Staying Savvy

How governments can become even smarter customers of cyber insurance

BY SHAYNE KAVANAGH, TERI TAKAI, AND ALISON WUENSCH

Cyberattacks are expensive and highly disruptive. Over the years, many local governments have suffered high-profile cyberattacks. Some of the more recent include:

- The City of St. Paul, Minnesota, experienced a large ransomware attack in the summer of 2025. While caught early, it still resulted in months of disruption to the city's IT systems and the services that rely on them.[1]
- In 2024, the City of Columbus, Ohio, lost protected health information for hundreds of people, which was kept in a fire department database.[2]
- The City of Hamilton, Ontario, faces losses of several million dollars from a 2024 ransomware attack.[3]

Preparing for the potentially extreme consequences of a cyberattack is a fiduciary responsibility of local governments, much like preparing for a natural catastrophe like a flood or an earthquake. Given the potential losses, transferring risk to the insurance market could be an attractive proposition; however, cyber insurance is newer than more traditional forms of insurance, such as property and liability. The updates included in this article will help local governments keep up with the constantly adapting cyber insurance market in a risk-savvy manner.

Underwriting

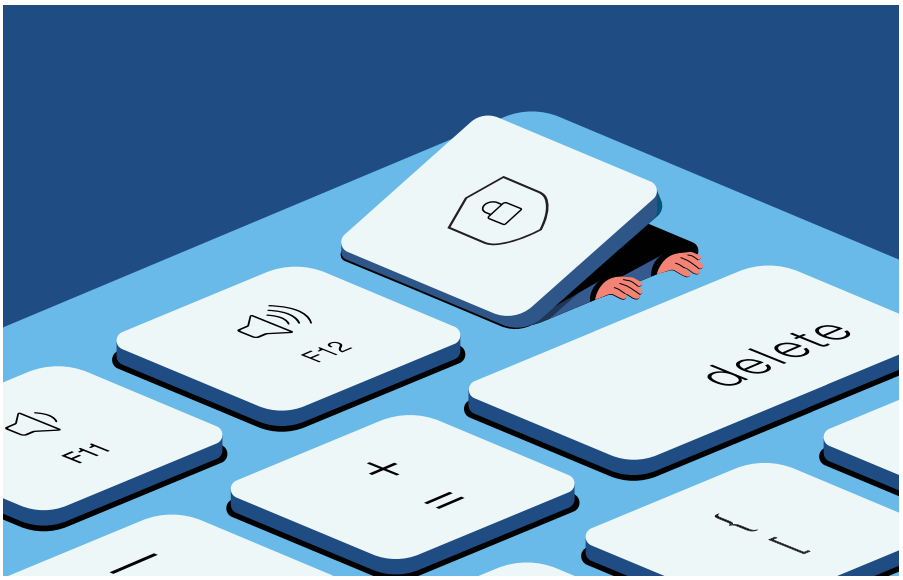
Underwriting is the process insurers use to determine the risks of insuring your government. The underwriting process has stabilized in recent years, and many insurance companies are using cyber risk consultants to help them assess risk more accurately. Underwriters are looking for the insured to have key security features as a prerequisite for a policy. Such features might include multifactor authentication, incident response planning, encrypted data storage, patching cadence, endpoint detection response, network monitoring, and firewalls between agencies and departments. Segmentation has become a requirement for public entities to ensure that a bad actor cannot move from agency to agency or department to department.

More recently, underwriters have placed more emphasis on human controls, like cybersecurity training, to address weaknesses in employees' understanding of cyber risks revealed through that training. Governments that don't have adequate internal security might have trouble getting a policy or might face increased costs.

Payout limits and sublimits

A policy limit is the maximum amount a policy will pay out. Sublimits—a traditional part of insurance policies—limit the reimbursable loss for a certain type of risk that is less than the total limit on the policy. The savvy customer will review all policy language and note any sublimits. Sometimes sublimits are stated clearly on the policy's

GFOA has updated our research paper, "Cyber Risk Savvy: How to Be a Smart Customer of Cyber Insurance" (created with the Center for Digital Government). The following article is adapted from new information in Version 2.0. To read the full report, including new details not included in this article, visit **gfoa.org/materials/cyber-risk-savvy-version-2-0**.



declarations page; other times you will need to review the policy definitions and endorsements to find them. You may find that you have less coverage for a particular type of risk than the policy might have led you to believe.

Sublimits often evolve with the cyber insurance market. A few years ago, two common sublimits were:

Ransomware. Limiting the total coverage available for a ransomware attack versus the total limit for all cybercrimes.

Bricking. Limiting the reimbursement for replacing hardware that is rendered unusable by a cyberattack. For example, the company may cover "hard bricks," where the device is made inoperable, but not a "soft brick," where part of the device may be operable or repairable.

The two sublimits above are now less common—but there are other sublimits to be aware of:

Betterment. A cyberattack requires upgrading a damaged system to a new and better version that is more resistant to attack. A sublimit limits the amount of coverage provided to upgrade above and beyond what was already in place.

Pixel tracking/wrongful collection. Another fast-emerging exclusion category relates to privacy-tracking technologies rather than direct network intrusions. Recent litigation has targeted public and private websites that transmit user data to analytics and social media platforms through embedded tracking pixels. Insurers commonly exclude such "wrongful collection" of information, arguing that it is not a network security failure. Governments using website analytics, ad-tech, or social media integrations may find that these activities are outside the scope of cyber insurance coverage, leaving potential legal defense costs fully retained.

