A COLLABORATION BETWEEN

CENTER FOR
DIGITAL
GOVERNMENT

VERSION 2.0

CYBER RISK SAVVY

HOW TO BE A SMART CUSTOMER OF CYBER INSURANCE

CENTER FOR DIGITAL GOVERNMENT

VERSION 2.0

CYBER RISK SAVVY

How To Be a Smart Customer of Cyber Insurance

This report is an update of the original Cyber Risk Savvy that was published by GFOA in 2022.

ABOUT THE AUTHORS

- **Shayne Kavanagh**, Senior Manager of Research, GFOA
- **Teri Takai**, Executive Director, Center for Digital Government
- **Alison Wuensch**, Consultant, GFOA

ACKNOWLEDGMENTS

GFOA would like to thank the following people for their review of the paper:

- **Deborah A. Snyder**, Senior Fellow, Center for Digital Government, former State of New York Chief Information Security Officer
- **Nancy Rainosek**, Senior Fellow, Center for Digital Government, former, Chief Information Security Officer, State of Texas
- **Temo Garcia**, Vice President & Team Leader, Aon E&O/Cyber Broking
- **Phil Bertolini**, Chief Delivery Officer, e.Republic*
- **Suzi DeYoung**, former Chief Financial Officer, Adams 12 Five Star Schools*
- **Stewart Ellenberg**, Director of Risk Management, Adams 12 Five Star Schools*
- **Kaela Nelson**, Finance Director, City of Powell, Wyoming*
- **Marc Pfeiffer**, Associate Director, Bloustein Local Government Research Center, Bloustein School of Planning and Public Policy*
- **Cody Olsen**, Vice President and Team Leader, Aon Cyber Solutions Group*

* Reviewer of the first edition of this report

ABOUT GFOA

The Government Finance Officers Association (GFOA) represents over 28,000 public finance officers throughout the United States and Canada. GFOA's mission is to advance excellence in government finance. GFOA views its role as a resource, educator, facilitator, and advocate for both its members and the governments they serve and provides best practice guidance, leadership, professional development, resources and tools, networking opportunities, award programs, and advisory services.

Cyberattacks are a clear and present danger for all organizations, but local governments are particularly vulnerable. A Comparitech study found at least 525 ransomware attacks on U.S. government organizations between 2018 and 2024.[1] Demands range from $1,000 to $23 million, with an average of $873,000. Governments lost an average of 19.5 days to downtime per attack, but the number of days lost can vary widely from this average. The study notes that "local governments have remained a key target for hackers over the years."

Local governments are attractive targets for cybercriminals for a few reasons.[2] First, local governments are "soft targets." Networks are typically not very secure. For example, smaller local governments may not have dedicated IT staff, much less dedicated cybersecurity staff. Local governments operate many disparate services, creating a large "surface area" for an attack. In other words, an attacker could gain access to a city government's network through information systems in public works, community development, or any other department. Second, local governments maintain sensitive data like tax records, voter information, citizen and employee health-related data, and employee Social Security information. They also provide essential services that can't be interrupted. A soft target with sensitive information and essential services is the proverbial "low-hanging fruit" for the cybercriminal. A third reason is the public profile of local governments—transparency requirements, open data sets, public-facing internet-enabled transactions, and more. This public profile means hackers have an advantage in calculating an effective strategy to penetrate a local government's defenses. This compares to private firms that have greater ability to conceal their activities from the public and, therefore, cybercriminals.

WHAT IS RANSOMWARE?

Ransomware is "a type of malicious attack where attackers encrypt an organization's data and demand payment to restore access."[3] Organizations fall prey by clicking on malicious links in phishing emails or visiting unsafe sites that download and activate malware.

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.[4]
- In 2024, the City of Columbus, Ohio, lost protected health information for hundreds of people, which was kept in a fire department database.[5]
- The City of Hamilton, Ontario, faces losses of several million dollars from a 2024 ransomware attack.[6]

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 earthquake. Given the potential losses, transferring risk to the insurance market could be an attractive proposition. However, cyber insurance is newer than traditional insurances like property and liability insurance. This paper will help local governments approach cyber insurance in a risk-savvy manner and make smart investment decisions to protect against cybercrime.

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 earthquake.

As a first step, let's understand three fundamental issues with cyber insurance that an informed consumer must be aware of.

First, insurance is remedial, whereas controls or cybersecurity measures can be preventative. Training in safe computing practices can make it less likely an employee clicks on a malicious email link, thereby avoiding an attack that could have otherwise succeeded.

Prevention is preferable to remediation. Cyberattacks can have consequences beyond what insurance can cover. For example, the City of Stuart, Florida, faced a ransomware attack and found that even if it had been able to use insurance to pay the ransom, the files that would be "restored" by the cybercriminal would go

to one folder, with new names and no file extensions. Insurance is not an "undo button" for a cyberattack. There will always be costs to a cyberattack that insurance doesn't cover. Further, insurance doesn't necessarily fix the insufficient controls that allowed the attack to happen in the first place.

Indirect effects of a cyberattack—such as the damage to a local government's reputation—are best avoided. Reputation is not inconsequential. A loss of public faith in government has consequences. A perceived vulnerability to cybercrime also could affect bond ratings.[7] *This means local governments must be savvy in choosing when to invest limited resources in stronger cybersecurity controls versus when to invest in cyber insurance.*

Second, commercial insurance, by design, is a "bad bet" for the insured, on average. If it weren't, insurance companies would go broke. This is why governments can sometimes reduce costs by self-insuring. This does not mean local governments should never buy commercial insurance. Commercial insurance is great for protecting against catastrophic losses that government isn't capable of absorbing. This means local governments must be savvy in determining when to accept the risk (self-insure) and when to transfer risk to commercial insurers.

Third, the cyber insurance market continues to evolve with the level of threat posed to governments by cybercrime. This market has matured in recent years, and insurers now have more/better actuarial models and underwriting tools to assess risks such as ransomware, data breaches, and systemic threats. However, the cyber insurance market still is not as mature as other insurance markets that have been around for decades and maybe centuries. Hence, the market for cyber insurance continues to evolve as insurers and buyers gain a better understanding of the nature of the peril and the financial implications of insuring it. As of this writing, the market for cyber insurance is stabilizing, with more insurers covering public entities. In fact, there has been a long-term decline in average policy costs.[8] Insurers are also becoming more discerning in segmenting potential clients by potential risk, which allows the insurer to price policies more accurately. *This means local governments must be savvy about recognizing the evolving nature of the cyber insurance market and not assume that today's coverage will necessarily be available at comparable prices in the future.*

With these issues in mind, how should a local government approach cyber insurance? This paper takes you through a step-by-step procedure for considering the costs versus the benefits of cyber insurance.

Risk Mitigation vs. Risk Transfer — or Cybersecurity Controls vs. Cyber Insurance

Local governments have limited resources, so a dollar invested in cyber insurance is a dollar not invested in controls. The advantage of controls is that they are preventative—they stop attacks before damage occurs. A software patching strategy leaves fewer vulnerabilities for cybercriminals to exploit. Controls also reduce potential damage from an attack if an attack succeeds. For example, high-quality data backups make it easier to recover lost data.

Insurance is always remedial—it cleans up the damage after it occurs. The advantage of insurance is that it can provide some relief from catastrophic losses, where it is impractical to develop sufficient controls. Hence, there is a trade-off to consider. How can this trade-off be analyzed? We will present a four-step process, summarized below.* During the course of this paper, there will be several technical cybersecurity terms used. If you are unfamiliar with these terms, you can consult our glossary in Appendix 1.

