The growing ransomware threat to government agencies

Article

A look at the recent trends

Tax payment systems frozen. Motor vehicle offices shut down. Police dashcam videos deleted.

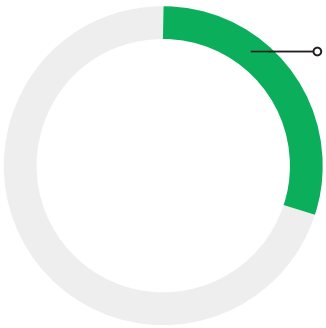
These are just some of the headaches suffered by government agencies as cybercriminals hit the public sector with an increasing number of ransomware attacks.

Ransomware—in which cyberattackers encrypt or lock down a victim's files or networks and demand a ransom to restore access—can hit anyone, from private individuals to multinational corporations. But in the last two years, attackers have struck government agencies especially hard.

In 2018, the cities of Atlanta and Baltimore were attacked, and Baltimore was attacked again in 2019. Both cities chose to spend millions on recovery costs rather than pay the attackers' ransom demands. Baltimore estimated its costs would exceed $18 million.

While attacks on big cities generate the most attention, small municipalities are not immune. In 2019, ransomware attackers hit 22 small cities in Texas—including Keene, population 6,100.

The federal government, with all its resources, is also vulnerable. In one survey, about 30% of federal agency respondents and 32% of state agency respondents reported that their agency had experienced a ransomware attack.[1]



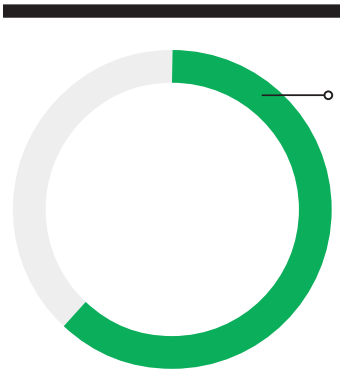
Thirty percent of federal agency respondents said their agency had experienced a ransomware attack.[1]

How big is the problem?

Ransomware was the most common form of malware for government agencies last year, accounting for 62% of malware incidents, according to the *2020 Verizon Data Breach Investigations Report* (DBIR).[2]

More than 100 U.S. state and local governments, including school districts and other educational institutions, were victimized by ransomware in 2019, according to cybersecurity firm Recorded Future.[3] That's counting an attack on 22 towns in Texas as a single event. That 100-plus total is nearly double the 55 attacks Recorded Future counted in 2018.[4]

And those numbers are probably an undercount. Ransomware is notoriously underreported in all sectors. "The estimate is less than 10% is getting reported," said Matthew O'Neill, Assistant Special Agent in Charge with the U.S. Secret Service, which investigates financial and electronic crimes.[5] Many organizations don't report the crime, preferring to deal with it privately.



Ransomware accounted for 62% of malware incidents among government agencies last year.

—2020 DBIR[2]

verizon

Why target governments?

Anyone can potentially become a victim of ransomware, and some organizations—say, large multinational companies—have significantly deeper pockets than a small town in Texas. So why do cybercriminals take on governments?

One reason is that they have found it's easier. Many government agencies don't have the sophisticated defenses and resources of a large enterprise. They often have older IT systems that are more vulnerable to intrusion, and they possess limited funding for upgrades and training.

That's because far more visible demands tend to compete for limited government resources. Constituents may call their city council to demand better schools, lower taxes or fewer potholes, but they aren't likely to demand better cybersecurity unless they see it affecting their daily lives.

Difficulty hiring qualified IT security professionals can further complicate attempts to combat cybercrime. The United States currently has a shortage of 300,000 cybersecurity practitioners.[6] Government agencies have to compete for those workers against businesses that are able to offer higher salaries.

