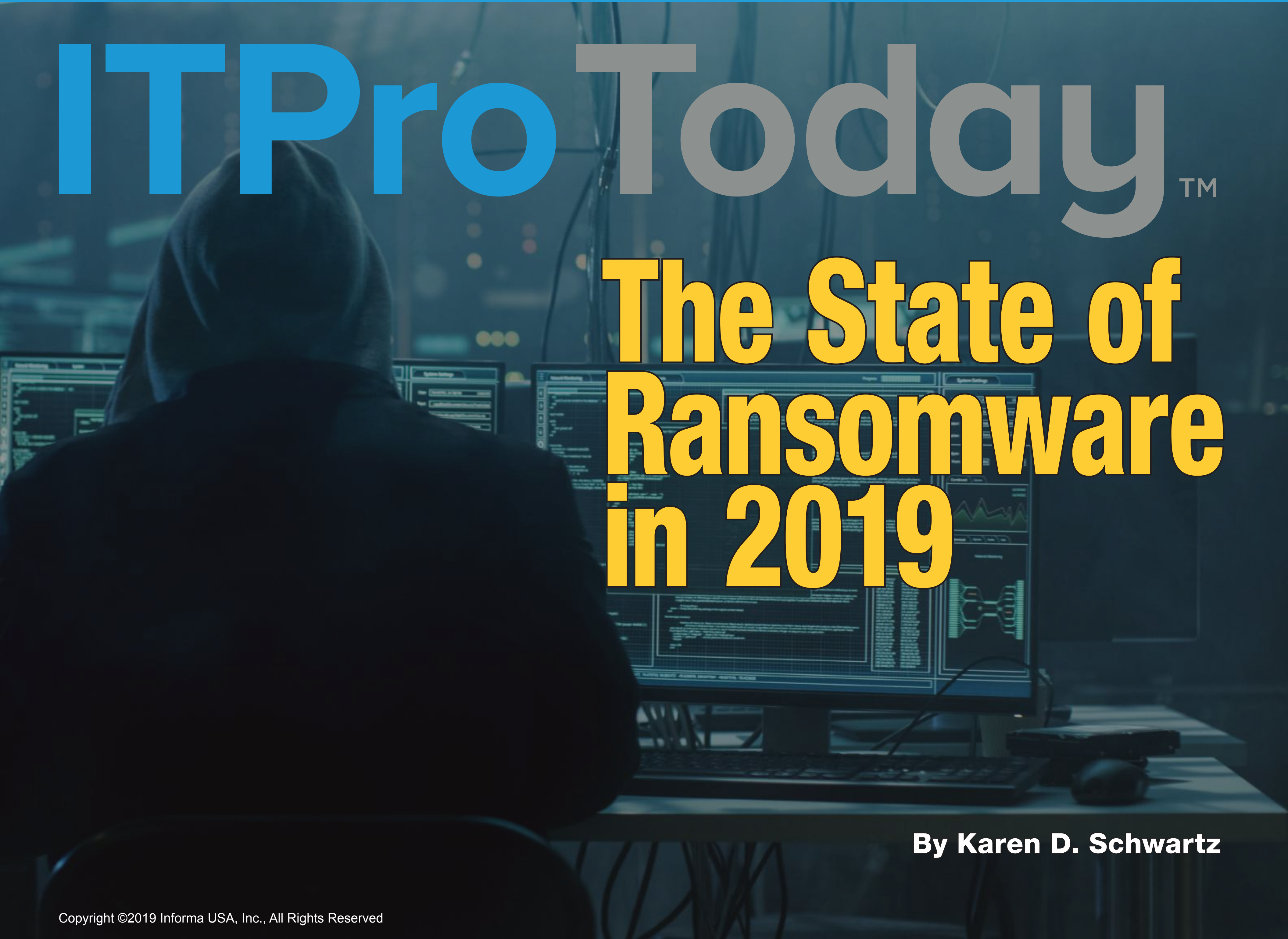
ITProtoday.com presents

Vol. 2, Issue 7 June 2019

ITProToday™



The State of Ransomware in 2019

By Karen D. Schwartz

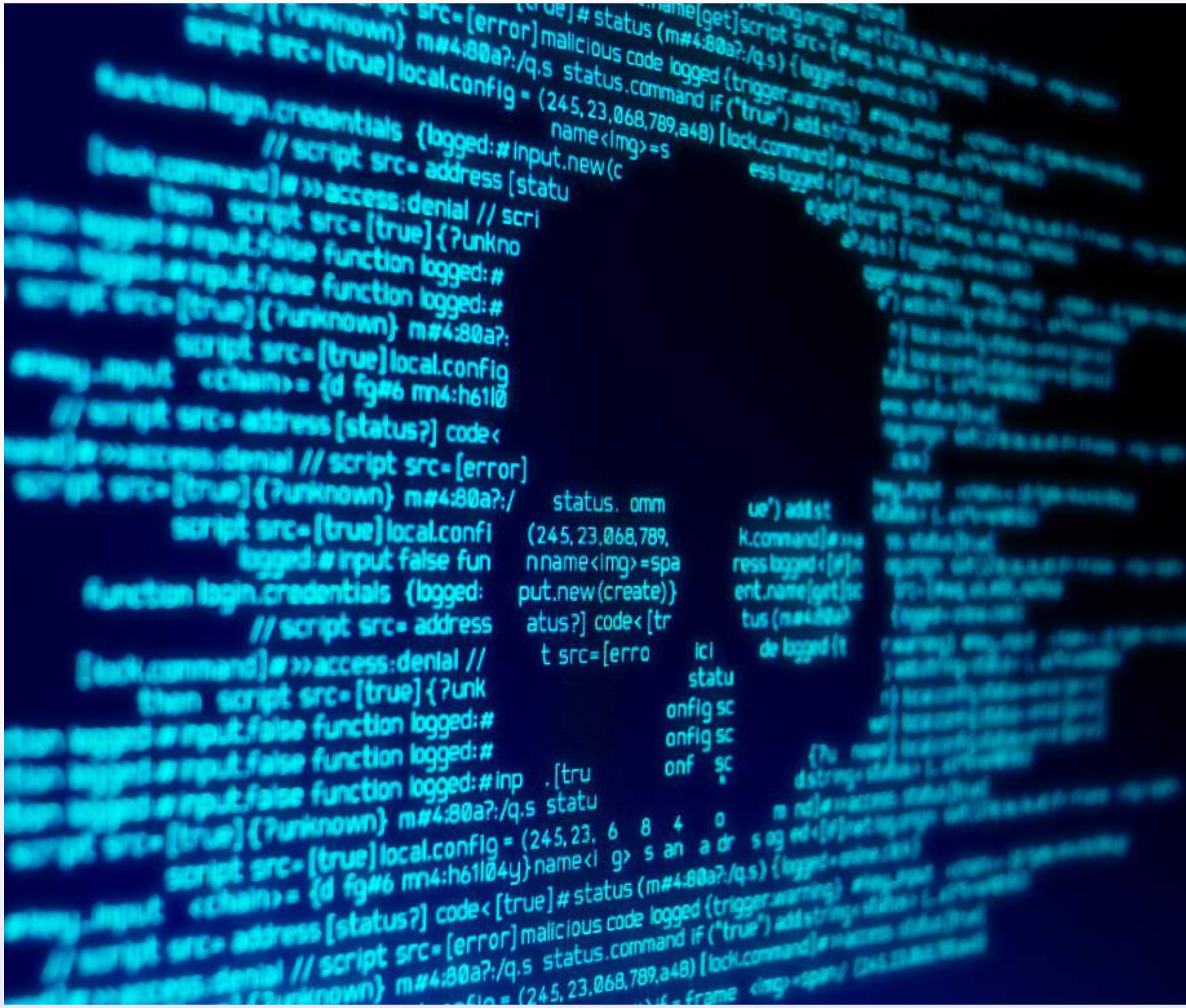
TABLE OF CONTENTS

The State of Ransomware in 2019

TeslaCrypt. SamSam. Ryuk. Leakerlocker. Reyptson. Cerber. While these may sound like the names of sci-fi characters or movie villains, they are actually types of ransomware. There are hundreds of others, and you've probably heard of some of the more famous varieties, like WannaCry and NotPetya. Some are more far-reaching than others, but it's safe to say that all ransomware is pervasive, insidious, and potentially ruinous to organizations.