STEP 1 **Know the Basics of Your Cybersecurity Situation**

STEP 2 **Quantify Your Risk**

STEP 3 **Examine the Potential of Insurance**

STEP 4 **Periodically Reassess**

* The four steps of this process are based on the *Cyber Loop* method described in: Aon. (2019). *Protecting today. Safeguarding tomorrow. The cyber loop: Managing cyber risk requires a circular strategy.* https://insights-north-america.aon.com/cyber/aon-the-cyber-loop-managing-cyber-risk-requires-a-circular-strategy-whitepaper

STEP 1
Know the Basics of Your Cybersecurity Situation

Some local governments understand their cybersecurity situation, but others may not. There are three questions to ask in Step 1:

What are the most important assets you need to protect? Technology assets with sensitive data or that administer mission-critical functions are the most important. These may include Social Security numbers, credit card and bank information, health data protected by law (for example, the U.S. Health Insurance Portability and Accountability Act), and criminal justice data. Critical systems might include enterprise resource planning (ERP), tax revenue systems, and public health or public safety systems.

What threats are most important? Today, ransomware attacks remain the most prevalent threat and are primarily driven by email compromises. Other threats include denial of service attacks, sensitive data leaks, cyber sabotage of various forms, or social engineering. Social engineering has become a more prominent threat across all industries. Ransomware attacks will likely continue to be the top threat because there is a financial incentive for the perpetrator. These threats can combine. For example, a ransomware attack could lead to data leaks.

What is the state of your controls? State and local governments have been challenged with finding resources to keep up with cyber threats. Important controls include multifactor authentication, firewalls, encrypted data storage, encrypted data backups, off-line backups, network segmentation, incident response planning, training staff to avoid phishing attacks, software patching, and endpoint detection response.* In a 2021 survey,[9] respondents indicated that spending on cybersecurity focused on software, hardware, backup, monitoring, and training. Incident response was listed as a lower priority. Focus areas for business continuity in the face of a cybersecurity attack include data backups and recovery, operational business plans, and ensuring manual workarounds in case of an outage.

There are comprehensive frameworks for addressing cybersecurity risks, like CIS Critical Security Controls (perhaps the most accessible for local government, especially small to mid-sized**), COBIT, NIST, and ISO. These frameworks and what they each offer are summarized at the end of this report. These frameworks are valuable for organizations with sophistication to use them. **However, even a basic assessment of whether you have the controls described in this paper, or not, can be useful for Step 1**. At the end of Step 1, many local governments will find they have opportunities to invest more in cyber controls. Multifactor authentication, firewalls, patching, and training employees on safe computing practices are potentially valuable controls and may represent a wise investment in cyber risk prevention.

CAN YOU **ELIMINATE RISKS?**

One risk management strategy is to eliminate risky activities. In the world of cyber insurance, an opportunity might be to reduce the amount of sensitive data the government collects and stores. Ask whether collecting and storing certain sensitive data is necessary and worth the exposure.

* If you are not familiar with the controls in this sentence, please see the Appendix.

**CIS includes "implementation groups (IG)", which are intended to scale CIS's guidance to organizations of different sizes. IG1 might be particularly salient to small and medium local governments, according to Marc Pfeiffer who studies local government cyber security issues at Rutgers University.

STEP 2
Quantify Your Risk

It's difficult, if not impossible, to make a savvy decision about the trade-offs between investing in controls and purchasing insurance without quantifying the risks. "Risk" can be defined as the chance of a loss, disaster, or other undesirable event ***multiplied by*** the magnitude of the loss. This implies that risk is a quantifiable property.*

People have attempted qualitative risk analyses in the form of a "risk matrix" or "heat maps," where risks are classified along a scale such as "low," "medium," and "high," and color coded according to severity. However, research shows this analysis can lead to *worse* decisions![10] This happens due to an "illusion of communication," where decision-makers falsely assume everyone shares a similar understanding of risk.[11] The problem is that categories like "low," "medium," and "high" are vague and invite different interpretations from different people. Imagine one of your colleagues is an inveterate sports gambler and another has never so much as purchased a lottery ticket. These two people probably have different definitions of "low" risk. However, if risk is quantified, like "we believe there is a 10% chance of a ransomware attack costing us more than $100,000 in the next year," there is less room for interpretation.

Another reason risk matrices can be counterproductive is they act as an "analysis placebo,"[12] where decision-makers think they understand the risk because they have subjectively characterized the risk as "high," "low," etc. But because the risk matrix is not based on hard data about the chance and potential magnitude of loss, decision-makers are overconfident about their understanding of risk.

Though risk matrices are easy to create, understand, and inexpensive to use, they aren't worthwhile if they lead to lower-quality decisions. The alternative is to quantify risks.

The Typical Risk Matrix Often Leads to Worse Decisions About Risk

Likelihood \ Impact	Negligible	Minor	Moderate	Significant	Severe
Very Likely	Low Med	Medium	Med Hi	High	High
Likely	Low	Low Med	Medium	Med Hi	High
Possible	Low	Low Med	Medium	Med Hi	Med Hi
Unlikely	Low	Low Med	Low Med	Medium	Med Hi
Very Unlikely	Low	Low	Low Med	Medium	Medium

* Loss includes things sometimes thought of as "intangible," like community trust, reputation, etc. These losses are also measurable, though not as easily as some other losses. For more on this subject, see: Hubbard, D. (2014). *How to measure anything: Finding the value of intangibles in business.* Wiley.

We will not get into the details of how to quantify risk. **That is best left to professional risk analysts. Instead, we will show concepts to help you think about cyber risks consistent with a quantified approach. This will help you ask the right questions of the risk professionals versed in risk quantification.** If you would like to dig deeper into risk quantification, here are three sources for further detail:

- GFOA has developed a sample Excel ransomware risk model that uses the same methods insurance companies use to quantify risk, but it is built on the open Probability Management standard.[13] This is not a substitute for professional risk analysis and is intended only as an educational tool for ransomware risk. It will provide the basics of how the risks of a cyberattack could be quantified. It is not meant to be a comprehensive analysis of your cybersecurity risk. The content of Step 2 will be largely based on the sample model but will not cover all the details in the model. You can get access to the model at gfoa.org/cyber-insurance.
- The book *How to Measure Anything in Cybersecurity Risk* by Doug Hubbard and Richard Seiesen goes deeper into the details than the GFOA risk model. The GFOA risk model is consistent with the ideas presented in this book.
- Finally, GFOA has found that some insurance companies are taking steps to provide clients with richer quantification of risk. They believe that more informed customers will be better, long-term customers. Understanding the concepts in this paper will help you ask insurance providers for the right information and help you make the best use of the information.

Before we begin our discussion of quantifying risks, we'd first like to acknowledge that quantifying risks is often not the normal course of business for local governments. As such, it is natural there might be skepticism about the potential for quantifying risks. Following are three common objections to quantification posed by the skeptic and our response:[14]

Objection 1: Quantifying risk is more appropriate for insurance industry analysis and is unlikely to be appreciated by local governments looking for practical advice.

Answer: We often underestimate others' capabilities relative to our own.[15] GFOA has presented quantified risk information to many elected officials and government staff and has yet to find one who could not grasp the essential point. As for practicality, given that subjective methods, such as a risk matrix, often lead to worse decisions, we would suggest that it is the subjective methods that don't work in practice.

Objection 2: The cyber insurance market can change, so decisions based on a quantitative model will be wrong.

Answer: Insurance companies have been making decisions based on quantitative methods as early as the 17th century. Not every insurance decision is perfect. But it is understood within the industry that it would be foolish to compete without quantitative methods.[16] The next objection is also relevant to this issue.

Objection 3: Within cybersecurity, there are too many complexities changing too quickly to make a reasonably accurate assessment.

