Sector in Focus October 2025

Cybersecurity for Institutional Investors:

Ransomware Basics and Recent Trends

Ransomware activity has been elevated and the frequency and sophistication of threats has risen in recent years. In the first installment of this two-part cybersecurity series, we will explore the basics of ransomware, recent trends, and the relevance to institutional investors.

At the beginning of 2025, Corvus, a firm that specializes in information technology, observed a spike in ransomware that brought activity to record levels. Their quarterly Cyber Threat Report noted a 35% quarter-over-quarter increase in such activity, and the numbers also marked the second straight quarter of record-high threats.[1]

These attacks disrupt services and are expensive in terms of costs to regain data or system access, as well as to repair security deficiencies. Unfortunately, many attacks were also aided by avoidable oversights. Here are a few examples of recent ransomware attacks:

Change Healthcare, a healthcare technology company owned by UnitedHealth Group, suffered a data breach in February 2024 that affected 100 million individuals. UnitedHealth Group CEO Andrew Witty testified during a Congressional subcommittee hearing that the company paid a $22 million ransom to restore operations.[2]

Cleveland's city government was forced to shut down its city hall for 11 days after a ransomware attack in June 2024. The attack affected residents' ability to submit payments, permits, and building or home applications.[2]

The **Port of Seattle**, a public agency that also oversees the Seattle-Tacoma International Airport, experienced outages after a ransomware attack in August 2024. The airport's bag checking, flight information, check-in services, and some phone systems were affected by the attack. Some services remained down for two weeks after ransomware encrypted the agency's systems.[2]

Minneapolis Public Schools suffered a breach in March 2023 that led to more than 300,000 files being distributed. Information that was affected included medical records, Social Security numbers, and discrimination complaints. The school district refused to pay a $1 million ransom.[3]

Ransomware attacks and other cybersecurity breaches can happen anywhere and to any organization with an internet connection. PFM Asset Management (PFMAM) takes these threats seriously. PFMAM believes raising awareness about cyberattacks like ransomware is essential to the stewardship of public funds.

1 https://www.corvusinsurance.com/blog/q1-2025-travelers-cyber-threat-report?hsCtaAttrib=190750099491.
2 https://www.techtarget.com/searchsecurity/news/366617564/10-of-the-biggest-ransomware-attacks-in-2024.
3 https://www.pbs.org/newshour/nation/after-school-hacks-ransomware-criminals-expose-kids-private-files-online.

A Division of U.S. Bancorp Asset Management, Inc.

pfm asset management

What is ransomware?

Ransomware is a type of malicious software designed to make files and systems inaccessible to the rightful owner in order to demand a price, or "ransom," for restoring access. Network hackers use a variety of methods to gain illicit access to computing devices to plant software. Once ransomware has infected a computer or a network, it quickly notifies users on the network that their data has been taken hostage.

Invariably, a payment (ransom) is requested, and instructions are provided for how to pay it. Some programs even employ negotiating tactics, such as offering some non-essential files back as a goodwill gesture or using a tiered pricing structure based on how long it takes to pay the ransom.

How can I recognize ransomware?

Unfortunately, when you see ransomware, your system has probably already been infected. There may be a countdown clock, a description of how the data has been made inaccessible, and something detailing what the user may need to do to get it back. Three of the most common forms of this type of software are blockers, encryption, and leakware.

A **blocker** is a program that prevents you from using the infected device. It could be a browser window that cannot be closed through the usual means, a fake software update window that demands action, a fake message from a law enforcement agency or a program that floods the screen with unwanted images.

Encryption scrambles data to protect it from being read by anyone except those with the "key," which is usually a random string of alphanumeric characters. Some forms of encryption can be reversed, but not without significant time and cost that is often beyond the value of the data. For this reason, to add a layer of fear to the attack, blocker ransomware will often claim that data has been encrypted, even if it has not.

Leakware is a form of ransomware that threatens to release sensitive information publicly instead of inhibiting access.

