Cyber Insurance for Drinking Water and Wastewater Systems

October 2024
EPA-810-F-24-031

WHY SHOULD WATER SYSTEMS CONSIDER CYBER INSURANCE?

Cyber insurance can play an important role in a comprehensive cyber risk management strategy. Cyber incidents can cause significant damage to operations and finances, so water systems must be proactive in protecting their facilities. The benefit of retaining cyber insurance is reducing overall financial risk to cover cybersecurity incidents.

CYBER INSURANCE CAN HELP:

- DRIVE CYBER RISK ASSESSMENT
- SUPPORT INCIDENT RESPONSE
- BUILD RESILIENCE

Cyber insurance protects organizations from the financial impact of cyber incidents and data breaches. It covers costs related to future cyber incident response and system recovery, provides access to experts (e.g., forensics, negotiations, legal, public relations) who can assist in training for and mitigating the impacts of cyber incidents, and bolsters customer confidence that a utility is prepared in the event of an incident. Cyber insurance is a key part of an organization's cybersecurity strategy that also includes proactive cyber risk management, controls, and defenses.

TYPES OF COVERAGE

Standard general liability policies typically have limited coverage for cyber incidents, such as data breaches, and supplementary policies may be required for more specialized coverage. In general, if cyber coverage is not explicitly included in your policy language, it is excluded. For example, ransomware may require a separate coverage and should be explicitly stated in the policy language. Cyber insurance policies generally cover first-party losses and third-party claims as a result of a cyber incident on a system or network.

- First-party cyber coverage protects you from costs associated with your data, including employee and customer information. This coverage typically includes your business's costs related to:
  - Crisis management expenses, such as:
    - Legal counsel
    - Breach notification, credit monitoring, and call center services
    - Forensic services to investigate the breach
    - Public relations
  - Recovery and replacement of lost, corrupted, or stolen data
  - Cyber extortion (e.g., ransomware)[1]
  - Denial of service (Verizon DBIR Report 2024)
  - Lost revenue and extra expenses due to business interruption
  - Policies may also cover lost revenue associated with a business interruption of a company on which you depend
- Third-party cyber coverage generally protects you from liability if a third party brings claims or a regulatory action against you. This coverage typically includes:
  - Claims and settlement expenses
  - Costs for litigation and responding to regulatory inquiries
  - Attorney and court fees
  - Compensatory damages, settlements, and court judgments
  - Civil regulatory fines and penalties

IMPORTANT CONSIDERATIONS FOR YOUR POLICY:

- Name of insured entity and subsidiaries covered
- Understand the steps required to submit a claim
- Preferred Breach Response Providers and Counsel

EXCLUSIONS

Like all insurance policies, certain losses are excluded from cyber insurance. Cyber insurance will typically not cover losses associated with or incidents derived from:

- Social engineering [2]
- Property damage (e.g., cyber event causing physical damage to a building)
- Value of intellectual property
- War
- Cost for proactive preventive measures (e.g., training staff, Virtual Private Network setup)
- Bodily injury
- Upgrades and improvements
- Loss due to the outage of public utilities you rely on (e.g., local power company)

It is critical that you review the terms and conditions of your policy and understand all applicable coverages and exclusions. Periodic review of your policy and coverage is also recommended.

WHAT TO EXPECT IN THE UNDERWRITING PROCESS

Insurers use the underwriting process to assess your organization's risk and evaluate exposures. The process can also help you better understand your cyber risk profile relative to your peers and model losses. The application process typically involves a thorough assessment of the measures that your organization has in place to protect against cyber incidents and mitigate their impact. Water systems are also encouraged to take actions to reduce cyber risk, improve resilience to cyber incidents, and utilize free services (Top 8 Fact Sheet). Underwriting questionnaires are not harmonized across the industry, but insurers typically inquire about:

- Multi-Factor Authentication (MFA)
- Security awareness training and testing
- Data backups
- Endpoint detection and response/managed detection and response
- Vulnerability management (for computer and network security)
- Incident response and business continuity plans
- Third-party vendor management program

1 The U.S. government strongly discourages the payment of ransoms. Every ransomware incident should be reported to the U.S. government. Victims of ransomware incidents can report their incidents to the FBI and CISA. A victim only needs to report their incident once to ensure that all the other agencies are notified. You can report a ransomware incident to the FBI through the Internet Crime Complaint Center or through CISA's reporting tool. Visit StopRansomware.gov for more information and resources to prevent ransomware attacks.