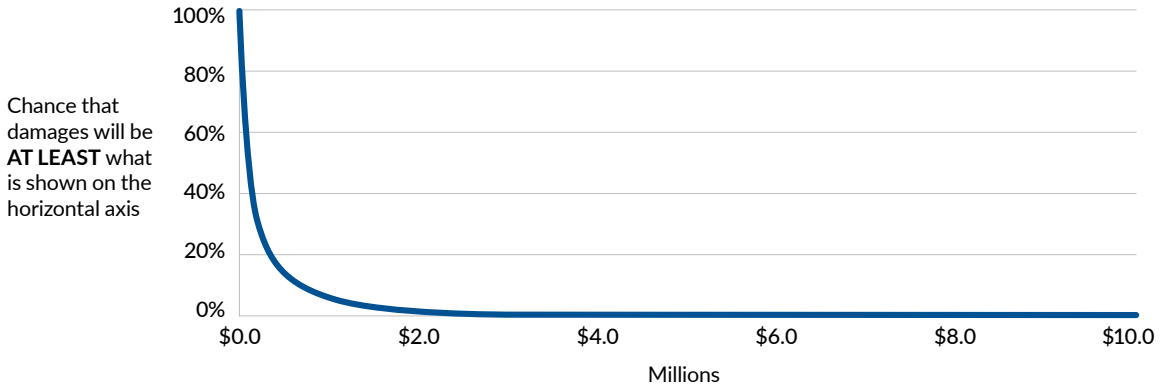
Answer: A government must decide how to invest in commercial insurance, self-insurance, and controls for cybersecurity. A government can either take a wild guess and hope for the best or take a more rigorous approach. A quantitative model does not have to be perfect to be useful—it just needs to outperform the alternative, which is a subjective judgment. Because a quantitative model forces rigor and transparency in how you think about a question, there is a good chance that even an imperfect model will outperform subjective judgment.[17]

With the objections to quantifying risk addressed, the first step is to gather data on how likely a cybercrime loss is and how large that loss might be. First, we must recognize that good data will be difficult to obtain, but not impossible. But remember, a model does not have to be perfect—it just needs to outperform the alternative (e.g., guesswork). Doug Hubbard, suggests the following data sources can inform cyber risk models: VERIS, DBIR, and IRIS.[18] Let's start with the chance of a ransomware attack, defined as multiple computers infected ***and*** files successfully encrypted. This means the local government is ***not*** able to stop the attack once the computers are infected. Our off-the-record conversation with a local government risk pool found that their pool members experienced roughly a 5% to 10% chance of a successful ransomware attack in a given year. Moving on to damages from a successful attack, according to the NetDiligence Cyber Claims Study: 2025 Report, the five-year average total incident cost was $180,000 for public entities, with claims ranging from $2,000 to $4,000,000.[19] According to the report, the average incident cost has increased substantially for public entities since 2022. Total incident response includes costs like forensics, business interruption, recovery, and ransom payments (if one is paid). Finally, cyber is an evolving threat, so these figures could change year to year, perhaps significantly.

Next is to visualize this data to understand the implications of your baseline risk. There are many ways to do this, but we'll use what is known as a "loss exceedance curve" (LEC). An LEC presents risk the way insurance companies think about it and is commonly used in different industries to depict risk. An LEC can be constructed for specific applications (e.g., ERP), departments (e.g., police), risks (e.g., ransomware), or any other relevant perspective. Exhibit 1 shows an LEC for a successful ransomware attack. The vertical axis shows the chance of a given loss (or greater) occurring, and the horizontal axis shows the loss. For instance, there is about a 40% chance of losing at least $160,000 because an attack was successful. This is because the blue line passed through the 40% mark at about $160,000. The blue line skims along the bottom of the graph for some distance, which indicates a small chance of catastrophic losses.

EXHIBIT 1 | LOSS EXCEEDANCE CURVE FOR A SUCCESSFUL RANSOMWARE ATTACK

This shows the risk present from a ransomware attack for a hypothetical government, ***given that an attempted attack has succeeded.***

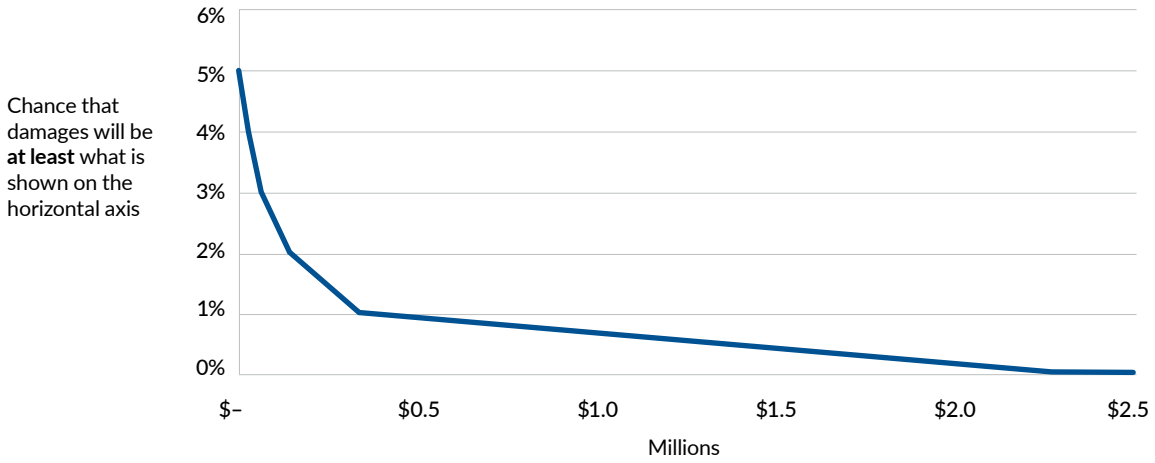


It will be difficult, if not impossible, to make a savvy decision about the trade-offs between investing in controls and purchasing insurance without quantifying the risks.

However, the damages from a successful attack must be considered against the chance an attack will succeed in the first place. Exhibit 2 shows an LEC with the chance that a successful attack will occur factored in. You can see that the blue line intersecting the vertical axis has a much lower chance in Exhibit 2. This is because a successful attack is a low-probability event.

EXHIBIT 2 | LOSS EXCEEDANCE CURVE, GIVEN THE CHANCE OF ONE OR MORE SUCCESSFUL ATTACKS IN A YEAR

This shows the risk present from a ransomware attack for a hypothetical government, ***given the chance that an attempted attack will or will not succeed.***

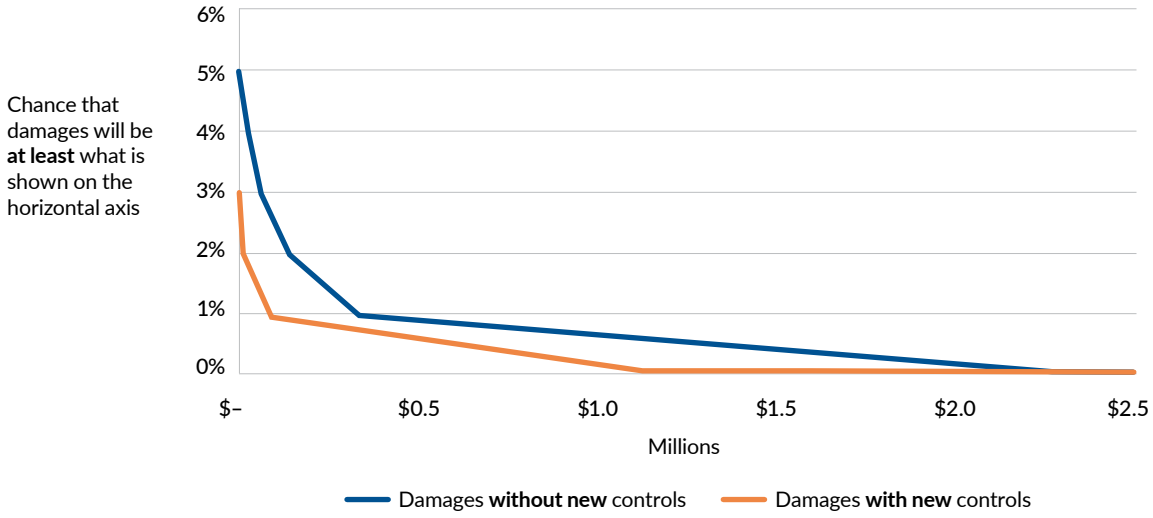


The blue lines in Exhibits 1 and 2 show what is known as "inherent risk." This is your baseline level of risk, reflecting the controls you have in place now. The analysis can show how the curve would change if you invested in additional controls. For example, you could invest in better data backups to reduce the damage from a successful attack—and in better employee training to guard against phishing attempts to lower the chance of an attack occurring. The red line in Exhibit 3 shows what a 10% reduction in the chance of a successful attack and a 30% reduction in potential damage would look like. You can see that the red line intersects with the vertical axis at a lower point, which means you've lowered your chance of experiencing damage. There is also a substantial gap between the red and blue lines all along the curve. This gap represents the lower potential damages from the mitigations.

