This presentation has been prepared for the National Association of Women in Construction and will be recorded and utilized for training purposes. It will be posted on the National website - Member Center - Education - Webinars.

By remaining on this conference call you are giving consent to recording this session.

This series is OPEN to any NAWIC member.
PROTECTING YOUR CHAPTER’S ASSETS

Presented By: Sharon Scharf & Allison Hill

The information provided in this presentation is for training and informational purposes only and should not be distributed outside your organization without our written agreement to do so.
Theft can happen in any business, of any size, in any industry – including a nonprofit.

What would happen if you received your bank statement which indicated a $250 balance when you expected it to be $25,000?

How would your members respond to a letter alerting them to the disappearance of the membership dues collected for the 2020 calendar year?
To protect the company from direct loss of money, securities, property caused by:

- Employee Dishonesty
- Forgery or Alteration
- Theft
- Robbery
- Safe Burglary
- Counterfeit currency/money
- Computer Fraud
- Funds Transfer Fraud
- Social Engineering Fraud
FIDELITY

Coverage Grant

Coverage for employee theft and employee theft of client property.

Claim Example

An employee in role as executive assistant used her position to procure payment to fraudulent vendors for her personal benefit.
FORGERY OR ALTERATION

Coverage Grant

Coverage for loss through forgery or alteration of negotiable instruments drawn on your account.

Claim Example

A signature was forged on a check and cashed at the insured’s bank resulting in a loss of money from the account.
MONEY ORDERS AND COUNTERFEIT CURRENCY

Coverage Grant
Coverage for loss caused by Insured acceptance of worthless money orders or counterfeit money.

Claim Example
A company received a counterfeit cashier check for payment of delivered equipment.
COMPUTER CRIME

Coverage Grant

Coverage for loss from damage to money, securities and other property caused by computer fraud.

Claim Example

An employee of a vendor fraudulently gained access to the Insured’s computer and changed the bank routing number from the vendors to the employee’s bank account causing a large sum of money to be transferred to the employee’s account rather than the vendors.
SOCIAL ENGINEERING FRAUD

Coverage Grant
Coverage for losses sustained due to social engineering.

Definition
Social Engineering: A confidence scheme that misleads an employee into sending money, or diverting a payment based on fraudulent information provided to the employee verbally (phone) or in written format (an email, fax, letter).

Claim Example
A Third Party impersonates a vendor and tricks the Insured into transferring money to them under false pretenses. Due to the trust factor and credibility associated with the person being impersonated, the Insured transfers the money.
A company’s finance director opened an email with an attached .zip file containing a virus. The virus accessed the user ID and password for the company’s online banking account.

An unknown person immediately initiated a fraudulent wire transfer of $147,000 to an unknown account. The money was withdrawn before it could be recovered. (Source Travelers)

An employee forged thirty payroll checks then cashed some and deposited the remainder into her personal savings account.

*The Insurer paid $10,000 representing the amounts of the cashed and unrecoverable checks. (Source Hartford)*

An office employee and warehouse employee conspired to ship hundred of pieces of inventory to fictitious customers over a six month period of time. When the office employee went out on sick leave, his replacement discovered the scheme.

*The Insurer paid $110,000 representing the value of the inventory. (Source Hartford)*
RISK MITIGATION

• Maintain Strong Internal Controls
• Encourage Volunteers to Report Suspicious Behavior to Identified Company Contact
• Train employees, volunteers on use of email, internet and social media accounts and strong password creation
# RISK MITIGATION EXAMPLE

**Segregation of Duties in Two Person Company:**

<table>
<thead>
<tr>
<th>Secretary</th>
<th>President</th>
</tr>
</thead>
<tbody>
<tr>
<td>Record accounts receivable entries</td>
<td>Sign checks</td>
</tr>
<tr>
<td>Mail checks</td>
<td>Complete deposits slips</td>
</tr>
<tr>
<td>Write checks</td>
<td>Perform inter-bank transfer</td>
</tr>
<tr>
<td>Reconcile bank statements</td>
<td>Reconcile petty cash</td>
</tr>
<tr>
<td>Record credits/debits in accounting record</td>
<td>Process vendor invoices</td>
</tr>
<tr>
<td>Receive cash</td>
<td></td>
</tr>
<tr>
<td>Disburse petty cash</td>
<td></td>
</tr>
<tr>
<td>Authorize purchase orders</td>
<td></td>
</tr>
<tr>
<td>Authorize check requests</td>
<td></td>
</tr>
<tr>
<td>Authorize invoices for payments</td>
<td></td>
</tr>
</tbody>
</table>
WHAT IS THE PURPOSE OF THE POLICY?

