



# Social Engineering:

What is it?

Should you be worried about it?

How can you mitigate your risk of an incident?

*Presented By:*  
*Brown & Brown Executive Risk Team*

*Hays Companies, Inc., an owned  
subsidiary of Brown & Brown, Inc.*



# Presentation Agenda



1

**Elements of Social Engineering**

2

**Coverage and Claim Issues**

3

**Mitigation Tools/Best Practices**

4

**Q&A**

# Panelists



**Aaron Stone**

*Brown & Brown, Moderator*



**Alyssa Turek**

*Brown & Brown, Panelist*



**John Barker**

*Beazley, Panelist*



**Carolyn Purwin Ryan**

*Mullen Coughlin, Panelist*



**01**

# Elements of Social Engineering

# What is Social Engineering?

- Criminal enterprise
- Psychological manipulation – **not** a breach incident
- Referred to as “human hacking”

## How

- Communication
- Gain Trust
- Deceive
- Only needs to work against a **single** individual



## Why

- Gain passwords and/or credentials
- Money
- Information
- Reputational Harm



# How is it Manifested?

---



## Email

- Trusted source
- Link/Download
- Phishing



## Telephone/Verbal

- TA Access to System by Fake Subscription Method
- Request to Access



## Wire Transfer Fraud



# Economic Impact

---



## Loss Estimates

- Ranked as #1 type of attack in 2022
- Average organization has 2 attacks per day
- Internet Crime Complaint Center reported nearly \$2.4B in adjusted losses in 2021

## Carrier Impact

- Loss leader for some carriers
- Impacts all industries and organization sizes- causes underwriting issues
- Many carriers offer risk management resources and loss prevention programs for their policy holders

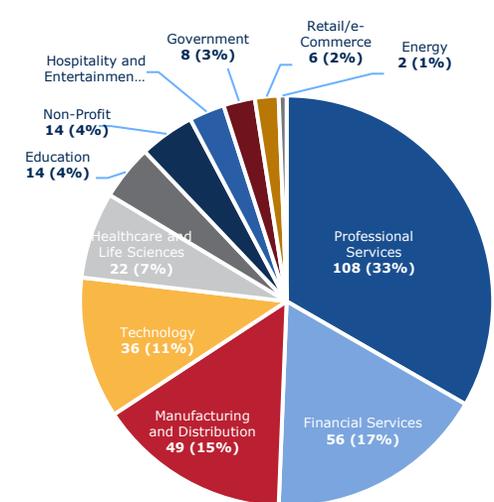
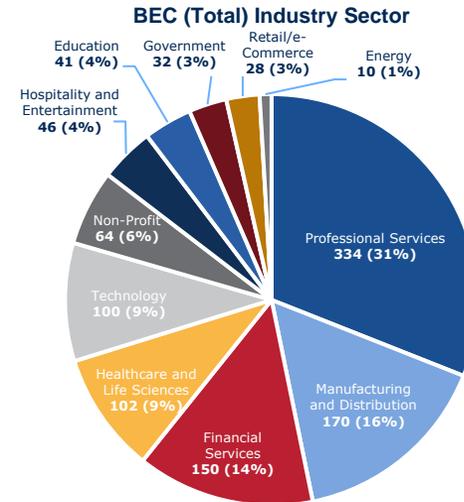
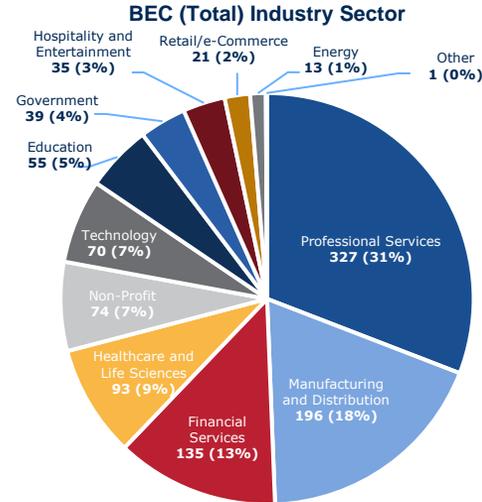
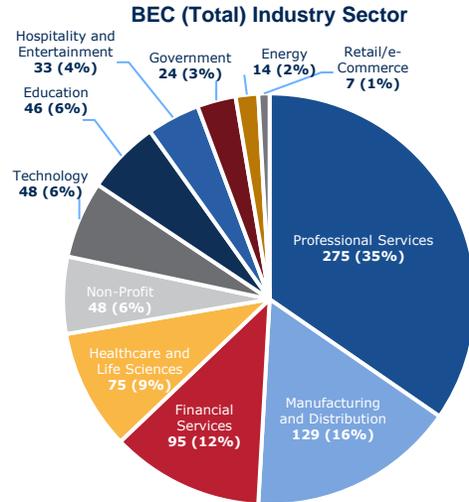
# Business Email Compromise Incidents