So what is ransomware, exactly? At its most basic, it is any method that exploits digital weaknesses for financial reward. Typically, ransomware attacks a workstation or mobile device via email, an application, a macro, an operating system, a website, a download or a network channel. Once a user clicks on a link or opens an attachment, that action begins the process of encrypting files or limiting the functions of the device in some way. If the user pays the ransom, the thief promises to send the encryption key or release hold of files. But then again, we're talking about thieves. They may or may not keep their promises, despite payment. Today, cybercriminals demand to be paid in Bitcoin and Monero, which are virtually untraceable cyber-currencies.

And it's a huge problem. In 2018, the [FBI's Internet Crime Complaint Center](#) (IC3) received nearly 1,500 complaints identified as ransomware with adjusted losses of over $3.6 million.



For the enterprise, ransomware is a two-pronged challenge: Not only are enterprise assets under attack by bad actors, enterprise end users present ample opportunities for breaching security. Thanks to an uptick in social engineering attacks, i.e. emails or phone calls that can trick users into offering sensitive information or downloading a malicious software package, user behavior presents a significant vulnerability to the enterprise when it comes to ransomware.

> “In those early days, ransomware attacks were very unsophisticated, but so were users, who had no reason to believe that these demands wouldn’t be backed up with action.”

How Did We Get Here?

Ransomware has been around, in some form or another, since the late 1980’s. The first recorded instance of ransomware was the 1989 AIDS Trojan. During this exploit, a biologist sent 20,000 infected diskettes labeled “AIDS Information” to attendees of the World Health Organization’s international AIDS conference. When unsuspecting attendees inserted the diskettes into their computers, they were informed that their files had been encrypted and would only be released after they mailed $189 to a Panamanian P.O. box.

In those early days, ransomware attacks were very unsophisticated, but so were users, who had no reason to believe that these demands wouldn’t be backed up with action. They might be presented with a popup message and law enforcement logo on their screen warning them that if they didn’t pay the fine, they would be arrested.

Over the next several years, ransomware became much more sophisticated and effective, using RSA encryption and other methods. By July of 2011, [experts had identified 60,000 incidents of ransomware](). The following year, ransomware became much easier to implement with Citadel, a toolkit for distributing malware and managing botnets.

During the next decade, the number and types of ransomware attacks skyrocketed. There were: trojans targeting mobile devices; ransomware hidden in infected Word files; ransomware that made hard disks inaccessible; ransomware that started deleting files if the target didn’t pay the ransom; ransomware that infected machines through drive-by downloads from compromised websites; ransomware that stole and hosted personal information gathered from social networks; ransomware that used malicious macros to infect its victims; and, for enterprising cyberthieves, ransomware-as-a-service, which took the work out of the entire process. There was even ransomware that could avoid detection by the kinds of cybersecurity tools that used machine learning to identify threats, and ransomware that could lock cloud-based backups during persistent synchronization.

Today, ransomware is pervasive. Criminal organizations are well-funded, and have the technical resources to create new and increasingly better attack methods. And it's lucrative, with an average payout of $2,500, but reaching as high as $55,000 per incident.

"It's also the anonymous nature of digital currencies that feed cyber criminals' demand for payments with a low potential of being caught," says Troy Kitch, senior director of enterprise solutions at Malwarebytes. "A case in point: we saw a decline in ransomware at the beginning of 2018 when attacks shifted to cryptojacking as the value of Bitcoins spiked. After the value of Bitcoins declined, we saw the switch back to ransomware attacks."

