TRAVELERS

5 Cyber Readiness Practices for Public Entities

1 Implement Multifactor Authentication (MFA)

MFA includes the use of two or more authentication factors to verify a user's identity prior to allowing access to IT resources. Factors can include:

- Information only the user knows, such as a password or passphrase.
- A token, smartcard or device.

99.9%
of account compromise attacks can be prevented by using MFA.*

2 Keep Systems Current

Apply the latest patches for security weaknesses in order to:

- Help track, obtain and validate available patches.
- Permit priority-based patching, with critical patches being applied as soon as possible.
- Perform reporting and auditing to detect if a patch fails anywhere on the network.

3 Use Endpoint Detection and Response (EDR)

To help provide advanced, automated detection of suspicious activity, intrusions and attacks in real time and protect endpoints, including:

- Network servers and hardware
- Internet of Things (IoT) devices
- Cloud-based apps
- Operational technology (OT)
- Mobile and desktop devices

4 Have an Incident Response (IR) Plan

To limit the damage and lessen the time it takes to return to "normal" operations following a cyber incident, an incident response plan should outline:

- **WHO** does what
- **HOW** it gets done
- **WHEN** it gets done

5 Back Up Data

Adopt a 3-2-1 strategy to reinforce your data:

Investing in cyber insurance can be a smart strategy, too.

Travelers CyberRisk is a modular cyber insurance solution for public entities, offering **16 insuring agreements**, including potential coverage for:

- Liability
- Cybercrime
- Business loss
- Breach response

To learn more about cyber insurance for public entities, visit: travelers.com/cyber-insurance/public-sector.

*https://www.travelers.com/iw-documents/travelers-institute/TravelersInstitute-US-CybersecurityGuide.pdf