To protect the company from the cost to deal with a Cyber event including:

- Data Breach
- Ransomware, Extortion Demand
- Media Liability
- Social Engineering Loss
A officer of a company stopped at a local grocery store on his way home from work. While he was shopping, someone broke into his car and stole the laptop, which contained personal information, credit card information and bank information of business clients. The company was sued by its clients for damages resulting from their failure to protect their private information.

*Estimated total costs exceeded $250,000 (Source Travelers)*

A manufacturer leased a copy machine over a two-year period. During this timeframe, the company made copies of proprietary client information and its employees’ personally identifiable information, including social security and drivers license numbers. After the lease expired, the manufacturer returned the machine to the leasing company through an intermediary company. Prior to making its way back to the leasing company, a rogue employee at the intermediary firm accessed the machines data for illegal purposes.

The manufacturer incurred $75,000 in expenses in connection with a forensic investigation, notification, identity monitoring, restoration services and independent counsel fees. It also incurred about $100,000 in legal defense costs and $275,000 in indemnity associated with theft and sale of proprietary client information.

*Total costs exceeded $450,000. (Source Chubb)*
DATA BREACH

Data Breach First Party:
Coverage for forensic, legal counsel, crisis management expenses due to a data breach. Crisis management expenses including public relations services.

Data Breach Third Party:
Coverage for regulatory defense and penalties and civil and investigative demands brought by governmental agencies or by private litigation.
An HR manager accidently sent an electronic file to the wrong email address. The file included the name, addresses and SSN for current and former employees.

- **First Party**: Incident response fees; cost of notification to affected individuals; identity theft monitoring services for affected individuals; legal consultation fees.

- **Third Party**: Defense expense arising from regulatory investigation; defense and settlement costs for claims from individuals whose identity had been stolen.
RANSOMWARE / CYBER EXTORTION DEMAND

Cyber extortion:
Coverage applies when a hacker or a cyber thief breaks into your computer system and threatens to commit a harmful act.

For instance, a hacker may threaten to damage your data, introduce a virus, or shut down your computer system unless you pay him or her a sum of money.

The thief may also threaten to release confidential data unless you pay the sum demanded.

Extortion coverage typically applies to expenses you incur (with the insurer's consent) to respond to an extortion demand, as well as the money (crypto currency) you pay the extortionist.
An employee of a construction company clicked on a malicious link in an email resulting in the downloading of malware onto the company server, encrypting all information. A message appeared demanding $25,000 be paid in Bitcoin within the next 48 hours in exchange for the decryption key.

Incident response expenses included:
- Consultant fees associated with assessing backup capabilities.
- Forensic investigation costs to locate malware, analyze impact, contain and calculate the extent of loss.
- Legal consultation fees.
- Extortion payment (with permission).
- Costs associated with replacing lost or corrupted data.
MEDIA LIABILITY

Media Liability:
Media liability covers lawsuits against you for acts such as libel, slander, defamation, copyright infringement, invasion of privacy.

These acts are covered if they result from your publication electronically (on the Internet) and can be extended to cover print media.

Coverage for claims for actual or alleged copyright infringement, plagiarism, defamation, libel, slander and individuals right of privacy in electronic or printed material.
An employee for a company sent an internal email containing negative comments regarding a competitor. The email was forwarded to others inside the organization and eventually was forwarded to others outside the company. The email was seen by the competitor resulting in a defamation lawsuit alleging harm to reputation.

Costs for defense and settlement for the claim as well as crisis management fees, public relation fees to minimize reputational harm.
SOCIAL ENGINEERING FRAUD

Social Engineering Fraud:
Coverage for losses sustained due to social engineering.

What is Social Engineering:
It is a confidence scheme that misleads an employee into sending money, or diverting a payment based on fraudulent information provided to the employee verbally (phone) or in written format (an email, fax, letter).

Claim Example:
A Third Party impersonates a vendor and tricks the Insured into transferring money to them under false pretenses. Due to the trust factor and credibility associated with the person being impersonated, the Insured transfers the money.
WE DECONSTRUCT RISK
CONTACT INFORMATION

Sharon Scharf  
sscharf@csdz.com  
(612) 349-2438

Allison Hill  
ahill@csdz.com  
(608) 242-2553
N.U.G.G.E.T.: Change in Leadership

- President
- Treasurer
- Membership Chair

PDF of Form Online: https://tinyurl.com/uzlrb4f

NAWIC'S Unique Groove for Gaining Extra Tidbits