What's more, cybercriminals are focusing more on businesses now. The latest Malwarebytes State of Malware Report for 2019 shows an explosion of nearly 200 percent more ransomware found on business endpoints than the previous quarter.

Ransomware in 2019

Today, most ransomware falls into three categories: scareware, screen lockers, and encrypting ransomware. All varieties aim for the same payday, but they get there using different methods.

Scareware is designed to do just that—scare the user. It may claim that it has discovered a virus or malware on their computer, but paying a fee will release a fix. It may send an email to users threatening to expose a secret to everyone on their contact list if payment isn't received in a certain amount of time. It may threaten that it has taken control of the user's bank account. Most likely, if you do nothing, you'll probably be safe. But these are criminals, so you can't be sure.

Examples of scareware include "rogue scanner" software or "fraudware" with names like SpySheriff, XP Antivirus 2009, and AdwarePunisher. But even legitimate companies can try to get away with it. One of the more recent high-profile scareware events occurred in March, when Office Depot and its tech support vendor urged customers to download a free "PC Health Check Program". Once downloaded, the program essentially frightened people into buying diagnostic and repair services they didn't need. Office Depot ended up paying the FTC $35 million in fines. They affect mobile devices as well.

Screen lockers freeze users out of their PC, laptop or mobile device entirely. Upon starting up the device, a full-size window will appear, often accompanied by an official-looking FBI or U.S. Department of Justice seal stating illegal activity has been detected on your computer and you

> "It's the anonymous nature of digital currencies that feed cyber criminals' demand for payments with a low potential of being caught."

must pay a fine. However, a U.S. government agency would never freeze them out or demand payment for illegal activity. Instead if they suspected you of piracy, or other cybercrimes, they would go through the appropriate legal channels. Users may not realize this, or they may be emotionally swayed by the situation.

Screen lockers started with WinLock back in 2007 and Reveton in 2012, followed by numerous types, such as Princess Locker, Virlocker, and many more. There are other variants that, instead of locking you out of your entire system, lock you out of part of it. One example is browser lockers, or "browlock". With this scam, users are directed to click on a link by pretending to offer a desired product or service. When they click on the link, the malware will either close the open tab or window, block access to the desktop of the system, or prevent the user from navigating to another site. There are also plenty of screen lockers that target mobile devices, such as LockerPin, which can reset the PIN number to lock users out of their devices unless they pay the ransom.

While scareware, screen lockers and their variants can be nasty infections, encrypting ransomware, also called crypto-ransomware or crypto malware, is considered far worse. In this scenario, a user's files, folders or drives are encrypted before they even know what has happened, and they are directed to pay the ransom before file are decrypted.

"This is the most destructive type of attack, because there is a real chance that they won't ever give you the decryption key," said Jon Clay, director of global threat communications for Trend Micro. "They just want to take your systems offline. It's very effective, especially if they don't deliver the decryption keys, because you'll have to go through a full system rebuilt to get them back."

Some of the most famous recent ransomware attacks have been encrypting ransomware, including CryptoLocker in 2013, and both WannaCry and Petya in 2017. In the case of Cryptolocker, Windows users first know they have been infected via a warning screen, which informs them that their data will be deleted if they don't pay the ransom to release the decryption key within 72 hours. It can infect any or all files

Should you pay the ransom?

The question of whether or not to pay the ransom is actually a bit tricky, despite the fact that the FBI recommends against it. In fact, one IBM study found that more than 70 percent actually do pay the ransom.

If you have put the processes in place to recover effectively and quickly from a ransomware attack, you probably shouldn't pay the ransom, says Trend Micro's Jon Clay. On the other hand, if your company's "crown jewels" are being held ransom, it may make sense to pay the ransom, just this once, which can buy you time to address the situation. It may also make sense to pay the ransom, some believe, if the cost of fighting it is more than the amount of the ransom. For example, if the ransom is $500 but it would take your entire IT team three days to figure out how to release the files, it may be tempting to pay up.

