Cyber Insurance vs Crime Coverage

Insurance Fundamentals

SCASBO

November 08, 2017

Presented by:

SURRY INSURANCE

Yogi Wright, CPCU, CSRM
Zach Wright, CIC, CSRM
Derek Slate, CIC, CSRM
Randy Cranfill, MESH,CPSI,CSRM

CRIME COVERAGES

- Public Employee Dishonesty
- Forgery or Alteration
- Money & Securities
- Computer Fraud
- Funds Transfer Fraud
- Fraudulent Impersonation Coverage

PUBLIC
EMPLOYEE
DISHONESTY
COVERAGE

EMPLOYEE DISHONESTY IS REAL!!

Protect your school, before it happens to you!

EMPLOYEE DISHONESTY CRIME STATISTICS

- The FBI calls employee theft "the fastest growing crime in America."
- The median loss from employee fraud is $175,000.
- The median length of time for occupational crime schemes is 18 months, and the number one way that an employer discovers crime is by accident.

MEN ARE MORE LIKELY TO STEAL … AND TO STEAL MORE!

WOMEN
$110,000
41%

Median
$110,000

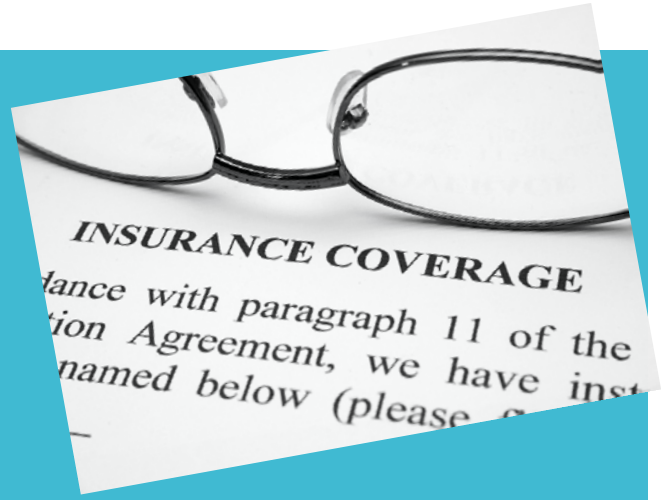
MEN
$250,000
59%

Median
$250,000

PUBLIC EMPLOYEE **DISHONESTY** COVERAGE The Basics:

- The policy covers the theft of money and/or securities by an employee.

- The policy also covers the theft of other property owned by the school if stolen by an employee.



PUBLIC EMPLOYEE **DISHONESTY** COVERAGE The Basics:

- **Coverage** should be written on blanket basis *(covers all employees).*
- Is there one employee who is not covered under the blanket?
- **Coverage** can be written on a *"per loss"* basis or *"per employee"* basis.

QUESTIONS

- Other than money and checks, what other property is covered?
- What is the difference between ***"per loss"*** basis and "***per employee"*** basis***?***
- **Others?**

CLAIM SCENARIO (1)

- The school carries a blanket **Public Employee Dishonesty** policy with limits of $25,000 with a $1,000 deductible. Four employees conspire to steal $80,000 from the school cafeteria over a period of two years. Each employee took $20,000 apiece.

Now, It's YOUR Turn...

How would the coverage work?

- Under a "*per employee*" coverage form, will all of the claim be paid?
- Under a "*per loss*" coverage form, are we in trouble here? Why?
- Does the number of years matter?

CONCERNS

- Check on the *"per employee"* versus *"per loss"* provision in your policy.
- Limits of $10,000 or $25,000 may be too low. **Consider higher options**.
- Rating is usually based on number of people whose job is to regularly handle money. It is not based on the total number of employees even though the coverage applies to everyone.

Forgery or Alteration

Coverage Form

Forgery or Alteration Coverage Form

The Basics:

- The coverage offers protection against third party forgery and alteration of written checks, drafts, or similar instruments made or drawn upon your account.
- The coverage applies only to checks and other financial instruments that are **outgoing** to other parties. *(No coverage for forged or altered instruments that are received from others.)*

Questions?

- Who are the third parties that forge or alter the instruments?
- What if the forgery or alterations were caused by your employees?
- What about credit or debit card forgery?

CLAIM EXAMPLES:

- A third party *(not an employee)* forges a check drawn in your name to a fake business or entity.
- Your blank checks are stolen by a third party and made payable to other people or businesses.
- It can be as simple as changing the amount of a check or draft by a third party.
- Any other examples or experiences?