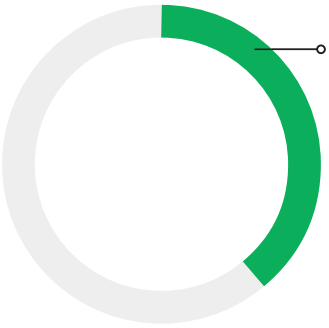
Additionally, the number of employees using computers, especially mobile devices, has grown. Inadequately trained employees can be vulnerable to phishing scams directed at email accounts—and those phishing scams can give cyberattackers the access they need to launch ransomware attacks.

Government agencies also have lots of valuable data—for instance, personally identifiable information on taxpayers, residents and employees that attackers might threaten to reveal if their demands aren't met.

"That's a prime target for any cyberattacker," O'Neill said.

When they are attacked, governments have a pressing need to remain open—emergency operations are often affected. And they face political pressure to respond quickly to fix the problem. That leaves them susceptible to ransom demands.

"They just want to be up and running," O'Neill noted.



Thirty-nine percent of public sector organizations have suffered a compromise involving a mobile device.

—2020 Mobile Security Index

300K

Estimated shortage of cybersecurity practitioners in the United States[6]

Who is behind the attacks?

Ransomware attackers can be lone wolves, but most of those who are targeting governments or other large organizations are part of organized crime groups, O'Neill said.

By studying tactics, techniques and procedures used in an attack, investigators can often get a general idea of the type of group behind it. That doesn't mean they can stop them, though.

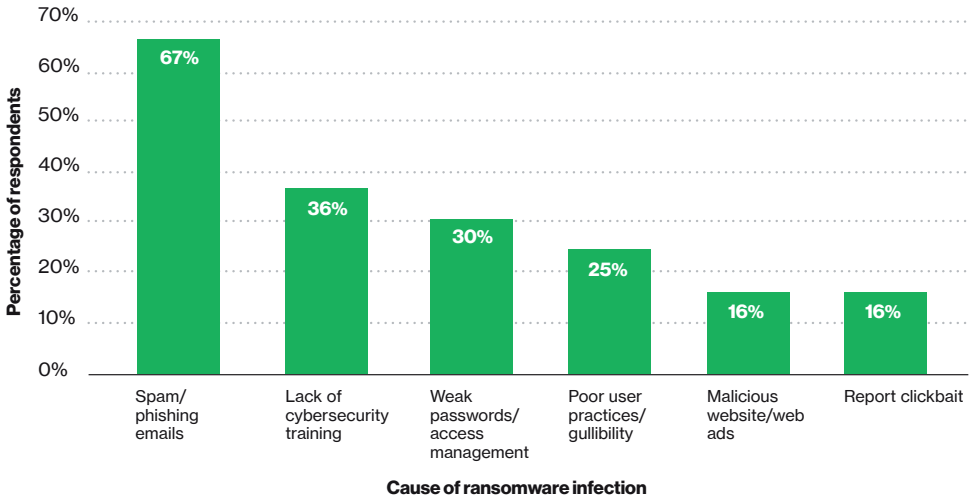
Because attackers typically demand payment in hard-to-trace cryptocurrency, such as Bitcoin, it's difficult to establish attribution. Threat actors often live in countries beyond the reach of U.S. law enforcement, and they are continually evolving their techniques to try to stay one step ahead of law enforcement and cybersecurity experts.

How do they break in?

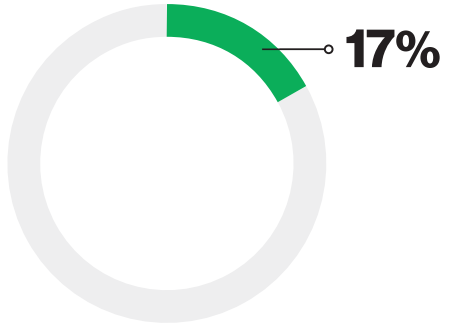
The main way cyberattackers get into networks is through phishing—using email to trick an employee into clicking on an attachment or link—which allows malware to be downloaded onto the network. Malicious PDFs can also be a source of malware.