| 2020                              |           |
|-----------------------------------|-----------|
| Number of BEC Incidents           | 794 (23%) |
| Number of BEC-WF Incidents        | 187 (24%) |
| Average Amount Fraudulently Wired | \$392,482 |
| Median Amount Fraudulently Wired  | \$100,000 |

| 2021                              |             |
|-----------------------------------|-------------|
| Number of BEC Incidents           | 1,059 (27%) |
| Number of BEC-WF Incidents        | 361 (34%)   |
| Average Amount Fraudulently Wired | \$343,303   |
| Median Amount Fraudulently Wired  | \$131,440   |

| 2022                              |             |
|-----------------------------------|-------------|
| Number of BEC Incidents           | 1,077 (36%) |
| Number of BEC-WF Incidents        | 344 (32%)   |
| Average Amount Fraudulently Wired | \$376,234   |
| Median Amount Fraudulently Wired  | \$145,000   |

| 2023 (through Q1)                 |           |
|-----------------------------------|-----------|
| Number of BEC Incidents           | 324 (33%) |
| Number of BEC-WF Incidents        | 94 (29%)  |
| Average Amount Fraudulently Wired | \$999,726 |
| Median Amount Fraudulently Wired  | \$152,000 |



**02**

## **Coverage and Claim Issues**

# What Coverage is Available?

---

## Social Engineering Fraud

- Reimburses an insured for the loss of funds due to phishing of an employee.
- Coverage can be found on a cyber or commercial crime policy.

## Funds Transfer Fraud

- Reimburses an insured for the loss of funds due to phishing of a financial institution.
- Coverage can be found on a cyber or commercial crime policy, but typically broader on crime.
- These are rare as financial institutions tend to have enhanced layers of due diligence.

## Invoice Manipulation

- Reimburses an insured for the loss of funds due to a change of an issued invoice.
- Coverage can typically only be found on a cyber policy or by endorsement.

## Fraudulent Instruction

- Carrier reimburses losses that an Insured transfers to a bad actor after they receive “updated” fraudulent payment instructions.
- Out of band authentication exclusions can apply if a second means of verification were not used, but this exclusion is often endorsed out.
- Often sub-limited as usually found on both cyber e-crime and crime policies.

# Claim Issues

---

## Confirming Cause of Loss and Validating Amount of Loss

- Carrier investigation
- Proof of Loss process
- Coverage review and potential exclusions
- Coverage determination

## Coordination of coverage

- What happens when both a Cyber and a Crime policy are triggered?
- Primary, excess and mutually repugnant policies.

## Subrogation

- Early involvement of Law Enforcement will maximize potential recovery
- Obligation to cooperate with carrier



# Carrier Issues

---

## Rates and Terms

- Crime Coverages Typically Unavailable for Financial Institutions or Similar Industries on a Cyber Placement
- Sub-limits Typically Range from \$50K – \$250K
- Narrow Language May Apply Requiring a Call Back Verification to Pre-Determined Number for Coverage to Apply

## Underwriting Friction

- Most Carriers Won't Offer Cyber Crime Coverages Without Appropriate Controls in Place (i.e., employee phishing training and simulations, callback verification procedures, etc.)

## Crime vs. Cyber

- When Duplicative Coverage is Found on Both, the Recommended Strategy is to Pre-Negotiate Which Policy is Primary & Excess at Renewal/in Advance

## Development of a stand-alone product?

**03**

## **Mitigation Tools/Best Practices**

# Mitigation Tools/Best Practices

---

- Employee awareness
- Training
- Internal policies and procedures
- Ensure software is up to date, vulnerabilities patched
- Anti-virus software, firewalls, and EDR solution
- VPN patching up to date
- Enforce multi-factor authentication, strong passwords on all business email accounts and remote access
- Implement complex password requirements and frequent changing of passwords
- Limit use of privileged accounts
- Understand where sensitive data resides and implement strong access controls
- Back up data regularly and store off-site or in cloud

04

## Questions and Answers





Find your solution at **BBrown.com**

---

*Any solicitation or invitation to discuss insurance sales or servicing is being provided at the request of Hays Companies, Inc, an owned subsidiary of Brown & Brown, Inc. Hays Companies, Inc. only provides insurance related solicitations or services to insureds or insured risks in jurisdictions where it and its individual insurance professionals are properly licensed.*