Money and Securities Coverage

Money and Securities Coverage Form

The Basics:

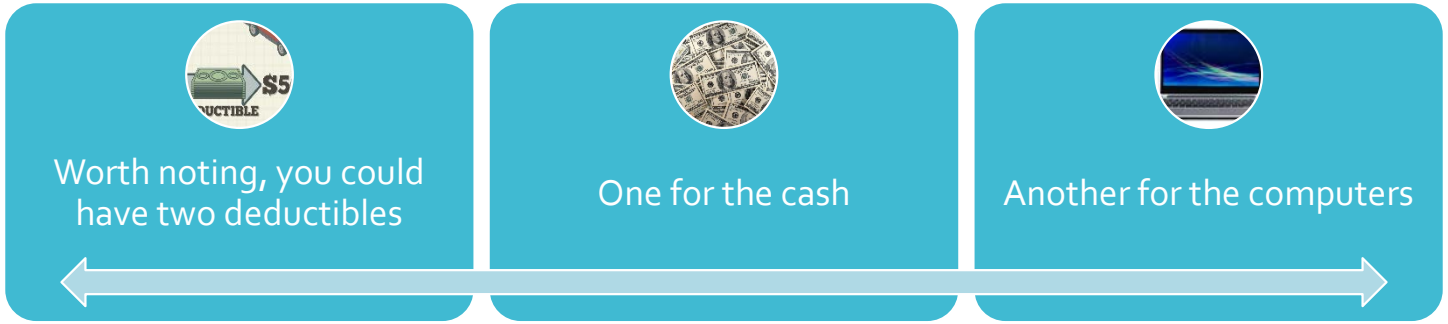
- Provides coverage for money and securities in the event of theft, disappearance, or destruction caused by a third party.
- The coverage can be also be called theft, disappearance, and destruction.
- Coverage is provided while inside your premises or inside a bank premises.
- Coverage is provided while the money or securities are in the care of a messenger outside your premises or the bank premises.
- Limited coverage is available for damage to the premises including the safe or vault during an actual or attempted theft.

Questions?

- Plain and simple, what kind of criminal act(s) are we covering with this policy?
- We know who third parties are by now, but who are messengers?

CLAIMS
SCENARIOS

- Non-employees *(robbers and burglars)* break into a school property seeking cash and other items such as computers and laptops. The cash would be covered under Money & Securities coverage, and the computers and laptops would be covered under the property policy.



- Where does your school have the most cash exposed to theft by others?
- Other examples?

COMPUTER AND FUNDS TRANSFER FRAUD COVERAGE

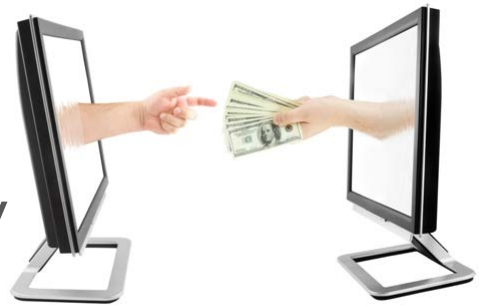
The Basics:

- A Computer Fraud policy provides coverage for theft of money, securities, and property (inventory) involving the use of a computer that would fraudulently transfer money, securities, or inventory from inside your premises or inside a banking premises to a place outside of these locations.

COMPUTER AND FUNDS TRANSFER FRAUD COVERAGE

The Basics:

- Funds Transfer Fraud coverage would cover the loss of money or securities after an electronic, telegraphic, cable, written, or telephone instruction that was fraudulently transmitted to a financial institution instructing the financial institution to release money from your account to a third party's account.



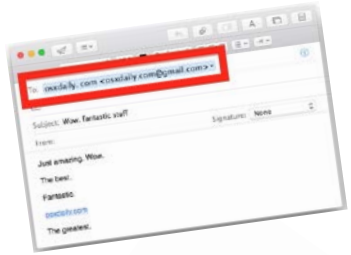
- These are third party claims. If employees were doing this, it would be an employee dishonesty claim.

Questions?

- What is the difference between the two coverages?
- Computer Fraud is the use of a computer (hacking viruses, etc.) to cause of transfer of cash or inventory.
- Funds transfer fraud results from a fraudulent communication (email, fax, etc.) directing to a financial institution to move cash or securities to another account.