Early research found that local governments were among the least effective sectors at stopping ransomware before data encryption. By 2024, the same research series reported that roughly 43% of public sector organizations managed to contain attacks before encryption—a substantial improvement attributed to stronger detection, MFA adoption, and incident response measures.[20]

EXHIBIT 3 | LOSS EXCEEDANCE CURVE WITH THE IMPACT OF NEW CONTROLS ADDED

This shows how the risk in Exhibit 2 changes when new contols are added. The blue line is the same as Exhibit 2. The red line is new and shows the imapct of adding more controls.



The red line in Exhibit 3 is also known as "residual risk." This is the remaining exposure after making optional investments in additional controls. In the sample risk model, you determine the size and type of the investment, and you could explore options for investing in controls. Making investments in controls shifts the curve downward, which means the risk profile becomes more favorable. There are two caveats to consider, though. First, controls can fail, be poorly implemented, or not live up to expectations. Hence, a good control strategy is diversified so you are not dependent on any single control. Second, residual risk can't reach zero. Not only is this a theoretical impossibility, as long as the government uses information technology, but it is also a practical impossibility, given the limited resources available for cybersecurity. Hence, being risk savvy is identifying where you are willing to make additional security investments, where you will rely on insurance, and where you will absorb risk.

Quantifying your baseline (or inherent risk) and your potential to invest in controls (or residual risk) accomplishes two goals:

First, it helps you evaluate the value of investing in additional controls. Local governments may find there is a strong case to invest in new controls, such as training on safe computing practices for staff, multifactor authentication, virtual private networks, and data encryption and backup services. This analysis can show decision-makers the value of training by illustrating the reduction in risk it provides. Early research found that local governments were among the least effective sectors at stopping ransomware before data encryption. By 2024, the same research series reported that roughly 43% of public sector organizations managed to contain attacks before encryption—a substantial improvement attributed to stronger detection, MFA adoption, and incident response measures.[20]

If your controls are already strong, the analysis might highlight the limited benefit from additional investment. For example, if you had to spend $1 million on new controls for an average reduction in damages of $100,000, you might question if that is a good investment. The GFOA sample risk model for ransomware walks you through some return on investment calculations for controls.

The second goal that quantification accomplishes is to set the stage for making a wise decision about investing in controls versus insurance. We'll take this up in more detail in Step 3.

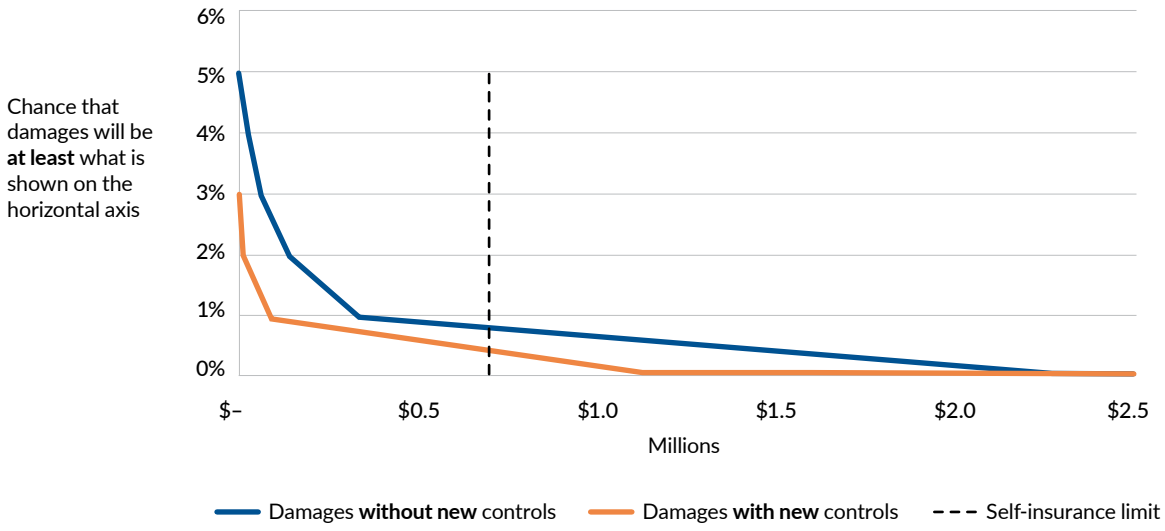
STEP 3
Examine the Potential of Insurance

First, "self-insurance" should not be overlooked. Local governments often set up self-insurance for all types of risks. There is no reason that self-insurance couldn't work for cyber risk as well. Although the market has stabilized, self-insurance remains important for two reasons: First, to reduce the cost of a commercial policy, governments might be forced to accept a higher retention amount* on the policy. Retention is a form of self-insurance. Second, if the market were to lose stability, making policies harder to obtain, self-insurance would be the alternative to commercial coverage.

For these reasons, Step 3 should include an analysis of self-insurance capacity to determine the amount of risk you are willing to absorb via self-insurance. Exhibit 4 adds to our LECs from Step 2 by including the amount a government is willing to put aside for self-insurance—$700,000 in this case. This could be derived from the number of liquid resources a government has available to respond to unplanned emergencies (e.g., reserves). You could determine the chance of exceeding this amount and compare it to your risk tolerance. We have indicated the chances in Exhibit 4, and the GFOA sample model shows the chances for any self-insurance amount you enter. Would you be comfortable with an 8% chance (or one in 12 years) that self-insurance would be inadequate for the losses you experience in a year—or, put another way, a 92% chance that self-insurance would be adequate? If not, you might consider commercial insurance if further self-insurance is impractical.

EXHIBIT 4 | LOSS EXCEEDANCE CURVE WITH AN AMOUNT AVAILABLE FOR SELF-INSURANCE

This shows the same curves as Exhibit 3, but adds in the horizontal line to show the capacity for self-insurance based on the amount of money that is available to be put aside for self-insurance.



* Retention is the total amount of a loss the insurance policyholder must pay out of pocket. It includes the deductible but is not limited to the deductible. For example, insurance policies have limits on how much will be paid out. The government is retaining the risk that the cost of a cyber incident could be more than the policy limit.

Self-insurance is often most valuable when: A) investing in more controls loses cost-effectiveness, and B) commercial insurance can be made more affordable by accepting higher retention. Knowing the amount available for self-insurance is a good place to start when considering commercial insurance.

Commercial insurance is most useful at the far end of the loss exceedance curve. There are some unavoidable risks in operating a modern local government. For example, a local government could reduce cybercrime risk by severing all its connections to the internet, but that would present an unacceptable cost in lost operational efficiency. This means the risk of extreme losses is unavoidable. The far end of the loss exceedance curve is where the potential losses are too high to absorb via self-insurance. Some local governments transfer this kind of risk via pooled risk programs or intergovernmental insurance trusts, which increasingly include cyber modules.

