The main root causes of a data breach in the U.S. are malicious/criminal attack, human error and system glitches.1

Any organization that retains physical or electronic records of employees, customers, or other third parties is vulnerable and can be a victim of a cyber event.

95% of businesses rely on their computer systems functioning properly for their business to operate.2 If systems go down due to a glitch, error or attack businesses can be at risk of suffering loss of income and customers.

Ransomware is evolving and becoming more advanced with infections up 40% within the past year.3 Extortion events can have a significant impact on businesses' operations and often require payment of ransom to regain access to data and systems.

49% of organizations with at least one significant attack were successfully attacked again within one year.4

CyberRisk coverage is specifically designed to help in the event of a cyber breach and is available for businesses of all sizes. And CyberRisk protection doesn't end after a breach occurs. New to CyberRisk is betterment, an insuring agreement that provides coverage for costs to improve a computer system after a security breach, when the improvements are recommended to eliminate vulnerabilities that could lead to a similar breach.

In addition to coverage, Travelers provides policyholders pre-breach and post-breach risk management services at no additional cost. These include access to pre-breach services provided by Symantec™, a global leader in cybersecurity solutions and access to Travelers' eRiskHub® an information portal of risk management tools powered by NetDiligence®.

1 Ponemon Institute® 2018 Cost of Data Breach Study: Global Overview
2 Travelers Risk Index 2018
3 Symantec™ Internet Security Threat Report, Volume 23, April 2018
4 Mandiant M-Trends® 2018