CLAIMS
EXAMPLES

- Viruses online and contained in emails
- Email addresses captured and used for attempted fund transfers
- Lost or stolen laptops and/or zip drives with account information used to attempted transfers



FRAUDULENT IMPERSONATION COVERAGE

FRAUDULENT IMPERSONATION COVERAGE

- This is the latest Commercial Crime Insurance coverage available
- Offered in response to a new twist on an old crime

FRAUDULENT IMPERSONATION COVERAGE

- In property insurance terms, this is **"voluntary parting"** under a standard commercial policy.
  - If it is damaged by fire, lightning, wind, hail, etc., the property is covered.
  - If property is stolen by criminals *(computers, laptops, lawn mowers, tractors, etc.)*, the property is covered.
  - Problem occurs when you willingly give the property to a thief.
  - **Voluntary parting** is expensive coverage and is usually provided as a sub-limit.

FRAUDULENT IMPERSONATION COVERAGE

- Now, the "twist" is where do we get coverage when we actually give the money away due to a fraudulent scheme?
  - ENTER – **Fraudulent Impersonation Coverage** (Form CR 04 17)

THE BASICS:

- The policy will provide coverage under two scenarios:
  - **Fraudulent** Impersonation of Employees
  - **Fraudulent** Impersonation of Customers and Vendors

FRAUDULENT IMPERSONATION OF EMPLOYEES

- The school makes a good faith transfer of money, securities, or others property in reliance upon transfer instruction purportedly issued by an employee or any of your officials if under a Government Crime Form.

SCENARIO OF A CUSTOMER/VENDOR CLAIM:

- Criminals impersonate an IT vendor and emails an invoice for work they say was completed *(or not?)* and want the money sent to them *(the impostor).*

Actual claims or close calls?

We know of 3-4 schools that have had this happen.

Would any of you care to discuss an actual claim or a very close call?

QUESTIONS

Regarding Crime Coverage

1. What do all of the crime policies do for a school system that a Internet or Privacy Security Policy (Cyber Policy) will not???

1. What is the number one enemy of your crime limits?

Cyber Insurance

(Cyber Liability)

Allianz 2017 Risk Barometer

A survey at Allianz of corporate clients, brokers, risk consultants, underwriters, senior managers, & claims experts around the world was taken.

Top Five Current Risks were:

1. Business interruption/supply chain
2. Market developments
3. Cyber incidents
4. Natural catastrophes
5. Changes in legislation and regulation

Are Businesses the only ones facing cyber threats?

Miscellaneous Business	443 million records
Financial/Insurance	350 million records
Retail/Merchants	183 million records
Government	20 million records
Health	14 million records
Education	12 million records

Note: Data are for the last three years and include breaches affecting more than 10,000 records from an identifiable entity; excludes breaches where the number of records exposed is unknown. © Privacy Rights Clearinghouse; Adobe; The Wall Street Journal

Data Breach Stories of 2017

1. Yahoo update October 2017 – over 3 BILLION users impacted
2. Equifax: 143 million records impacted and growing
3. Blue Cross/Blue Shield – Anthem: updated from 2016 – now 80 million impacted – ***settlement of $115 million reached*** (June 2017)
4. Dunn & Bradstreet: 33 million impacted (March 2017)
5. Whole Foods Market: will not reveal number impacted (Sept. 2017)
6. Verizon: over 14 million users impacted (July 2017)
7. Dow-Jones & Company: 2.2 to 4 million impacted (July 2017)
8. G-Mail Users: over 1 million impacted (May 2017)
9. FAFSA (Free Application for Federal Student Aid): Total number affected not released (April 2017)
10. Local - UNC Health Care: 1,500 impacted (April 2017)

Sources: Identityforce.com, upgard.com

The Equifax Data Breach

- If you have a **credit report**, there's a good chance that you're one of the **143 million** American consumers whose sensitive personal information was exposed in a data breach at Equifax, one of the nation's three major credit reporting agencies.

