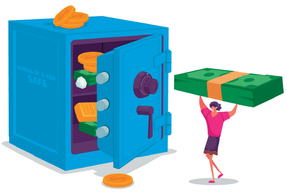
CYBERSECURITY AND GOVERNMENT

15 THINGS TO KNOW

The U.S. had the highest number of cyberattacks (156) between May 2006 and June 2020.[1]



The U.S. government allocated approximately $18.78 billion for cybersecurity spending in 2021.[2]

Ransomware is the main way municipal assets are attacked.[3]

$835K

The average ransom amount demanded by cybercriminals from 2013-2020 was $835,758.[4]

$500K

Average ransom demands rose from $30,000 to nearly $500,000[3]

53.2% of attacks in state government are targeted towards cities and local schools across the nation.[5]

58.5%

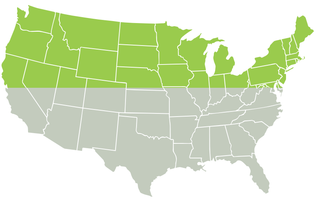
Between 2018 and 2019, known attacks on local governments rose 58.5%.[6]

48% of elected councilors and/or commissioners are only slightly aware or don't know the need for cybersecurity measures.[6]

The average cybersecurity breach costs states between $665,000 and $40.53 million.[7]

50%

Since 2017, attacks on state and local government are up 50%.[3]



60% of states either have "voluntary" or no cybersecurity training programs at all.[4]

CITY & TOWN HACKS

Atlanta suffered a ransomware attack that took many city services offline for nearly a week, forcing police to written case notes, hampering the court system, and preventing residents from paying water bills online. It took $17 million to recover.

In 2018, **Baltimore's** 311 and 911 dispatch systems were taken offline for more than 17 hours, forcing dispatchers to log and process requests manually. A year later, a ransomware attack cost the city more than $18 million in damages and remediation.

A 2020 ransomware attack on **New Orleans'** government cost the city upwards of $7 million.

Paying ransom does not guarantee you get your data back and it spurs ransomware because hackers know it works.

Smaller cities are targets, too. Just ask Frankfort, KY, Ellensburg, WA, Chicopee, MA, and these five other victims:

Last May, **Florence, AL** fell victim to an attack that cost it nearly $300,000 and compromised the personal information of city employees and customers.

The city of **Paducah, KY** paid out $30,000 in ransom money to gain access to data that the hacker had blocked.

Lake City, FL paid a ransom demand of 42 bitcoins (approximately $485,000 at the time). Fortunately, the city was insured.

Wilmer, TX was struck by a ransomware attack in 2019. Police, water, and even library computers were corrupted.

In January 2020, a ransomware attack in **Tillamook County, OR** brought government computer systems down for a week.

> It makes sense that smaller towns are being attacked, because typically their cyber defenses are going to be leaner, budgets are lower, they're not aware, and they just don't have the staff to put a framework in place to defend against these kind of attacks." – *Cybersecurity expert Keith Barthold*

When it comes to cybersecurity, inaction can be costly. Talk to a TPx specialist to see how we can help.

Learn more at tpx.com/cybersecurity

TPX

[1] Specops Software Study [2] Atlas VPN [3] BlueVoyant [4] National Conference of State Legislatures. (Published 2017- Revised Feb.2020) State Cyber Training for State Employees [5] The Council of Economic Advisers (2018, Feb.) The Cost of Malicious Cyber Activity to the U.S. Economy. White House [6] Donald Norris, A. J. (2018). Local Governments' Cybersecurity Crisis in 8 Charts. Baltimore: The Conversation [7] Freed, Benjamin. (2019, Oct.). Ransomware Attacks Map Chronicles a Growing Threat. State Scoop.