There really is no right answer; even if you pay the ransom, you're dealing with criminals, who may or may not deliver on their promises.

on hard drives, USB memory sticks shared network drives, or files and folders stored in the cloud.

WannaCry took the fear factor up a notch. While its request for a $300 ransom seemed fairly routine, its real power was in its ability to replicate through a worm virus. Petya encrypts select files and blocks the boot sector of the system after users click on an email masquerading as a job applicant's resume. The ransomware then reboots the computer, showing a Windows CHKDSK screen, while it is installing a boot loader and encrypting the master file table. Users are informed that their hard drives will be decrypted once a payment is made in Bitcoin.

Hackers Are Getting Smarter

As if the situation isn't already bad enough, hackers are getting smarter, developing more customized and targeted approaches to separating users and companies from their money.

"Where they sprayed out spam messages to many people or organizations and hoped one hit and caused an infection, it's much more targeted today," Clay said. "We're definitely seeing them targeting organizations that they feel may not have taken the right precautions. Think small businesses, municipalities, education—types of organizations that have had challenges in building more secure networks."

Smart hackers also are increasingly targeting business systems, where they can affect daily operations, along with profit and revenue streams. According to Cybersecurity Ventures, businesses will fall victim to a ransomware attack every 11 seconds by 2021, up from every 14 seconds in 2019, and every 40 seconds in 2016.

They are also getting smarter about the way they devise and implement their ransomware. For example, they take their time in encrypting files, which helps avoid detection by traditional tools. They are getting better at writing code and using multiple processes to perform the encryption, both of which stymies anti-ransomware efforts. They are focusing more on encrypting hard drive instead of individual files. And because so many users now are more wary about clicking on email links, hackers are embedding links in other types of files, such as Word documents, photos or PDFs.

Ransomware perpetrators also are getting braver. A recent report from Coveware found that ransom demands are getting higher, rising 89 percent from last year to this year. It also found that attackers are specifically targeting high-value systems using more manual methods, which can result in greater damage to businesses.

Steps to Take to Protect Your Company

If you're discouraged, you're in good company. But there are ways you can protect your company from getting infected in the first place.

First, address underlying vulnerabilities that may make it easier for ransomware to get through. This is especially true for operating systems and major applications. Alex Grohmann, an independent consultant at Sicher Consulting and a Fellow at the Information Systems Security Association (ISSA), gives the example of Windows, which retired Windows XP in 2014 and plans to retire support for Windows 7, as well as mainstream support for Windows 10 and Office 2016, next year.

"If Microsoft finds a vulnerability in an operating system or application it is still supporting, it generates a patch and that takes care of it. But after they stop updating, vulnerabilities become well known and can be exploited more easily," he explained.

In fact, that's one of the reasons WannaCry was so successful. The ransomware hit a lot of systems running Windows XP, which is no longer supported.

Also, make sure you are backing up your files regularly. If you are attacked, one of your best resources will be your recently backed up files. In other words, if you can't get your recent files decrypted, you can at least rely on the next best thing.

Next, survey the security tools you have in place to make sure you are covering all bases. This includes robust email messaging security for both email entering the organization and internal email, as well as web application firewalls, endpoint protection and vulnerability scanning, patch management.

After taking inventory of existing tools and implementing policies, you'll be able to better see potential gaps. That's where it makes sense to add tools as necessary. Today's most effective tools tend to take advantage of artificial intelligence, machine learning and behavior monitoring. Sandboxing is another effective method; by sandboxing suspicious files as they enter the environment, they can't infect other company resources.

"The best approach to combat ransomware is to implement a holistic security strategy that includes an incident response plan and security layers of defense, because no one security control can mitigate all attacks," Kitch said. "It's important to deploy security controls that encrypt data at rest and in transit, manage endpoint detection and response, maintain the best practices of separation of duties and least privilege, and keep current on the latest software patches and updates. It's better to be proactive against ransomware and prevent it from ever being executed in the first place."