Top 6 Causes of Data Breaches

1. Phishing, hacking, or malware (31%)
2. Employee action or mistake (24%)
3. External theft (17%)
4. Vendor (14%)
5. Internal theft (8%)
6. Lost or improper disposal of data (6%)

Source: Is "Your Organization Compromises Ready" Baker Hostetler 2016 Data Securities Incident Response Report
Property Casualty 360 05/04/16 article

Source – Your Data at Risk: 2015 Was a Year Full of Memorable Hacks by James Eng 12/23/15

Nine Hacking Terms You Need to Know

1. Botnets – large networks of computers used by hackers to send spam and conduct widespread theft
2. Denial of service – used to interrupt a website or computer network
3. Internal threats – employees (both accidental and intentional)
4. Exploits – errors or weaknesses in software or hardware
5. Hacktivists – attack entities and businesses for social or political causes
6. Malware – programs used by cyber thieves to hack networks
7. Network reconnaissance – the use of automated tools to search for computer systems to attack
8. Ransomware – encrypts victim's data and demands money be paid to restore
9. Social engineering – victims are tricked or deceived into releasing data or monetary funds

Source – propertycasualty360.com 12/09/2015

Impact of Social Media Networks

- How can a Social Media Network lead to a breach?
  - Provides a source of information for hackers looking to create a Phishing scheme on an intended target.
  - Provides different avenues with which a person can disseminate private or confidential information.
  - Provides opportunities for viruses, Trojan horses, etc. to infiltrate a system.
  - Targeted info includes email addresses and phone numbers
- 53% of companies identify Facebook and LinkedIn as a high concern for information leakage.

Do schools and students have social networking sites, blogs, etc.?

Claim Examples

- A hard drive was stolen containing transcripts, test scores, addresses, and SSNs of students that graduated from 1994 to 2004. All affected alumni have been notified by regular mail.
- How far back do you keep your records? Are they online? Bankers boxes?

Claim Examples

- Staff and faculty SSNs used as employee ID numbers were embedded in file photos by the company that took yearbook pictures and were inadvertently placed in a search engine on the school system's website.
- Outside vendor coupled with the school system's website.

Claim Examples

Employee and volunteer records were found in a recycling bin near the school.

The list goes on and on….

Source: www.infosecurityanalysis.com

Recent NC School Example

- An email from what appeared to be a trusted vendor resulted in the release of over 3,000 W-2's with names, social security numbers, addresses, wages, etc.
- The district first purchased standalone coverage in 2015.

Lessons Learned

- No such thing as impenetrable IT systems
- Often times you don't realize you've been hacked
- What is your response plan? Who is your first call?
- Employee training matters
- Monitor employee access to sensitive data – upgrade finance systems
- Physical controls and employee training

- Remote wipe capabilities
- Encryption (whole disk) for sensitive data on portable media
- Large black market for personal information with growing connection to organized crime
- Know your vendors and your responsibilities in the event of a loss
- ***Contractual indemnity language is important***
- ***Will soon ask for proof of insurance from vendors like you ask for GL and WC.***

Ransomware


RANSOMWARE
JUST WHEN YOU THOUGHT IT WAS SAFE TO TRUST EMAIL
DON'T BE A VICTIM
THINK BEFORE YOU CLICK

What is Ransomware?

- Ransomware is a type of malicious software that prevents the victims from accessing their documents, pictures, databases and other files by encrypting them and demanding a ransom to decrypt them back.
- Ransomware is an ever-increasing threat worldwide, claiming a new victim every 10 seconds.

Common Ransomware

WannaCry - is the most recent (last May) and the largest Ransomware attack to date. It infected more than 100,000 computers by taking advantage of an unpatched Microsoft Windows vulnerability.

- Locky - first seen arriving as a **macro in a Word document**, and then spotted being spread via Adobe Flash and Windows Kernel Exploits. Locky ransomware is known for deleting shadow copies of files to make local backups useless.

How does a ransomware infection occur?

- ***A typical ransomware infection can begin with any of the following routes***:
  - Email messages that carry a downloader Trojan virus, which attempts to install ransomware.
  - Websites hosting exploit kits, which attempt to exploit vulnerabilities in the browser and other software to install ransomware.

How do I protect my computer against ransomware?

- As with all threats, **prevention** is key. This is especially true for malware as damaging as ransomware.
  - Back up your important files regularly. Consider using the 3-2-1 rule: Make three backup copies, store in at least two locations, with at least one offline copy. Use a cloud storage service.
  - Install and use an up-to-date antivirus solution.
  - Don't click links or open attachments or emails from people you don't know or companies you don't do business with.
  - Make sure your software is up-to-date to avoid exploits.

Prevention: Train Employees

- Review e-mails closely to make sure they are from a trusted and known sender before links and/or attachments are open.
- Never download attachments from suspicious e-mails.
- Don’t store important data on the PC if possible.
- Keep them up to date on what and how cyber attacks occur.
- Periodically test employees with mock phishing e-mails.

Questions?