Commercial cyber insurance can, *theoretically*, cover various losses. Exhibit 5 provides an overview of the coverages that *could* be available.[21] Make note of our use of conditionals like "theoretically" and "could." Market conditions will determine if an insurance company is willing to sell you any of these policies.

EXHIBIT 5 | CYBER COVERAGES OVERVIEW

OPERATIONAL RISKS
Network Business Interruption—Covers lost net income caused by a network security failure, as well as an associated extra expense.
System Failure—Expands coverage trigger for business interruption beyond computer network security failure to include system failure.
Dependent Business Interruption/Dependent System Failure—Coverage for lost income caused by a network security failure of a business on which the insured is dependent, as well as an associated extra expense.
Cyber Extortion—Coverage for expenses incurred in the investigation of a threat and any extortion payments made to prevent or resolve the threat.
Digital Asset Restoration—Coverage for costs incurred to restore, recollect, or recreate intangible, nonphysical assets (software or data) that are corrupted, destroyed, or deleted due to a network security failure.
PRIVACY AND NETWORK SECURITY RISK
Privacy Liability—Coverage for defense costs and damages suffered by others for failure to protect personally identifiable or confidential third-party information.
Security Liability—Coverage for defense costs and damages suffered by others resulting from a failure of computer security, including liability caused by theft or disclosure of confidential information, unauthorized access, unauthorized use, denial of service attack, or transmission of a computer virus.
Privacy Regulatory Fines and Penalties—Liability coverage for defense costs for proceedings brought by a governmental agency in connection with a failure to protect private information and/or a failure of network security pursuant to applicable laws or regulations.
Media Liability—Coverage for defense costs and damages suffered by others for content-based injuries such as libel, slander, defamation, copyright infringement, trademark infringement, or invasion of privacy.
PCI Fines and Penalties—Coverage for a monetary assessment from a payment card association (e.g., MasterCard, Visa, American Express) or bank processing payment card transactions (i.e., an "acquiring bank") in connection with an insured's noncompliance with PCI Security Standards.
Breach Event Expenses—Reimbursement coverage costs to respond to a data privacy or security incident. Covered expenses include certain computer forensic expenses, legal expenses, costs for a public relations firm and related advertising to restore your reputation, consumer notification, call centers, and consumer credit monitoring services.

EXHIBIT 5 | CYBER COVERAGES OVERVIEW (CONTINUED)

CYBERCRIME INSURANCE COVERAGE
Social Engineering Coverage—Coverage for direct financial loss as a result of fraudulent instructions provided by a third party that is intended to mislead an insured through the misrepresentation of a material fact.
Funds Transfer Fraud—Coverage for direct financial loss as a result of fraudulent instructions provided to a financial institution that authorize the transfer of the insured's funds by a third party impersonating an insured.
Computer Fraud—Coverage for direct financial loss sustained resulting from the unauthorized seizure of funds from their computer network by a rogue employee or malicious third party.
MISCELLANEOUS CYBER INSURANCE COVERAGES
Reputational Income Loss—Coverage for lost net income caused by bad publicity resulting from a security event.
Bricking Coverage—Coverage to replace hardware rendered inoperable due to a security breach.
Claims Avoidance Coverage—Coverage for expenses incurred as a result of the insured's reasonable investigation of a potentially covered claim.
Reward Payment Coverage—Coverage of payment for information that leads to the conviction of any individual committing or attempting to commit an illegal act relating to a security event.
Betterment Coverage—Coverage for expenses incurred to update, restore, or improve computer systems to a level beyond that which existed before a security event.

That said, as of this writing, more insurance providers are willing to sell policies than a few years ago. Even so, they may place limits on the policy—that is, boundaries on what is and isn't covered. Smart customers will understand these limits and their implications. Now let's examine the limitations in cyber insurance policies. We'll cover major categories of limitations below and Appendix 2 fashions this information into a questionnaire you can use to evaluate your own cyber insurance program.

Underwriting

Underwriting is the process insurers use to determine the risks of insuring your government. The underwriting process has stabilized in recent years. 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 with inadequate internal security might have trouble getting a policy or might face increased costs.

Key questions to ask: *How can you make the best impression on your underwriters to convince them you are a good risk? Do you have cost-effective opportunities to improve your security controls?*

Payout Limits and Sublimits

A policy limit is the maximum amount a policy will pay out. Sublimits are a traditional part of insurance policies. They are a limit on 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 clear on the policy's declarations page. Other times you will need to review the policy definitions and endorsements to find sublimits. 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 repaired.

The two sublimits above are now less common. However, 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.

Key questions to ask: *What are the sublimits in your policy? Do these sublimits change your understanding of the level of coverage you have? What implication does that have for your investment in cyber insurance (commercial or self-insurance) versus cyber controls?*

"Self-insurance" should not be overlooked. Local governments often set up self-insurance for all types of risks. There is no reason that self-insurance couldn't work for cyber risk as well.

Retentions

Retentions are another traditional part of an insurance policy. Retention is the risk retained by the insured—or, put another way, the damages the insured must pay out of pocket outside what is covered by insurance. Lower retentions are not necessarily better, since a policy with a lower retention will cost more. A higher retention may help reduce the policy's cost if the government can self-insure for the larger amount. Note that "retention" commonly refers to policy deductibles but also encompasses other retained risks. For example, if a policy has a low limit, the risk that an incident will cost more than that limit would also be retained by the government.*

Another issue is "single highest retention." Exhibit 6 shows a hypothetical cyber insurance plan with five policies. An attack happens and triggers three of the policies. The single highest retention looks across all three policies and selects the highest retention (deductible) as the amount the insured pays. The multiple retention policy sums up all the retentions. Though a multiple retention policy would likely be less expensive, a single retention policy might be preferable because it will be easier for the insured to estimate the retention cost of a given attack. In Exhibit 6, the insured need only look across the retentions of all five policies, find the minimum and the maximum, and that is the range of possible retentions for a given attack under a single retention policy. For a multiple retention policy, the range is the smallest single retention to the sum of all the retentions in the policy. The latter would be more difficult to plan for.

Key questions to ask: *What balance between retention (self-insurance) and policy price (commercial insurance) is best for you? Is your policy the single highest retention?*

EXHIBIT 6 | SINGLE RETENTION VS. MULTIPLE RETENTIONS

	Retention
Security liability	$500,000
Regulatory liability	$500,000
PCI (payment card industry)	$500,000
Breach response	$750,000
Business interruption	$500,000

↓

Attack happens and triggers these policies:
PCI (payment card industry)
Breach response
Business interruption

If you had **Single Highest Retention**:	
PCI (payment card industry)	$500,000
Breach response	$750,000
Business interruption	$500,000
You pay **max** of the group above	**$750,000**

If you had **Multiple Retentions**:	
PCI (payment card industry)	$500,000
Breach response	$750,000
Business interruption	$500,000
You pay **sum** of the group above	**$1,750,000**

* Other examples of retained risk include 100% self-insurance strategies that are apart from a commercial policy or risks that a government chooses not to insure at all (self or commercial).

Panel Requirements

Next, know the requirements to secure assistance from a preapproved cybersecurity contractor in the event of a breach. The list of preapproved contractors is known as a "panel" and may include all aspects of support for a breach (e.g., legal counsel, technology support, etc.). This is similar to personal automobile insurance where the insurer, in the event of an accident, requires the insured to use an approved repair shop. With cyber insurance, if you use a cybersecurity contractor not on the insurer's list of approved providers—known as going "off panel"—you may lose all coverage for a breach response. While some insurers remain strict about going "off panel," many insurers are open to reviewing vendors chosen by the client. It is recommended that you include any vendors you plan to use in your policy so they can be treated as approved vendors. Some insurers offer options for which contractors you may use while others require you to use a single contractor. You may also need prior authorization from the insurer before engaging certain kinds of solution providers during a cyber incident (e.g., lawyers) – make sure any such requirements to get prior authorization are built into your response plan. It is important to know the requirements and your options at the start of the policy period.