Another avenue is Remote Desktop Protocol servers, which cyberattackers can break into through a brute-force attack or by buying credentials on the dark web. Attackers also take advantage of unpatched vulnerabilities in widely used applications such as Adobe® Flash,® Acrobat Reader® or JavaScript.®

Most common delivery methods and cybersecurity vulnerabilities causing ransomware infections according to MSPs worldwide as of 2019



Source: *Datto's Global State of the Channel Ransomware Report 2019*, page 9.



In publicly reported attacks in recent years on state and local governments, only about 17% paid the ransom.[8]

To pay or not to pay

When governments are hit by ransomware, they must decide whether to pay the ransom or not. Paying can cost tens of thousands of dollars or more. But if backups or files on local systems are not available, not paying typically equates to doing without the affected data.

Law enforcement professionals generally urge victims not to pay because that rewards criminals and increases the likelihood of future attacks.

Because reporting on ransomware is so spotty, it's not clear how frequently ransom is paid. Research by Recorded Future found that in publicly reported attacks in recent years on state and local governments, only about 17% paid the ransom.[8]

Some victims do opt to pay, though, because the costs of recovery without a decryption key can greatly exceed the cost of the ransom. Also, government agencies want to get back to business quickly. Many have purchased cybersecurity insurance, which helps cushion the costs.

The percentage of organizations worldwide purchasing cybersecurity insurance grew from 35% in 2011 to 75% in 2018.[9]

But do cyberattackers hold up their end of the bargain if you pay ransom? Surprisingly, they often do.

Cyberattackers typically run their organization as a business. “It’s almost like the bad actors want to provide this customer service of decrypting the data,” O’Neill said. “They don’t want the reputation of having people pay the ransom and not getting their data back.”

Still, paying ransom doesn’t necessarily take care of the problem.

Cyberattackers don’t unencrypt the data 100% of the time, and when they do, flaws in the encryption process can mean some data is lost.

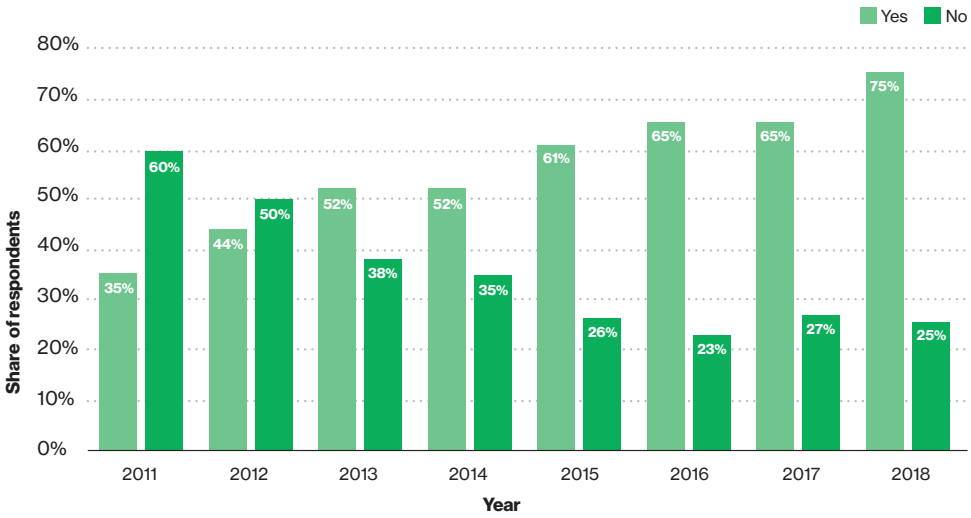
Even if decryption is successful, government agencies will have more work to do. They will need to rebuild servers, update computers and devices, and make certain the bad actors haven’t left a “back door” that allows attackers to make a repeat visit. And they should assume the criminals made copies of their data.

“These cyberattackers ... could have exfiltrated the data they’ve encrypted. So the decryption of a victim’s system doesn’t necessarily mitigate a possible data breach or the future monetization of the stolen data,” said O’Neill.

In fact, cyberattackers sometimes try to force the hand of victims who refuse to pay by threatening to publish their stolen data—which means that all sorts of sensitive data about citizens and employees could wind up on the dark web.