2 Social engineering may be excluded and/or it may be an optional add-on to the cyber insurance policy. Check to see if the policy that you are considering includes this coverage and discuss options with your insurer.

- Firewall protection of company network
- Central patch management (to ensure critical updates are applied in time)
- Cybersecurity governance (who manages cyber risk for your organization?)
- Cybersecurity policies and procedures

APPLICATION

Underwriting applications or questionnaires can be lengthy, as insurers attempt to better understand your organization's operations and cybersecurity posture. An insurance application may inquire about:

- Security controls
- Operational Technology (OT)
- Information Technology (IT)
- Water rate revenue and service area
- Amount and type of Personally Identifiable Information (PII) or sensitive data held
- Claims activity
- Cybersecurity governance
- Third-party vendors
- Patch management protocols and disaster recovery architecture

ASSEMBLING YOUR TEAM

Identify who should be involved in the underwriting process to ensure that those with knowledge of your organization's operations and cybersecurity measures are represented. In a small utility, this might be a superintendent and an IT/OT contractor. In a large utility, several team members may be involved in the underwriting process, including:

- Risk Manager
- Chief Financial Officer (CFO)
- Chief Information Security Officer (CISO) or Chief Information Officer (CIO)
- General Counsel
- Third-party IT Representative
- Communications Manager

RIGHTSIZING THE POLICY

Assessing your organization's cyber risk and risk tolerance is important when considering how much cyber insurance is necessary and what types of coverage are beneficial. When considering how much insurance is needed, think about the financial impact to your organization if a cyber incident exposed customer data, corrupted systems and data, or shut down operations.

- What will it take to get your facility back up and running?
- Who needs to be involved?
- What is your litigation risk?
- How much risk are you willing to absorb through a deductible?

Depending on the size of the facility, coverage needed, and the level of risk, insurance companies can design a policy that will specifically meet the needs of your water system. There are many insurance specialists that can help you assess your cyber risk and recommend policy amounts, terms, and conditions within your budget.

RESOURCES

- EPA Cybersecurity for the Water Sector
- CISA Water and Wastewater Cybersecurity
- Cyentia Institute: Information Risk Insights Study
- Loss Magnitude Estimation in Support of Business Impact Analysis

FREQUENTLY ASKED QUESTIONS

WHAT IMPACTS MY ORGANIZATION'S PREMIUM?

A number of factors impact the premium of a cyber insurance policy, including your cyber controls, risk profile, claims history, coverages, limits, and deductible, as well as the overall cyber threat landscape. Depending on your location and affiliation, you may have the option to purchase cyber insurance through a state entity, pooling agreement, or trade association, which may help reduce costs. Options could include:

- Co-operatives
- Municipal or county pools
- Trade groups
- County associations (add-on policy)
- Umbrella policies
- State-level policies

ONE OF OUR SYSTEM'S INSURANCE POLICIES MENTIONS COVERAGE FOR CYBER LOSS AND DATA BREACHES. DO WE NEED A STAND-ALONE CYBER POLICY?

Cyber risk can be covered under multiple insurance policies. However, this coverage may not be as comprehensive as a stand-alone cyber policy. Examine the terms and conditions listed within your organization's policies. The following may cover cyber-related incidents:

- Kidnap and Ransom (K&R) or "Special Crime" Insurance
- Property Insurance
- Crime Insurance
- Business Owners Policy (BOP)

AFTER PURCHASING CYBER INSURANCE, DOES MY UTILITY NEED TO SPEND MONEY AND TIME ON OTHER CYBER MITIGATION MEASURES?

Yes, while cyber insurance can be beneficial, it should only be a small part of your overall cybersecurity plan.

WHAT DO WE DO IF WE ARE BREACHED?

Contact your insurance company immediately, as they may have a preferred list of vendors you can use under the policy. The contact information for the insurance provider should be included in your incident response plan.

Scan QR code for web version of this fact sheet

Acknowledgements: *This factsheet was generated by a work group composed of representatives from the U.S. Environmental Protection Agency (EPA), Office of National Cyber Director (ONCD), Association of State Drinking Water Administrators (ASDWA), Cybersecurity and Infrastructure Security Agency (CISA), North Dakota Insurance Reserve Fund (NDIRF), South Central Connecticut Regional Water Authority, Water Information Sharing and Analysis Center (WaterISAC), and Water Sector Coordinating Council (WSCC).*

EPA

October 2024
EPA-810-F-24-031