TRIDENT
PUBLIC RISK SOLUTIONS

Member Argo Group

New Data Compromise and Cyber Coverage Helps Protect Governments

GOVERNMENTS OF ALL SIZES FACE AN INCREASINGLY PERVASIVE THREAT: CYBERATTACKS. BUT TRIDENT PUBLIC RISK SOLUTIONS HAS THE TOOLS TO HELP REDUCE THEIR EXPOSURES.

Whether it's a data breach involving hacked, stolen or lost information, a computer attack, or an extortion attempt, local governments can fall prey to cybercriminals in a variety of ways.

Trident understands these threats, which is why it has developed a comprehensive coverage platform to help governments respond to an attack while also giving them the tools to bolster their defenses.

Introducing Data Compromise 360©, which is designed to help local governments respond to data breaches, and Cyber Coverage 360©, which helps local governments respond to computer attacks and cyber extortion.

Data Compromise 360©

Data Compromise 360© was designed to help local governments respond to the financial burden and service obligations a data breach can cause.

The discovery of a personal data breach triggers this coverage, which includes:

- Payment of first-party expenses incurred from responding to a personal data breach. That includes outside legal counsel, a forensic IT review, public relations costs, notifications, reimbursement for fines and penalties, and credit monitoring and other services for those affected.
- Defense and liability costs for actions brought by those impacted or government entities.

Cyber Coverage 360©

Cyber Coverage 360© is an insurance solution provided by Trident that is designed to help local governments respond to cyber exposure incidents such as computer attacks, cyber extortion, network security liability and electronic media liability.

It provides first-party and third-party liability coverage that's triggered when an insured discovers an attack on an owned or leased computer.

Coverage for computer attacks includes:

- Data restoration costs – coverage for the cost of a professional firm hired by the insured to replace lost or corrupted data from electronic sources.
- System restoration costs – coverage for the cost of a professional firm hired by the insured to restore its computer system by replacing or reinstalling software, removing malicious code, and correcting the configuration of the insured's computer system.

Coverage for cyber extortion incidents includes:

- The cost of hiring a professional firm – coverage for a firm hired by the insured to investigate and negotiate a cyber extortion threat, which is deemed a credible threat, or series of threats to launch a potential denial-of-service attack.

TRI-7929-040218

Claims Examples

Who: county law enforcement agency

What: A cybercriminal who hacked into a sheriff's department data system held sensitive information for ransom until certain demands were met. The hacker extorted funds from the county by locking up sensitive data with ransomware nationally known as CryptoWall, which encrypts files on a compromised computer.

Cost: $1,000 ransom plus $3,000 for system restoration

Who: school district

What: A spear phishing email purportedly from a district superintendent resulted in the release of personally identifiable information on more than 1,500 employees.

Cost: $125,000 for breach notification and two years of identity protection

Who: city's financial and public safety operations

What: A phishing scheme – a weaponized document spread via email – resulted in the finance department being unable to execute external banking transactions. Additionally, 185 surveillance cameras were impacted, and the police department could not access its databases.

Cost: $185,000 for the initial emergency response plus between $800,000 and $900,000 to fully remediate the damage

Who: parks and recreation

What: A laptop containing personally identifiable information on 250 summer sports registrants was stolen from an office.

Cost: $25,000 for credit reporting and monitoring

Gain Access to Valuable Online Resources

Another benefit of Data Compromise 360© and Cyber Coverage 360© is access to Trident's eRiskHub® portal, an online resource for training, best practices and other risk management tools for cyber exposures.

This easy-to-use website includes:

- Notification requirements.
- Self-assessments.
- A step-by-step guide on what to do following a data breach.
- Online training modules.
- Risk management tools.
- A directory to quickly find external resources, including industry links.
- The latest news on cyber risk and security and links to compliance blogs.
- A learning center including best practices and white papers written by leading authorities.

To learn more about eRiskHub®, contact your Trident territory marketing manager.
Visit www.argolimited.com/trident/contact to see a staff directory.