Finally, panel requirements are not necessarily a bad thing. For example, ransom payments might require cryptocurrency. An experienced consultant, like would be found "on panel," will be able to secure the right kind of cryptocurrency faster than a government.

Key questions to ask: *What obligations do you have to use a specified security contractor to help respond to a breach? What options do you have to select between contractors?*

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. According to one cybersecurity expert we spoke with, in almost every cyber insurance event they've been involved with, the insured did not take the time to understand the exclusions, to their detriment. An example of a common exclusion for cyber policies is civil and legal liabilities for breach of personal data.

Ransomware continues to be the leading cyber threat for local governments, so let's examine some of the germane exclusions to that type of policy. In the previous section, we discussed "panel requirements," or the requirement that the insured use only preapproved cybersecurity contractors to respond to a breach. Going "off panel" is a form of exclusion, where using an unapproved contractor could result in an exclusion from coverage.

Another kind of exclusion would be failing to adhere to cybersecurity requirements described in the policy. Earlier, we described that the City of Hamilton was hit by a large ransomware attack. The insurer denied coverage, citing a lack of fully implemented multifactor authentication (MFA) as an exclusion in the policy. This means the City has retained the full cost of the attack (several million dollars).[22]

Federal government policy on responding to ransomware attacks is evolving.* From the perspective of an individual organization that is the victim of an attack, the logical response is for the insurer and the customer to figure out if it is better to pay the ransom or pay the cost to recover the affected systems without access to the ransomed data. However, this presents a collective action problem: When any single victim pays a ransom, it encourages cybercriminals to launch more attacks. Federal law enforcement and regulatory agencies **continue to strongly discourage ransom payments**, and the U.S. Treasury's OFAC has warned that **payments involving sanctioned parties may be illegal**. The 2021 **Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments** remains a cornerstone document in U.S. policy, guiding risk assessments and due diligence obligations in ransomware response.[23] An insurance

* Known as OFAC guidance, promulgated by the U.S. Department of the Treasury's Office of Foreign Assets Control.

policy would exclude coverage for ransom payments when making the payment would violate federal policy. State governments could join the federal government in creating an exclusion. In April 2022, North Carolina became the first state in the U.S. to prohibit state agencies and local governments from paying ransoms or even communicating with attackers. While a few other states, such as Florida, have adopted similar measures, the approach remains relatively rare, and enforcement and impact vary.[24]

Another sticky area is exclusions of "acts of war." Damages from acts of war are excluded from many types of insurance policies, not just cyber. The reason is 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.* Earlier, we noted that more sophisticated underwriting now allows insurers to price policies more accurately. 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.

Key questions to ask: *What exclusions does the policy contain? What are the exclusions specific to ransomware attacks? What are the exclusions related to potentially overlapping or complementary types of insurance policies?*

Definitions

The customer should be familiar with key provisions within the definitions of the policy. First, we'll reiterate the importance of understanding the requirements to use certain preapproved cybersecurity contractors in the event of a breach (the panel requirements).

Next, be aware of when the insurance provider must be notified of claims and how that relates to your knowledge of when an insurable event has happened. For example, if malicious software infiltrated your network two months ago but you just found out about it today, then you can only report it today. Know how your policy would cover that situation. If your policy went into effect last week, would you be covered?

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 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. This issue is one to pay extra attention to if you are considering switching insurance providers because the definitions for reporting periods between different insurance providers may not align.

Be aware of definitions related to internal security control standards that you must maintain as a condition of the policy. Earlier, we described how the underwriting process has become more sophisticated. Insurance companies are expecting customers to have robust internal security in place as a prerequisite for the policy. Unsurprisingly, the insurance company will also expect the insured to maintain those standards over the life of the policy. The definitions are important for making sure the customer understands and meets the requirements. For example, does the policy require that the customer remain current with software updates? Many local governments are not in the habit of applying new patches immediately because of the risk that a patch breaks important operational functions of the software—or because an update might disrupt the integration of software that needs to remain compatible. Hence, it would be important to know what "remain current with updates" means. Gaps in maintaining the standards also arise from renegotiating software contracts, changes in key personnel, and broken equipment. Earlier, we saw how the City of Hamilton's failure to maintain multifactor authentication proved costly.

Key questions to ask: *Do you understand important definitions in your policy, such as requirements to use specified cybersecurity contractors when responding to a breach, notice-of-claims provisions, and security standards?*

* In health insurance, "lasering" means the insurer identifies a specific high-risk individual (e.g., 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.

As evidenced by the limits we just reviewed, even if your policy covers a cyberattack, there is a good chance you may not recover as much as you expected if you don't understand those limits. The savvy customer understands this risk and weighs it when deciding where and when to invest in insurance versus controls.

We'll cover one more potential pitfall of insurance purchasing that stems from customer psychology and purchasing behavior: buying a policy that is overly focused on a narrowly defined risk. Generally, the more focused a policy is on a specific risk, the less beneficial it is for the insured. This is because the customer is insured against a lower-probability event—the narrowly defined risk—instead of a higher-probability event—the broadly defined risk.

Insurance customers can fall into this trap due to what is called "recency bias." Recent events cause people to overestimate how likely a similar event is to occur in the future. A good example is flood insurance. Right after a flood, more people obtain coverage. Years later, many of them let it lapse, even though the underlying risk remains the same. In the cyber world, a local government might experience a certain type of cyberattack and then buy a policy to cover similar attacks in the future. The government may realize lower premiums by buying a narrowly focused policy. However, the likelihood of experiencing any given kind of cyberattack in the future is greater than the likelihood of experiencing the same kind again. In a rapidly changing market, narrow coverage can also be dangerous because the threats are evolving. Local governments should make sure that past firsthand experiences with cyberattacks or stories from peer governments aren't being overweighted when designing or selecting policies to protect against future and evolving risks. If a broader policy is too costly, it might be wise to invest in preventative controls.

Key questions to ask: *Are past, painful experiences with cyberattacks clouding your judgment in preparing for future risks? Is your policy too narrow and not providing adequate coverage for evolving threats? If a broader policy is too costly, would you be better off investing in preventative cybersecurity?*

The end of Step 3 is to ask: What prices or offers can you get from different providers? Working with a good insurance broker is important. Compare providers on:

- **Claims payment history.** Do customers get the coverage they thought they were buying? As we saw, limitations can cause customers to recover less than expected.
- **Pre-breach offerings.** Does the insurer offer useful advice for strengthening your preventative posture?
- **Flexibility on vendor use.** Does the insurer offer a range of contractor options to support you in the event of a breach?
- **Experience in the public sector.** Does the insurer understand the risks that characterize the public sector?

As with most forms of insurance, there may be significant benefits to pooling risk with other local governments, either through self-insurance pools or joint purchasing of commercial insurance.

The quantification of risk discussed earlier can be extended to include commercial insurance policies. The cost-benefit of a policy could be weighed based on its retention and limit. A key nuance, though, is that on average, an insurance policy will be a financial loser for the insured; otherwise, insurance companies would go out of business. But insurance isn't meant to protect against average conditions; it's meant to protect against extreme ones. Therefore, the cost-benefit analysis must examine the value of insurance at the extremes. The GFOA sample ransomware risk model illustrates how to quantitatively analyze the value of insurance in such cases. Also, remember that Appendix 2 includes a questionnaire based on the content we just presented, which can help you evaluate your current cyber insurance strategy.