System failure. Limiting the coverage for a cascading system failure, where a failure in one system leads to failures in other integrated systems. For example, staff may not be reimbursed for personal devices that were damaged as a result of connecting to an infected network at work.

Exclusions

Insurance exclusions are policy provisions that waive coverage for certain risks or loss events. Smart customers understand the exclusions; otherwise, their policy may not provide coverage for risks the customer assumed would be covered.

A more recent exclusion to watch for is for "acts of war." Damages from acts of war are excluded from many types of insurance policies, not just cyber. The reason is that an act of war would presumably result in widespread destruction, and an insurance company could not afford to cover large losses occurring to many customers simultaneously.

In some cases, cyberattacks are perpetrated by common cybercriminals, but many cybersecurity experts consider state-sponsored cyberattacks to be a significant risk. If a state-sponsored cyberattack is considered to be an "act of war," it might be excluded. That said, it is often difficult to attribute a cyberattack to a particular attacker, much less determine if the attacker is state-sponsored.

Customers should recognize that state-sponsored cyberattacks are a real threat, and policy exclusions could complicate receiving coverage. Review how "act of war" is defined in your policy.

A related concept is "systemic risk", where there is a broader exclusion for attacks that impact a large number of organizations at once. For example, GFOA has observed cyber modules in municipal risk pools that have a limit on the payouts to the entire pool in aggregate, not just individual participants. This is a way to exclude systemic risk.

Governments should also note exclusions in cyber policies where losses might overlap with other types of insurance.

A common example involves property coverage. Imagine a cyberattack that disables the control systems for a water or sewer utility, damaging not only software and IT hardware but also connected sensors and physical equipment. If the attack forces water/sewer machinery to operate outside design tolerances, resulting in physical damage, a cyber policy may not cover the entire loss. At the same time, a property policy may contain broad cyber exclusions—potentially leaving the government with no coverage under either policy.

An emerging example is social engineering fraud, where cybercriminals impersonate someone with legitimate authority and convince staff to transfer funds to an illegitimate account. For instance, a criminal might pose as the school district superintendent and contact a finance clerk with an "urgent" request to wire money to a "new contractor." Such attacks may fall outside a cyber policy because the fraudster never technically breached the district's network—an authorized employee carried out every action. Losses of this kind are more often covered under a traditional crime or fraud policy.

Finally, an emerging exclusion concern for local government is "lasering," a term we'll borrow from health insurance. (In health insurance, "lasering" means the insurer identifies a specific high-risk individual, such as someone with a chronic condition, and applies a separate, higher deductible or exclusion to that person's claims rather than raising premiums for the whole group.) More sophisticated underwriting now allows insurers to price policies more accurately, but these same techniques also enable insurers to pinpoint specific risks a client presents—including those the insurer would rather not cover. "Lasering" refers to excluding coverage for risks the insurer views as having an unacceptably high likelihood of loss. The name comes from the exclusions being narrowly targeted to a client's circumstances.

For example, an insurer might exclude coverage for cyber incidents involving an outdated software platform that the government maintains. Lasers are not limited to obsolete technologies. Policies have sometimes excluded sublimited losses arising from artificial intelligence systems—such as errors in AI-driven decision tools or AI-generated misinformation—reflecting insurer caution around untested exposures. Lasering lowers the price of the policy but results in the government retaining all risk related to the target of the laser.

Definitions

The customer should be familiar with key provisions within the definitions of the policy. In insurance, a "claims made" policy is one that provides coverage only if the claim is made (reported) during the time the policy is active. Cyber insurance policies are often "claims made." This can present a problem because, for instance, a malicious piece of software could breach the network during the term of a policy but only be discovered (and reported) after the policy is ended. Therefore, it is important to know if the policy is "claims made" or not. If so, be sure to understand the reporting period and the provisions for incidents that are discovered after the term of the policy.

For example, a policy could come with an "extended reporting period," giving the insured additional time to discover and report claims after the policy ends. You'll want to pay extra attention to this issue if you are considering switching insurance providers because the definitions for reporting periods between different insurance providers may not align.

Shayne Kavanagh *is the senior manager of research for GFOA's Research and Consulting Center.* ***Teri Takai*** *is the senior vice president of the Center for Digital Government.* ***Alison Wuensch*** *is a consultant with GFOA's Research and Consulting Center.*

[1] Alex Derosier, "St. Paul, Minn., systems come back online after cyber attack," Government Technology, August 29, 2025.

[2] "Columbus identifies protected health information from cyberattack," City of Columbus, February 3, 2025.

[3] Aaron D'Andrea, "Ontario city facing full $18.3M cyberattack bill after insurer denies claim," Global News, July 31, 2025.

Want to learn more about cybersecurity?

GFOA Chicago 2026

Join us at the GFOA Annual Conference for the session "Cyber Risk Savvy: GFOA's 2026 Cybersecurity Update" on June 29 at 10:30 a.m.

A cyberattack has the potential to shut down your organization's operations and inhibit its ability to deliver critical services to the community—and the cost of recovering from an attack can escalate quickly to millions of dollars. While governments will never completely eradicate this risk, there are effective practices and strategies that you can put in place to minimize your organization's risk. Topics covered in this session will include the latest on emerging threats, the role of artificial intelligence, managing risks related to suppliers and contractors, the value of cyber insurance, and the changing global landscape for cyber criminals. Attend to determine what you need to do to prepare your organization.