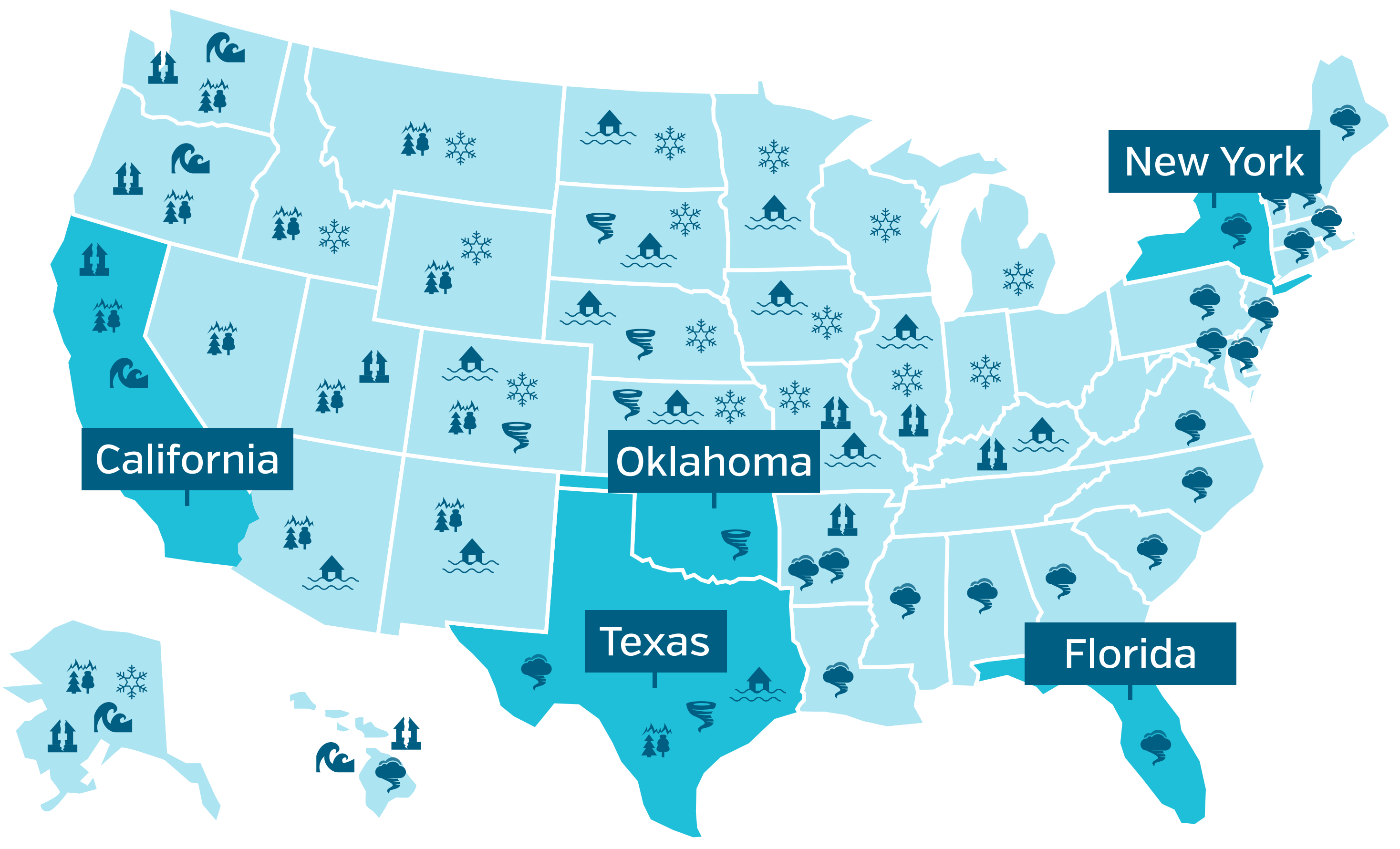
When Mother Nature Strikes:

Protecting Your Business Data

Natural disasters can have a devastating impact on your small and medium-size business (SMB)—and the valuable company, employee and customer data it holds. Take steps now to understand and mitigate your risks in order to preserve business continuity and your company's brand.

Disasters That Put You at Risk



- Blizzards
- Earthquakes
- Floods
- Hurricanes
- Ice Storms
- Nor'easters
- Thunderstorms
- Tornadoes
- Tsunamis
- Volcanoes
- Wildfires

Top 5 States with Presidential Major Disaster Declarations

1	Texas	86 major disasters
2	California	78 major disasters
3	Oklahoma	73 major disasters
4	New York	67 major disasters
5	Florida	65 major disasters

Small and Medium-Sized Business Risks

SMB Risks

43%
Of businesses have a disaster recovery plan

94%
Of small businesses back up critical financial data to prepare for an emergency, but ...

4 in 10
Of those small businesses keep the data off-site

Post-Disaster Impacts

1 in 4
The number of SMBs that don't re-open after a major storm

84%
The percentage of SMBs that don't have disaster insurance

1 in 3
The number of SMB owners who are personally affected by a storm or extreme weather

$3,000
PER DAY
The average amount lost per day for SMBs after closing post-storm

Disaster Planning

Perform an information inventory

1. Locate data types
2. Prioritize business information that is most critical to running a business
3. Address type of protection data needs: confidentiality, integrity, availability

UPS

Install Uninterruptible Power Supplies (UPS) on computers and critical network components

3-2-1 Rule for Backing Up Data:

1. Keep three copies–one primary, two backups–of your data available.
2. Retain two backup copies on different media.
3. Store one backup copy offsite.

How to Protect Your Business Data

10 Tips SMBs Must Absolutely Follow:

1. **Use anti-virus, anti-malware and anti-spyware on every device.**
2. **Provide security for your internet connection.**
3. **Install and activate software firewalls on all systems.**
4. **Patch operating systems and applications.**
5. **Make backup copies of important data. (See 3-2-1 Rule)**
6. **Control physical access to computers and networks.**
7. **Secure wireless access point and networks.**
8. **Provide employee security training on a regular basis.**
9. **Require individual user accounts for each employee on business computers and for business applications.**
10. **Limit employee access to data and limit authority to install software.**

For more information on data breach protection, please contact your agent.

Sources:
Small Business Information Security: The Fundamentals, National Institute of Standards and Technology, U.S. Department of Commerce, 2009; "Top Natural Disasters That Threaten Business," EKU Online, http://safetymanagement.eku.edu/resources/info-graphics/top-natural-disasters-that-threaten-businesses/.

IDT911