STEP 4
Periodically Reassess

As cybersecurity threats evolve, a government's posture toward them must evolve as well. Reassessment is critical after an event but should also be done regularly, even if no events have occurred, to maintain security. The Step 4 reassessment can ask many of the same questions asked in Step 1. The goal is to identify new vulnerabilities, perhaps due to:

- Evolving attack methods used by cybercriminals.
- New or modified technologies, operations, or other changes that increase or alter the attack "surface area" presented by the local government to cybercriminals.

The reassessment can also look for opportunities to improve controls as new technologies and methods emerge. This may allow the local government to improve its preventative security posture and reduce reliance on insurance.

Conclusion

Cybercrime is an evolving threat to local governments. Savvy risk management requires making smart use of strategies, including reducing risk through cybersecurity controls, absorbing risk through self-insurance, and transferring risk to the insurance market by purchasing a commercial policy. Below is a recap of the four steps along with the most important actions in each step.

- **Know the basics of their cybersecurity situation.** Understand the most critical IT assets you need to protect and the state of your current cyber security controls.
- **Quantify risk.** Get a sense of where the biggest bang-for-the-buck is in implementing additional security controls. Understand your capacity for self-insurance and. This determines your ability to retain risk on commercial insurance.
- **Examine the potential for insurance.** Make savvy informed decisions about what risks to transfer via commercial insurance and what risks to retain via self-insurance. Use the questionnaire in Appendix 2 to help guide these decisions.
- **Periodically reassess the situation.** Make sure your risk transfer, retention, and prevention strategies are evolving along with the threat environment. Periodically reexamine where you are on each of the three streps above.

CYBERSECURITY FRAMEWORKS

This paper focused on cyber insurance and covered security controls at the most basic level. Additional resources on cybersecurity include the below frameworks:

Framework	Core Structure / Functions	Last Revised	Source
CIS Controls v8.1	18 Controls grouped by Implementation Groups (IG1–IG3): Inventory, Access Control, etc.	June 25, 2024	https://www.cisecurity.org/controls/v8-1
NIST CSF 2.0	6 Functions: Govern, Identify, Protect, Detect, Respond, Recover; 108 subcategories	February 26, 2024	https://www.nist.gov/cyberframework
ISO/IEC 27001:2022	93 controls in 4 themes: Organizational, People, Physical, Technological; Annex A controls	October 25, 2022	https://www.iso.org/standard/27001
COBIT 2019	40 Governance & Management Objectives in 5 domains: EDM, APO, BAI, DSS, MEA	November 2018	https://www.isaca.org/resources/cobit

Appendix 1

DEFINITIONS OF KEY CYBERSECURITY CONTROLS

Zero Trust Architecture. A security architecture that assumes no implicit trust in any actor, system, network, or service, whether inside or outside the organizational perimeter. Instead, every access request must be authenticated, authorized and continuously validated before access to resources is granted.

Network Segmentation. The process of dividing a network into discrete zones or segments (e.g., via VLANs, firewall rules, software-defined network controls) so as to limit lateral movement, contain breaches, and apply differentiated security policies per segment.

Endpoint Hardening. The process of securing endpoint devices (laptops, desktops, mobile devices, servers, IoT devices, etc.) by reducing vulnerabilities: applying security configurations, removing unnecessary services, patching, restricting privileges, enforcing strong authentication, and applying security controls to limit attack surface.

Incident Response Tabletop Exercises. A discussion-based exercise in which personnel with roles and responsibilities in a particular incident response plan meet (usually in a classroom or breakout-group setting) to walk through a hypothetical incident scenario, discuss roles, responsibilities, coordination, decision-making, communications, and validate (or discover gaps in) their incident response procedures.

Multifactor Authentication (MFA). A multilayered approach to security where a second step of authentication is required to complete a transaction. An example of MFA is entering a username and password to log into email as a first step. But the second step of receiving a code to your registered cell phone is required and entered to access the email. The user must enter the code; otherwise, the user cannot access email even if the user enters the correct username and password. MFA is used to prove that the user is legitimate.

Incident Response Planning. Development of a plan based on a risk portfolio of potential cyber events. Each type of risk is typically assigned a priority, and a mitigation strategy is developed for each. Service-level agreements may be applied to outsourced technology services as part of the incident response plan.

Patching Cadence. The established frequency for applying patches or fixes to software and other applicable technologies. The cadence should be considered from two perspectives. A vendor may establish a cadence for normal fixes and bugs. In these cases, the customer (the second perspective) takes into consideration the cadence to apply the fixes. For example, a vendor may release a patch each month while the customer applies them quarterly to ease testing efforts. This strategy should be defined and included in the risk mitigation plan.

Endpoint Detection and Response (EDR). A process of monitoring endpoints of technologies—such as devices and nodes—for suspicious activity and, in most cases, automatically removing the threat. Antivirus software can be considered a simple EDR tool since it is designed to actively monitor a device and remove issues that fit within certain risk categories. Advanced EDRs constantly learn, analyze, and communicate to develop mitigation strategies to respond to evolving cyber threats.

Firewall. A combination of devices and software that separates internal networks from external networks, such as the internet. Firewalls are configured to guard against intrusions and other unauthorized network traffic through device ports and other hardware, software, or telecommunication means.

Training. Almost all cyber incidents start at a system's weakest link—the user. Users should be trained in how to identify suspicious emails, conduct good password practices, use multifactor authentication, and maintain other safe computing practices.

Data Backups. The practice of safely backing up enterprise data according to a defined methodology. This approach is typically based on a risk mitigation strategy that defines the type of data to be protected, the backup frequency, the physical requirements to back up the data, and the disaster recovery response requirements.

Encrypted Storage. The practice of storing data in a format that cannot be read without a key and code interpreter. If stolen, the data cannot be read by criminals and is therefore useless. Encrypted storage is not commonly used since it can slow computing resources during the encryption and reading process. It can also be expensive to encrypt data and store it. Some organizations will select the type of data that is encrypted to avoid latency and minimize costs.

Appendix 2

KEY QUESTIONS FOR THE POTENTIAL FOR COMMERCIAL INSURANCE

Underwriting

Key questions to ask: *How can you make the best impression on your underwriters to convince them you are a good risk? Do you have cost-effective opportunities to improve your security controls?*

Hot Topics to Consider:

- **Do we have essential controls in place?** These include (though not limited to): Multi-factor identification, endpoint protection, regular backups, access control, patch management, incidence response planning, network segmentation, and email / remote access security. Consider using an established cybersecurity framework to guide your control strategy.
- **Are we paying adequate attention to the human element of controls?** At a minimum, this includes training on common attack vectors like phishing and social engineering. Consider the role of simulations to test users' applied skills in cybersecurity and follow up with those that fail the tests.
- **What can we do to stand out as a particularly good risk to insure?** There are many ways to stand out, but a very good place to start is to align your cybersecurity approach with one of the major cybersecurity frameworks we have referenced in this report and make sure your insurance provider knows you are doing it. Demonstrating that you understand and act on risk quantification can also set you apart.
- **What pre-loss services can the insurance company offer?** What proactive services does the insurer provide (vulnerability scans, employee training, tabletop exercises)?

Payouts and Sublimits

Key questions to ask: *What are the sublimits in your policy? Do these sublimits change your understanding of the level of coverage you have? What implication does that have for your investment in cyber insurance (commercial or self-insurance) versus cyber controls?*

Hot Topics to Consider:

- **What is your betterment coverage?** If an attack requires upgrading to a better system, who pays for that?
- **Is pixel tracking / wrongful collection an issue?** Is this an exposure for you (e.g., if you operate websites with embedded tracking pixels)? If so, what is your coverage under a wrongful collection claim?
- **What is our exposure for cascading system failure?** What are the coverage limits for cascading system failure?

