# RANSOMWARE – THE THREAT IS REAL

Controls and coverage are necessary to protect public entities from liability.

BY LISA HAMMOND

**CYBERCRIMINALS HAVE WREAKED HAVOC** on local governments in recent years, primarily through costly ransomware attacks. Ransomware is the fastest growing type of cybercrime, and because public entities are especially vulnerable, they continue to face the real and ever-increasing threat of this type of attack.

In a ransomware attack, cybercriminals infect a public entity's computer system with malware, software most often installed when an employee opens a "phishing" email and unwittingly clicks on a malicious link or attachment. The malware encrypts the system's data, restricting the entity's access to it. The criminals then demand a ransom to restore the data, usually threatening permanent destruction of the data unless the ransom is paid.

## PUBLIC ENTITIES ARE SOFT TARGETS FOR RANSOMWARE ATTACKS

Cybercriminals consider public entities soft targets because their defenses are often inadequate to repel their ever-evolving and expanding attacks. They know many public entities operate on tight budgets and lack the funding to develop a robust defense.

Many public entities are vulnerable to attack because they do not:

- Have staff with cybersecurity expertise (the cybersecurity skills shortage disproportionately affects the public sector because it has more difficulty attracting talent than the private sector)
- Make necessary upgrades to their IT systems and equipment
- Identify and correct vulnerabilities
- Operate secure backup systems
- Provide ongoing security awareness training for all employees
- Invest in cyber insurance

Cybercriminals also understand that public entities provide critical services that, when interrupted, cause major disruption and public safety concerns. This creates an urgency for public entities to pay the ransom in the hopes of restoring their systems as quickly as possible.

## WAYS PUBLIC ENTITIES CAN IMPROVE SECURITY—AND INSURABILITY

Public entities can mitigate the increasing costs of cyberattacks and cyber insurance by implementing these security measures:

- Two-factor or multi-factor authentication (MFA)
- Updated antivirus and anti-spyware software (antivirus software should include firewall protection)
- Encrypted data storage and data backups
- Software patching
- Vulnerability testing and endpoint detection response (EDR)
- Ongoing security training for employees that includes strong password practices and how to identify phishing emails
- Hardware and software inventory (uninstalling unused software, updating outdated software, and replacing equipment every three to five years)
- Rapid response plan in place in the event of a breach, including identifying a response team, including vendors and template notifications for quick access
- Improved physical security, including restricted access to buildings and server rooms and use of surveillance cameras
- Protected personally identifiable information (PII) encryption and a policy that outlines the handling and sharing of PII
- Monitored email traffic
- An isolated area on the network for public access (where applicable)
- Prohibited use of personal drives on business equipment
- Virtual private network (VPN) for remote access
- Social media policy outlining acceptable use for computer equipment
- Protocol for reporting security incidents (including language about internet safety, downloading software, accessing unauthorized websites, and guidelines for the secure handling of payment cards, such as using chip technology instead of magnetic strips)
- Vendor security controls, including a process to terminate vendor, contractor, and temporary employee accounts at the end of their contract
- Secure electronic records storage and a record destruction policy

Public entities should assess and regularly reassess opportunities to improve controls as technologies can change rapidly.

Other contributing factors to public entities' vulnerability include:

- Transparency requirements
- Storage of personal information, tax records, and other sensitive information
- 24/7 availability requirements for networks and applications so constituents can access resources and conduct transactions (making it challenging to take systems offline for maintenance)

An evolving issue is federal and state government policy on responding to ransomware attacks. While an affected entity may believe it is in its best interest to pay the ransom, doing so presents a collective problem. When a single victim pays ransom, it encourages cybercriminals to launch more attacks. Federal law enforcement officially discourages ransom payments. In April 2022, North Carolina became the first state to prohibit state agencies and local governments from paying ransoms.

## IT'S PREVALENT BECAUSE IT'S PROFITABLE

Ransomware is an extremely profitable crime, and the number of attacks is dramatically increasing. Reports indicate that in the U.S., cybercriminal black markets can be more profitable than illegal drug trafficking. Given the significant revenue that can be generated by cybercrime, cybercriminals are often well-funded and well-organized, financing their abilities to swiftly conduct sophisticated attacks.

Cybersecurity Ventures, a researcher and publisher covering the global cyber economy, predicts that the global cost of ransomware will exceed $265 billion by 2031, with an attack carried out every two seconds, up from every 11 seconds in 2021.

It is critical that public entities identify and address vulnerabilities *before* an attack happens. Whether an entity pays the ransom or expends considerable time and resources to restore access, a ransomware attack can be an extraordinary expense and seriously impact operations for weeks and even months.

The cost of an attack on a public entity is also not limited to the ransom demand. Costs can also include forensic investigations, system recovery services or new systems, claims services and related expenses, improved security, cybercrime prevention and response measures, and lost or delayed revenue.

## INCREASING ATTACKS LEAD TO CHANGES IN THE CYBER INSURANCE MARKET

More frequent and costly ransomware attacks, spiking insurance claims, and increased demand for coverage have led to changes in the cyber insurance market.

Cyber insurance premiums have risen, coverage limits have changed, and insurers are requiring stricter security controls before issuing or renewing policies. Without certain controls, an entity may be considered uninsurable. See the sidebar on p. 7 for controls public entities can implement to help improve their insurability for cyber coverage.

## CYBER INSURANCE COVERAGE SHOULD BE PART OF EVERY DEFENSE PROGRAM

Public entities' commercial general liability policies *do not* cover cyber liability, and errors and omissions insurance is *not* cyber insurance.

Cyber insurance is purchased as either a standalone policy or as an extension to another policy. The range of cyber risk is broad, and not all risks may be covered by cyber policies. Coverage can vary significantly between different insurers and different policy forms.

Cyber insurance policies typically include coverage for:

- Cyber extortion
- Data restoration
- Loss of income and extra expenses
- Crisis management costs, including notification and IT forensics expenses
- IT security liability
- Privacy liability
- Confidentiality liability
- Data protection regulatory fines and costs

Policies may also include additional coverages such as:

- Network security and privacy liability
- Electronic media liability
- Regulatory proceedings

Public entities should always discuss cyber coverage and policies with their insurance agent.

*Lisa Hammond is risk control and business development manager of Tokio Marine HCC's Public Risk Group.*

## CYBERSECURITY RESOURCES FOR PUBLIC ENTITIES

**CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY (CISA)**
www.cisa.gov/free-cybersecurity-services-and-tools

**NICCS – CISA GLOSSARY OF CYBERSECURITY WORDS AND PHRASES**
niccs.cisa.gov/cybersecurity-career-resources/glossary

**U.S. GENERAL SERVICES ADMINISTRATION**
gsa.gov/technology/government-it-initiatives/cybersecurity/cybersecurity-programs-policy

***GOVERNMENT TECHNOLOGY* MAGAZINE**
govtech.com/tag/cybersecurity

**FEDERAL TRADE COMMISSION**
ftc.gov/business-guidance/small-businesses/cybersecurity/cyber-insurance

**GOVERNMENT FINANCE OFFICERS ASSOCIATION**
gfoa.org/cyber-insurance