Key insight: Decryption doesn’t mean an agency’s problems are over. Cybercriminals sometimes make copies of the agency’s data or leave a “back door” open so they can reenter.

Does your organization purchase cyber liability insurance?



Source: *Information Security and Cyber Risk Management,* page 32.

What is ransomware?

Ransomware is a type of malware that prevents users from accessing their computers or files stored on their computers. Cyberattackers demand that their victims pay a ransom before they'll provide access.

Ransomware generally falls into three categories:

- **Crypto ransomware:** Encrypts files on a computer so users can't access them
- **Locker ransomware:** Doesn't encrypt files but locks users out of their devices
- **Wiper:** Wipes the hard drive of infected computers, so that the files aren't recoverable even if a ransom is paid

Cyberattackers' choice of weapons is continually evolving as criminals try to outsmart cybersecurity experts. A sampling of methods includes:

- **CryptoLocker:** First seen in 2007 and spread through email attachments, this ransomware is thought to have affected around 500,000 computers
- **WannaCry:** Exploited a vulnerability in Windows,® affecting users in 150 countries in 2017 and causing an estimated $4 billion in financial losses worldwide
- **SamSam:** Developed and released in late 2015, it has been used against healthcare organizations, governments, schools and private businesses
- **Ryuk:** Used in a number of the attacks on state and local governments and school districts in 2019, as well as large enterprises, it disables the Windows System Restore option and encrypts network drives
- **Robinhood (or Robbinhood):** Used in several recent high-profile attacks on city governments, including Baltimore, Maryland, and Greenville, South Carolina

A history of ransomware

- **1989:** The first "ransomware" attack occurs when a biologist sends diskettes supposedly containing information about AIDS to attendees at a World Health Organization AIDS conference; the diskettes in fact contain a Trojan that encrypts file names on the recipients' computers
- **2006:** The Archiveus Trojan, which encrypts the files of the My Documents directory, is launched; victims must make purchases from certain websites to regain access
- **2008:** Bitcoin gives cyberattackers a powerful new tool, as they can demand ransom using hard-to-trace digital currency
- **2012:** A Trojan called Reveton is introduced, eventually hitting half a million computers
- **2013:** The first known ransomware attack against a local government agency occurs when the Swansea Police Department in Massachusetts is hit with CryptoLocker, encrypting files on network shares and effectively preventing the police from accessing data within those files
- **2017:** WannaCry ransomware hits over 200,000 networks in 150 countries, including the National Health Service in the United Kingdom; it encrypts systems and demands Bitcoin currency payment
- **2019**: At least 100 U.S. state and local governments, including school districts or other educational institutions, are victimized by ransomware

What's next

To learn more about how to protect your organization, read our report on countermeasures that government agencies can take to help keep their networks secure.

Download the report on countermeasures >

What can government agencies do?

To cope with this new challenge, government leaders need to arm themselves with the best possible information about how to protect their data and avoid spending taxpayer money on ransoms or recovery efforts.

verizon✓

1 https://www.fedscoop.com/ransomware-threats-gov-agency-preparedness-to-protect-data/

2 *2020 Verizon Data Breach Investigations Report.*

3 Liska, Allan, "State and Local Government Ransomware Attacks Surpass 100 for 2019," Recorded Future, December 20, 2019. https://www.recordedfuture.com/state-local-government-ransomware-attacks-2019/

4 https://www.recordedfuture.com/state-local-government-ransomware-attacks-update/

5 Teleconference interview with Verizon and MRM, March 10, 2020.

6 https://www.dhs.gov/news/2019/05/02/white-house-cybersecurity-workforce-executive-order-bolsters-us-frontline-defenses

7 *Datto's Global State of the Channel Ransomware Report 2019*, Datto, 2019.

8 Liska, Allan, "Early Findings: Review of State and Local Government Ransomware Attacks," Recorded Future, May 10, 2019. https://www.recordedfuture.com/state-local-government-ransomware-attacks/

9 *Information Security and Cyber Risk Management*, Zurich North America and Advisen Ltd., October 2018.