

**BLOGS**

Cyber Insurance

Protection for Public Entities – Cyber Insurance

In today's digital age, practically anything can be accessed online or remotely—even private and confidential information. So, unsurprisingly, various institutions that receive, maintain, and store substantial amounts of financial or personally identifiable information have suffered a record number of cyber-attacks in recent years, and America's judicial system is no exception.

*Oprah Bennett is a 2022 Summer Associate at Lathrop GPM who contributed to the writing of this blog post.

In today's digital age, practically anything can be accessed online or remotely—even private and confidential information. So, unsurprisingly, various institutions that receive, maintain, and store substantial amounts of financial or personally identifiable information have suffered a record number of cyber-attacks in recent years, and America's judicial system is no exception. On April 16, 2022, the Unified Government of Wyandotte County and Kansas City, Kansas's court system was forced to halt all judicial proceedings as hackers commandeered access to the municipality's online records. With their system breached, Wyandotte County's court officials were unable to conduct business—leading to key services being crippled within the community.

Now more than ever public entities have an urgent need for coverage in the event of a cyber-attack as cyber-related events have crippled the public sector over the past few years, affecting everyone from local municipalities to the federal government. As the Wyandotte County data breach demonstrates, a public entity is at an increased risk for such attacks because they not only use their online systems to make revenue and store private information, but they collect taxes, schedule court cases, dispatch law enforcement and emergency personnel, and administer public services. Accordingly, a complete shut-down in operations of any government entity could be catastrophic not only to a municipality's budget, but to public confidence in the administration of justice.

Cyber insurance continues to be crucial in helping institutions combat cyber-attacks by protecting against losses that inevitably result from data breaches, ransomware, or even terrorist acts. Although cyber insurance won't prevent a cyber-attack, it can provide financial, technical, and legal resources and expertise to help an organization more quickly and efficiently respond to an attack, potentially lessening the impact on the institution's budget and reputation. Cyber coverage is often not included in general liability insurance policies, but policyholders should review any already existing policies they may have—including errors and omissions, public entity liability, directors and officers liability, and property damage policies—to determine whether additional coverage for cyber-related risks may be needed. Standalone cyber insurance policies can also be obtained and specifically tailored to each organization's current needs or

Related People

Alana M. McMullin

Associate

Kansas City

816.460.5531

alana.mcmullin@lathropgpm.com

Related Services

[Insurance Recovery & Counseling](#)



concerns. The most common coverages for cyber-related risks include network security and privacy, cyber fraud and extortion protection, business interruption, crisis management, and public relations. Depending on the specific policy language, these coverages can protect an entity against data breaches, ransomware, virus or computer attacks, and hacker attacks and may pay for resulting losses, including recovery and replacement of lost or stolen data, legal expenses, breach notification costs, regulatory fines or penalties, computer forensics and rebuilding, server backups, and ransom negotiation and payment. Even without private insurance coverage, public entities can self-insure cyber-related risks by setting aside funds earmarked for cyber-attacks or join a risk pool with other local entities, effectively creating their own insurance company to mitigate potential future losses.

In this era of prevalent and potentially devastating cyber-attacks, public entities should determine the best manner in which to protect themselves, as having no protection whatsoever no longer appears to be feasible. Entities should carefully consider all options and have an experienced professional review any standalone coverage to get the most out of that coverage. For more information, contact [Alana McMullin](#) and [Kim Winter](#) with any questions on cyber insurance.