HOW IS **BUSINESS EMAIL COMPROMISE** PUTTING MY COMPANY AT RISK?

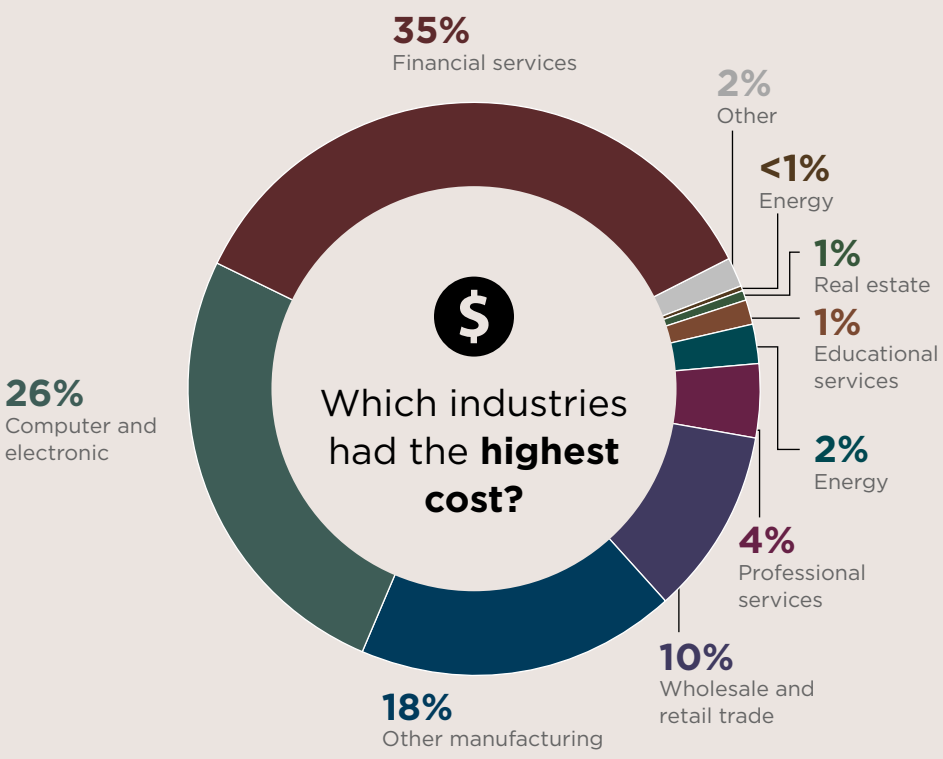
Business Email Compromise (BEC) is a sophisticated scam targeting organizations to fraudulently induce their employees to make funds transfer payments as a result of an impersonation of an employee, vendor or customer.

It is carried out when a legitimate business email account is compromised through social engineering or computer intrusion techniques.

BEC can occur through:

- Businesses working with a foreign or domestic supplier
- Business executives receiving or initiating a request for a wire transfer
- Business contacts receiving fraudulent correspondence through compromised email
- Business executive and attorney impersonation
- Data theft

BEC Cases from 2008 to Present



Which industries were **targeted the most**?

Who was targeted **within a company**?

Who was being **impersonated**?

Crime and Fidelity insurance can help insure against such loss when an organization's defenses have been penetrated and an unrecoverable, direct financial loss has been suffered. This insurance can be provided in the form of tailored coverage against loss from **"Social Engineering"**, also known as **"Fraudulently Induced Funds Transfers"**.

For more information on how Nationwide can provide specialized cyber and fidelity commercial crime insurance and loss prevention expertise, visit Nationwide-mls.com or contact James Kardaras, Underwriting Director, Crime and Fidelity at **james.kardaras@nationwide.com**.

Nationwide® is on your side

Advisen Transforming • Insurance™

A.M. Best Rated A+ XV | S&P A+ | Fortune 100 Company

1. Based on Advisen Ltd. data from 2008-present;
2. Sources: https://www.ic3.gov/media/2017/170504.aspx