure that they have strong and unique passwords for different systems. Password managers can also flag which passwords have been involved in a breach. Other password policies can be valuable, such as requiring strong passwords and frequent password changes.

- **Keep software and operating systems up to date.** Once a new version of software or an operating system is released, it's easy for hackers to identify the unpatched zones on outdated versions. Aim to update all software and operating systems as soon as new versions are published.
- **Use antivirus software.** There are several mainstream antivirus providers, and they all essentially approach malware the same way – by monitoring the behavior of networks and flagging abnormalities and by tracking network code for signs of known viruses. Because malware is constantly evolving, the real-time updates in popular antivirus programs are valuable.
- **Use multi-factor authentication (MFA) on internal and external logins.** MFA, which requires users to log in to software through two or more steps, is an effective way to block malware that guesses single-step passwords. It's important to use MFA not just on your own network software but also on cloud applications and online software that employees use for company purposes.
- **Restrict media and other outside websites and applications.** Knowing that most malware comes in when users voluntarily click links, it can help to restrict what outside sites and applications can be accessed by network users.
- **Restrict outbound user traffic to aid in detecting malware.** Configure networks so that outbound user web traffic can only go through a web proxy, allowing for detection of malware that managed to get installed. This approach can also block second-stage downloads for malware that is trying to bypass the proxy.

### Percent of middle-market employees receiving training on how to detect, identify and prevent attempts of unauthorized access




**Source:** RSM U.S. Middle-Market Business Index Cybersecurity Special Report, 2021

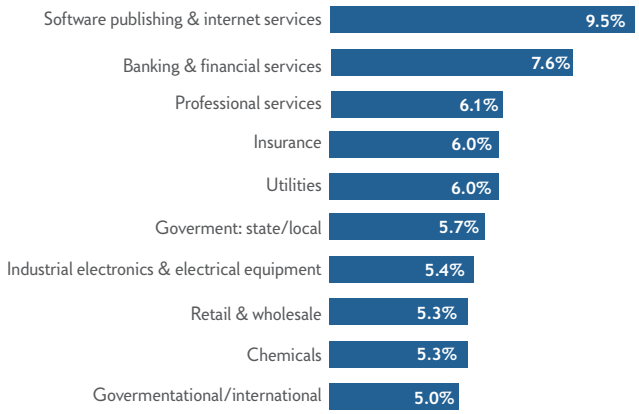
## Response Tactics to Minimize Damage or Loss

When a network is attacked, an organization's response will have a significant impact on the outcome. A swift and decisive response can limit the attack, while a slow or ineffective response could result in widespread business disruption, significant financial losses and costly reputational damage.

**Here are a few ways that organizations can prepare to respond:**

- **Draft an incident response playbook.** Plan out how your organization would respond to an attack. Identify who in the company will be involved and what individual responsibilities will be.
- **Conduct tabletop exercises.** Convene all the appointed responders to act out the scenario of responding to a cyberattack. Just like a classic fire drill, an attack-response rehearsal is a helpful way to ensure that each person fully understands his or her duties in case of a real emergency.
- **Establish and test robust backups of all data.** Data backups can be a significant investment. Organizations must balance the cost and time of creating backups with their operational needs. The key decisions are how frequently to backup networks, and where feasible, how to maintain an offline or "air-gapped" version that is not connected to the network. It's also critical to test backups periodically to confirm that they are functioning properly.
- **Hire (or contract) a dedicated head of cyber defense.** Companies are increasingly hiring an internal cyber defense person or team, according to Coveware. If your organization is not large enough to warrant a full-time position, establish a contract with a reputable cyber defense firm.

### Percent of overall IT spending reserved for security by industry




**Source:** Cybersecurity Dive and Gartner

Citizens™

## Vigilance is Mandatory – But Manageable

The threat of ransomware is a critical issue for middle-market companies today. Hackers have identified mid-sized organizations as an especially profitable target. With more valuable data and more ransom-paying ability than small businesses, but having less network protection than the largest companies, such organizations can be ideal victims. Meanwhile, the consequences of committing a cybercrime remain limited. Most middle-market executives expect cyberattacks to continue escalating in the near term, according to RSM.

Fortunately, it is possible and cost-effective to establish prevention and response practices that guard against attacks and limit the damage when they do occur. As with any defense, strategy matters. Fortunately, most of the strategic tools that are available to organizations, like password management and employee training, are more an issue of good "hygiene" than of cutting-edge, high-cost technology.

### Key Takeaways:

1. Middle-market companies are a prime target for ransomware attacks, especially larger firms.
2. To defend against attacks, companies need to establish good preventative protocols, including employee training, strong password policies and timely software updates, among other practices.
3. A swift and effective response can curtail damage when attacks do occur, and companies should prepare and rehearse a response.
4. While high-cost security investments can be useful, good practices and tech "hygiene" go a long way toward keeping company networks safe.

**Holly Ridgeway** is the Chief Security Officer at Citizens. She has over 20 years of experience building enterprise security programs in both the commercial sector and the federal government. Learn more at: citizensbank.com/fraud-protection

**Find more articles, industry insights and interactive experiences on the latest corporate finance, risk, cash management and M&A trends at: citizensbank.com/insights**