Public Entity Cyber+ Liability℠ Protection

Claim Scenarios

Third-Party Coverages

Network and Information Security Wrongful Acts

Privacy: A hacker infiltrates the Web site of a large municipality, gaining access to the credit card numbers of 10,000 of its community members who pay their utility bills online. The municipality faces claims from the community for unauthorized charges made on their credit cards, as well as claims from the banks to cancel and reissue the credit cards.

Transmission of a Computer Virus: A county employee opens an attachment to an email that contains a computer virus. The virus infects the county’s computer system and then is inadvertently transmitted to third parties via email, causing some of them to shut down operations. The county faces claims from the third parties’ lost profits and expenses associated with the malfunction of their computer systems due to the virus transmission.

Failure to Provide Authorized Users With Access: A new city subdivision is under development and building contractors are working under tight deadlines. As part of the city’s efforts to become technologically advanced, permit applications are only taken through its online permit service. The city’s computer system malfunctions and shuts down for three weeks, preventing permit applications from being submitted. The shut down causes the construction project to be delayed and results in financial loss to the contractors. The city faces claims for the contractors’ financial loss associated with the city’s failure to provide access to its online permit service.

Communications and Media Wrongful Acts

Copyright or Trademark Infringement: While preparing marketing materials for a new program, a county employee comes across useful logos and diagrams from a private company’s Web site and incorporates them into the program materials. The county faces claims by the company for copyright or trademark infringement.

Plagiarism: A police department decides to implement risk management best practices following a risk management seminar offered by a local insurance agency. In order to save time and money, a department employee copies the information contained in the agency’s seminar handouts and incorporates them into the department’s new risk management program. The police department faces plagiarism claims brought by the agency.

Optional First-Party Coverages

Security Breach Notification Expenses Coverage

Crisis Management Service Expenses Coverage

A city employee leaves his laptop at the airport, where it is stolen. The thief subsequently gains access to the computer’s hard drive and obtains sensitive personal information about the city’s taxpayers. As a result, the city incurs significant security breach notification expenses to identify and inform the affected individuals of the breach, as well as other expenses necessary to comply with security breach notification laws. The city also incurs crisis management service expenses in hiring a public relations firm to mitigate the negative publicity generated from the security breach and to regain the trust of its community.
Public Entity Cyber^ Liability℠ Protection Resource Guide

- Potential Vulnerabilities in Municipal Communications Networks, A US-CERT Informational Focus Paper – www.us-cert.gov/control_systems/csarchive.html. On the Control Systems Highlights page, scroll down to 12/5/06 report prepared by the National Cyber Security Division, Control Systems Security Program, of the US Government. It outlines potential exposures and key areas on which public entities can focus to protect data assets. Additional information can be found under Control Systems Standards & References, accessible from the left navigation bar.

- www.truste.org – TRUSTe (a leading organization in privacy). Select Privacy Resources section of the home page to access the following resources. Other information is available as well.
  - Privacy Policy Whitepaper – Information about drafting or updating an online privacy statement. A privacy statement or privacy disclosure statement tells web site users how their personal information is used by the entity. The whitepaper also provides sample disclosure wording.
  - Forrester Report – Privacy Seals: Opt In Or Opt Out? – explains the use of privacy seals which serve to verify to web site users that an entity has exceeded minimum guidelines regarding the business process by which it addresses the collection and use of users’ private information.
  - Security Guidelines – provides general guidelines around web application data security.

- www.sans.org – SANS Institute (a leading organization in computer security training). Select Security Policy Samples option under the Free Resources section of home page for links to the following resources. Additional information is located in the Reading Room of Free Resources.
  - Policy Primer – “A Short Primer for Developing Security Policies”
  - Examples & templates for various types of policies


- Information Compromise and the Risk of Identity Theft: Guidance for Your Business – www.ftc.gov/bcp/edu/pubs/business/idtheft/bus59.shtm. FTC guidance on actions entities can take if personal information of others has been compromised.

For more information, call your independent agent/broker or Public Sector Services Territory Manager at Travelers.