Types of Ransomware

- **Phishing:** An email that makes a personal appeal to influence a user to click a link or run a program. Once the link is opened, the software gains access and infects a user's system.
- **Trojan horses:** Viruses that are embedded or disguised within innocuous programs or even seemingly necessary software that an unwitting user runs on their machine.
- **Worms:** A self-replicating program that moves through computer networks. Unlike the methods above, a worm does not depend on tricking users – all this form of ransomware needs is an undefended device to access and infect a network.
- **Password hacks:** A program that seeks access by using common passwords until one works. This approach may seem like a longshot for a hacker, however, it simply plays the percentages. Careless or simple passwords and poor network security can turn an impossibility into an inevitability.
- **Networking vulnerabilities:** Many programs simply exploit missing operating system patches, outdated software releases, and misconfigured firewalls to gain access.

How big of a problem is this for public entities?

There are a number of factors behind the steep jump in attacks referenced in the beginning of this article, but the most conspicuous one is the rise of hybrid and remote work patterns brought about by the COVID-19 pandemic.

With more employees working from home, it may be harder to verify whether messages are genuine. If employees are connecting from outside the company's

network perimeter, or using personal devices, it may be difficult for traditional anti-malware technology to block these incoming messages.

With many local governments and other public entities making these remote and hybrid work practices a permanent part of their operations, hackers have many opportunities to target isolated employees who have become familiar with using digital channels like email as their main way of keeping in touch with colleagues.

Anyone can fall victim to a ransomware attack, but the financial constraints placed on a township's ability to fund cybersecurity, combined with internet-delivered services and the data stored in municipalities' systems, and incentives to resolve public services as rapidly and easily as possible make governments a perfect target.

It is also important to note that the damages of a ransomware attack go well beyond the actual ransom. In fact, paying the ransom could only be the beginning.

It is also important to note that the damages of a ransomware attack go well beyond the actual ransom. In fact, paying the ransom could only be the beginning. A ransomware attack can cost an organization millions in lost productivity and damages to its reputation. Costs may also include time and resources it could take to get the affected systems in full working order again.

How you can protect yourself

Everyone with internet access at a local government or public entity should understand the current cybersecurity risks that exist and their role in helping to avoid potential breaches. The reality is that today, you may be as likely to benefit from your cybersecurity training as you are from your fire safety or medical emergency training.

The fallout from a ransomware attack can be at best an inconvenience, and at worst, crippling. The good news is that there are ways to help prevent them:

Spam filters can stop almost all potentially malicious emails, especially emails containing suspicious attachments, links, etc. Unfortunately, it only takes one email to get through to cause significant damage. Therefore, end-users must be vigilant as well, understanding the risks associated with clicking on unknown links and downloading attachments.

Antivirus software plays an important role in protecting against ransomware, which is a type of malware. While antivirus software may not prevent the next big breach, if kept up to date, it can be good way to help protect against more well-known forms of malware. To keep antivirus software up to date, local governments and public entities should regularly conduct scans of their individual computers and networks.

Vigilance applies to both information technology processes and the people who use them. Each year, new software vulnerabilities are raised, and patches to fix them are issued, and some of the largest ransomware attacks take place after those weaknesses and solutions have already been identified. Local governments and public entities should have a routine process for distributing and installing critical security patches, especially considering the increases in remote-work scenarios. They should also have trained security professionals who understand the vulnerabilities of their system and can take proactive steps to mitigate the risks.

Since a ransomware threat is directly related to data, one of the chief ways local governments and other public entities may mitigate ransomware risk is by designing a **back-up system** that is largely independent from its regular network. The separation helps ensure that a ransomware attack doesn't infect the back-up as well. Installing a back-up system will not prevent a cybersecurity threat, but it can make

an attack less damaging, especially if a response is executed quickly.

Ransomware attacks have reached new levels in the cyber threat equation for local governments. While the most sophisticated attacks may require equally sophisticated prevention measures, the majority can be avoided with widely available technology, a well-thought-out approach to network and data protection, and end-user vigilance and education.

PFMAM continues to emphasize both educating public funds investors on the importance of cybersecurity, as well as being diligent about its own cybersecurity efforts. We can offer investors the knowledge that their funds are protected by the cybersecurity infrastructure of one of the nation's largest banks.

For questions about this report, please reach out to your relationship manager.

In part two of this series, we will conduct a Q&A with Murray Kenyon, Information Security Director with the Information Security Services team at U.S. Bank, about cybersecurity concerns for institutional investors and the resources USBAM has committed to guarding their data and funds.