Policies also are important; enforce application control, apply network segmentation to contain infections that may occur, and assign data access and application privileges based on the "least privilege" methodology, which only allows users to access the resources they need to do their jobs.

There are also a host of ransomware tools that can help both test against ransomware scenarios and upload ransomware for identification. These include ID Ransomware, HitmanPro, KnowBe4's Ransomware Simulator and Malwarebytes's Anti-Ransomware.

In addition, consider adopting the NIST Framework for Improving Cybersecurity Infrastructure, which explains in detail how to implement access control, awareness and training, data security, information protection processes and procedures, maintenance and protective technology.

Finally, don't underestimate the effect of good user education.

"Teach users to follow procedures, not to click on suspicious links, not to download things from unknown sources, not to save things to their desktops, and to always back files up to the corporate servers," Grohmann said. "Education is better than any technology or process you put in place. It helps ensure that you have an army of people working with you."

Help! We're Infected!

Despite doing everything right, you can still get infected. For example, Sophos found more than 77 percent of companies infected with ransomware were running up-to-date endpoint protection.

If your organization is infected, take these steps:

- Notify law enforcement.
- Implement your incident response plan.
- Shut down all systems, both infected and uninfected. Wipe all infected machines and reinstall the operating system and applications.
- Recover uncompromised data from your latest backup.

- Decrypt data, if possible. There are plenty of decryptors available, and one might just work. Try Trend Micro's Ransomware File Decryptor and Screen Unlocker Tool, Kaspersky's NoRansom or the No More Ransom online portal, which provides links to dozens of free decryption tools.
- Consider a full system restore.
- Consult NIST's Cybersecurity Practice Guide "Data Integrity: Recovering from Ransomware and Other Destructive Events".
- Learn from your mistakes and vulnerabilities for next time.

The Future of Ransomware

According to a 2017 report from Cybersecurity Ventures, ransomware will cost victims $11.5 million globally and will reach $20 billion by 2021. Clearly, extortion is here to stay. It will also continue to evolve into areas like industrial Internet of Things (IoT). Hackers will continue to get smarter, using machine learning to develop automated and evolving viruses. This can help ransomware evade detection for longer periods of time as it spreads throughout the network, infecting new endpoints. Cybercriminals are also finding new ways to move laterally across networks, and they are increasingly targeting mobile devices.

In fact, in the first quarter of 2018 alone, Kaspersky Labs detected more than 8,000 mobile banking ransomware Trojan installations. And they are no longer focused solely on Android devices. Today, they have spread to Mac and iPhone users.

And don't give up.

"It may seem hopeless, but in fact, there is progress being made," Grohmann said. "There are better tools that are closing the gap, and we're getting better with countermeasures. Just keep in mind that it's a constant battle."

DRaaS as a Ransomware Defense

When it comes to restoring files to a normal state, time is of the essence. That's why there is a fair amount of support for Disaster Recovery as a Service (DRaaS) as an effective solution for recovery from ransomware.

By creating a total redundancy, especially among critical applications and infrastructure, a DRaaS solution may be just the key to a smoother recovery from ransomware, said Jennifer Curry, vice president of global cloud services at INAP.

"It's an insurance policy for your mission-critical production systems and applications. Even if your organization is hit by ransomware, a sound disaster recovery plan can have you up and running before the attack can severely affect operations," she said.

A good DRaaS solution will allow organizations to restore their system much faster (with faster recovery time objectives, or RTOs), than backups or complete rebuilds, she said.

"Once an environment is infected with ransomware, DRaaS allows you to efficiently bring a clean image of the production virtual machine, server, or cluster back online within minutes," she explained. "Even if you are not sure of the precise time the attack took place, DRaaS software will allow you to quickly boot different images until you find the most recent clean image. Once the system is restored, it is crucial to diagnose the source of the attack and review account access controls if necessary.