Retentions

Key questions to ask: *What balance between retention (self-insurance) and policy price (commercial insurance) is best for you? Is your policy the single highest retention?*

Hot Topics to Consider:

- **What is the limit on the policy?** Deductibles are just one source of retained risk. Be aware of limits. Lower limits aren't necessarily bad – they lower the cost the policy. However, they leave the government more exposed to extreme consequences.
- **Do you have single highest retention or multiple retention?** If an attack triggers multiple coverages, will you pay the deductibles associated with all of the coverages triggered or just the biggest one?
- **What resources do we have available for self-insurance?** This will affect your ability to take advantage of the lower premiums associated with higher retention.

Panel Requirements

Key questions to ask: *What obligations do you have to use a specified security contractor to help respond to a breach? What options do you have to select between contractors?*

Hot Topics to Consider:

- **Do you have a preferred cybersecurity solution provider?** If so, can you have them added to the panel of permissible providers before an incident occurs?
- **What notifications are required before engaging solution providers on the panel?** Make sure you understand what clearances might be needed from the insurance provider before a given type of solution provider (e.g., lawyer) can be brought in to assist with an incident. Build this into your response plan.

Exclusions

Key questions to ask: *What exclusions does the policy contain? What are the exclusions specific to ransomware attacks? What are the exclusions related to potentially overlapping or complementary types of insurance policies?*

Hot Topics to Consider:

- **What is the legal environment around paying a ransom?** Federal and some state laws make paying ransoms illegal, at least in certain circumstance. Be sure to know what laws you are subject to and that your insurance policy and response plan aligns with those laws.
- **What does the policy say regarding systemic events like "acts of war"?** A state-sponsored cyberattack could be considered an act of war, and thereby, potentially, be excluded. What does the policy say about systemic events that impact large numbers of clients all at the same time?
- **What are the important overlaps with other kinds of coverages?** Be sure salient risks don't fall between the cracks of different coverages. Examples include property insurance (cyber-attacks damage equipment that is not normally considered "IT equipment") and crime/fraud (social engineering attacks where the attacker does not directly infiltrate the computer network).
- **Third-party vendors.** Are breaches caused by third-party vendors and/or cloud service providers covered?
- **Have any risks been "lasered" out?** An insurance company could exclude a very specific risk you have that they don't want to insure. Make sure you know what this is and that you are retaining it.

Definitions

Key questions to ask: *Do you understand important definitions in your policy, such as requirements to use specified cybersecurity contractors when responding to a breach, notice-of-claims provisions, and security standards?*

Hot Topics to Consider:

- **What are the notice-of-claims provisions?** Know when you need to report a breach and how the timing of when the breach actually first occurred versus your knowledge of it could impact your coverage.
- **What is your coverage for issues that are discovered after a policy concludes?** Policies sometimes have a "claims made" provision, which means that claims discovered after the policy expiration (but which occurred during the period covered by the policy) are excluded. Do you have provisions to mitigate this, such as an extended reporting period? Do you have retroactive dates on a new policy to cover issues which have already occurred, but which you haven't yet discovered?
- **What security controls are we obliged to maintain?** Some controls might require more definition than others. For example, how quickly do software patches have to be applied?

ENDNOTES

[1] Bischoff, P. (2025, March 18). *Ransomware attacks on U.S. government organizations have cost over $1.09 billion. Comparitech.* https://www.comparitech.com

[2] Information in this paragraph is based on an article written by: Dr. Oren Eytan, CEO of Odi-x. Eytan, O. (2021, June 22). *Municipal cyberattacks: A new threat or persistent risk? Forbes*. https://www.forbes.com/sites/forbestechcouncil/2021/06/22/municipal-cyberattacks-a-new-threat-or-persistent-risk/?sh=673e79ee3ffb. Information is also from personal correspondence between Dr. Eytan and the author of this paper.

[3] National Institute of Standards and Technology. *Definition from the National Institute of Standards and Technology (NIST).* https://www.nist.gov

[4] Derosier, A. (2025, August 29). *St. Paul, Minn., systems come back online after cyber attack. Government Technology.* https://www.govtech.com

[5] City of Columbus. (2025, February 3). *Columbus identifies protected health information from cyberattack.* https://www.columbus.gov

[6] D'Andrea, A. (2025, July 31). *Ontario city facing full $18.3M cyberattack bill after insurer denies claim. Global News*. https://globalnews.ca/news/11313018/hamilton-cyberattack-cost

[7] Fitch Ratings. (2021). *Rising insurance costs add to U.S. public finance cyber pressures* [Fitch Wire]. https://www.fitchratings.com

[8] Aon. (2025, May 14). *Cyber risk insurance market remains buyer-friendly.* https://www.aon.com

[9] Survey conducted by: Center for Digital Government (2021). https://www.govtech.com/cdg

[10] Hubbard, D. W. (2020). *The failure of risk management: Why it's broken and how to fix it* (2nd ed.). Wiley.

[11] Budescu, D. V., Broomell, S., & Por, H. (2009). Improving communication of uncertainty in the reports of the Intergovernmental Panel on Climate Change. *Psychological Science, 20*(3): 299–308. https://doi.org/10.1111/j.1467-9280.2009.02284.x

[12] Hubbard, D. W., & Seiersen, R. (2016). *How to measure anything in cybersecurity risk*. Wiley.

[13] The methods we are referring to are *Monte Carlo analysis and computer simulation.* Insurance companies will vary in the specifics of how these methods are applied. ProbabilityManagement.org. Monte Carlo analysis and computer simulation. https://www.probabilitymanagement.org

[14] The authors would like to acknowledge the attendees of the ProbabilityManagement.org March 2022 conference for their assistance with these answers.

[15] This is known as "overplacement bias," which is a subset of the well-documented psychological phenomenon of "overconfidence bias."

[16] Discussion of insurance industry taken from: Hubbard, D. W. (2009). *The failure of risk management: Why it's broken and how to fix it*. Wiley.

[17] There is no shortage of research that shows quantitative models regularly outperform human judgment. In the context of government finance, see: Kavanagh, S., & Williams, D. (2017). *Informed decision-making through forecasting*. Government Finance Officers Association. This book also discussed relevant research from other fields.

[18] Doug Hubbard suggests three industry-standard resources that function as variable inputs for quantitative models: 1) **The Vocabulary for Event Recording and Incident Sharing (VERIS)**: A common taxonomy that classifies incidents by actor, action, and asset. VERIS ensures that external datasets are compatible with internal risk registers; 2) **The Data Breach Investigations Report (DBIR)**: Published annually by Verizon, this report aggregates global investigation data. It establishes likelihood, providing the empirical "base rates" required to estimate the probability of specific attack vectors within a given industry; and 3) **The Information Risk Insights Study (IRIS)**: Published by the Cyentia Institute, this study focuses on the financial consequences of cyber events. The IRIS report can be used to model impact and capture extreme, high-severity loss events.

[19] NetDiligence. (2025). *Cyber claims study: 2025 report*.

[20] A white paper published by: Sophos. (2021, April). *The state of ransomware 2021*. https://www.sophos.com

[21] Aon. *[Definitions of coverages]*. https://www.aon.com

[22] D'Andrea, A. (2025, July 31). *Ontario city facing full $18.3M cyberattack bill after insurer denies claim.* Global News. https://globalnews.ca/news/11313018/hamilton-cyberattack-cost

[23] An advisory letter from the U.S. Department of the Treasury, Office of Foreign Assets Control Sanctions Compliance and Evaluation Division. (2021, September 21). *Updated advisory on potential sanctions risks for facilitating ransomware payments*. https://home.treasury.gov

[24] National Law Review. (2022, May 2). *North Carolina becomes first state to prohibit public entities from paying ransoms.* https://www.natlawreview.com