Filling the Coverage Gap: Property vs. Crime

Derek Bryan, Executive Director
Washington Counties Risk Pool
360-292-4497
derekb@wcrp.wa.gov

The Property Policy

What it covers:

Physical loss or damage to:

- ❑ Real and personal property
- ❑ Property of others in your care, custody and control.
- ❑ Extra Expenses – physical loss or damage required
- ❑ Business Interruption – physical loss or damage required

The Property Policy

What it <u>does not</u> cover:

- ❑ Land
- ❑ Water – except water stored in a tank, piping system or process equipment
- ❑ Growing crops, standing timber, animals (except for research or public service)
- ❑ Wear and tear, deterioration, vermin/insects, settling of walls, floors, foundations, faulty workmanship
- ❑ Money and securities

For Example…

Vandals break into your building and damage the walls & doors, break open a safe and steal $50,000 in cash.

Are the damaged walls, doors and safe covered under the property policy?

✓ Yes
__ No

Is the $50,000 in cash covered under the property policy?

__ Yes
✓ No

For Example…

Over a 5-year period, an employee has been stealing money, amounting to a total of $500,000.

Is this covered under the property policy?

__ Yes
✓ No

The Crime Policy

What it covers:

- ❑ Theft of Money and Securities
- ❑ Employee Theft
- ❑ Inside Premises Theft/Robbery
- ❑ Funds Transfer Fraud

The Crime Policy

What it <u>does not</u> cover:

- ❑ Acts committed by “you” or “officials”
- ❑ Bonded employees (some will apply in excess)
- ❑ Inventory shortages
- ❑ Computer Fraud

Key Takeaways…

- ❑ Many times, an exclusion in one policy or line of coverage is available in another policy or line of coverage.
- ❑ Find and fill the gaps in coverage.
- ❑ It's better to have too much coverage, or concurrent coverage, than none at all.
- ❑ Understand that property, casualty and fidelity are different lines of coverage.
- ❑ Insurance is for the unknown or unexpected. Are you being robbed right now?

Case Study: Spokane County

Steve Bartel, Director – Risk Management
Spokane County
509-477-6113
sbartel@spokanecounty.com

What was the procedure?

1. Checks were issued by County Auditor's Office based on approvals sent by departments.

2. Departments had back-up "approvers" that could sign authorization to issue payment.

3. Authorization to issue payment was then sent to Auditor's Office – check issued.

What happened?

1. Employee learned that getting authorization from back-up approvers was easy.
2. Started creating fake “claim payment vouchers” to issue payments to fictitious claimants.
3. Created fictitious claim numbers, claimant names, loss estimates and settlement agreements.
4. Waited until Director was out of office and would get the authorization signed by back-up.
5. Fake approval then sent to Auditor’s Office with note that employee will “pick up” check.
6. Over several years, the employee made 213 false payment requests, totaling $1,384,407.

How did they get caught?

1. Employee left County's employ for unrelated reasons.
2. One of the fraudulent checks was not cashed within 90 days.
3. County Auditor inquired with department head about stale check.
4. Department head looked into the check authorization and discovered it was not for a legitimate claim.
5. Busted!!

What were the gaps?

1. Backup check approval process was too easy to work around.

2. County Auditor relied on check authorization without Department Head approval.

3. The County's size and internal controls allowed the employee to learn, and therefore cheat, the system.

4. Employee's destruction of the records after payment made avoided detection during vouchers/payment reviews at month end.

What's the new procedure?

1. County revised its Department Payment Authorization and Signatory Policy.
2. Director approves claims created and deleted in claim system.
3. All payment vouchers are to be approved by Director with very limited exceptions.
4. County implemented staff training on claim and payment processes.

Key Takeaways…

- ❑ Secure a Crime policy. You won't know you need it until you do…and you'll be glad you did.
- ❑ Complacency and routine is a criminal's best friend.
- ❑ Don't just review your policies, but review your process. Could an employee steal from us if they wanted to?
- ❑ Consider multiple lines of approval or signature.
- ❑ Watch out for "employee will pick up or deliver check". Why have a different department issue payment if they will give the same check to the same employee?

Thank you!

Derek Bryan, Executive Director
Washington Counties Risk Pool
360-292-4497
derekb@wcrp.wa.gov

Steve Bartel, Director – Risk Management
Spokane County
509-477-6113
sbartel@spokanecounty.com

Cyber:
The risk that keeps getting riskier

Derek Bryan, Executive Director
Washington Counties Risk Pool
360-292-4497
derekb@wcrp.wa.gov

Noteworthy Terms

Noteworthy Terms

- First Party vs. Third Party
- Reporting Period
- Extended Reporting Period
- Claims Made vs. Occurrence
- Retroactive Date
- Per Claim/Occurrence Limit
- Aggregate Limit

Noteworthy Terms

- ❑ Sublimit
- ❑ Deductible vs. Retention
- ❑ Subrogation
- ❑ Indemnity vs. Expense
- ❑ Endorsement
- ❑ Erosion of Deductible or Retention
- ❑ Social Engineering

Social Engineering: Crime or Cyber?

Social Engineering: What is it?

"…the transfer of money or securities to an account outside the insured's control, pursuant to instructions made by a person purporting to be an authorized employee, provider or customer of the insured…"

Social Engineering:

Is it covered under a <u>CRIME</u> policy?

Look for these terms:

- ***Computer Fraud***
- ***Funds Transfer Fraud***
- ***Voluntary Parting***
- ***Transfer or Surrender of Property***

Social Engineering:

Is it covered under a <u>CYBER</u> policy?

Look for the endorsement:

- **Is it included?**
- **Does it have a sublimit?**
- **Does it have conditions? Such as:**

"…applies only if the insured verifies the instruction to transfer money or securities by following a pre-arranged callback or other established procedure to authenticate the validity of the request prior to transfer…"

Questions You Should Ask

Questions you should ask:

- ❑ **What first-party coverage do we have?**
- ❑ **What third-party coverage do we have?**
- ❑ **What are our limits (per claim & aggregate)?**
- ❑ **Does our policy include data breach response, such as crisis management and notification support?**
- ❑ **Is it a Deductible or a Self-Insured Retention?**
- ❑ **Do expense costs erode the deductible or SIR?**
- ❑ **Does the policy pay for the payment of ransom in a cyber extortion incident?**

Questions you should ask:

- **Is social engineering covered and, if so, do conditions apply?**
- **Do we have a retroactive date?**
- **Do we have “claims made” or “occurrence” coverage?**
- **If “claims made”, when is the claim made and do we have an extended reporting period?**
- **What is the definition of “occurrence”?**
- **Who qualifies as an “Executive Officer” for claim reporting purposes?**

Pre-Breach Resources

- ❑Phone Consultations
- ❑Social Engineering Assessment
- ❑Incident Readiness Assessment
- ❑Phishing Expedition
- ❑Incident Response Policy Review

Post-Breach Resources

- ❑Reporting Hotlines
- ❑Forensic Analysis
- ❑Legal Defense/Support
- ❑Business Interruption
- ❑Breach Response & Crisis Management
- ❑Cyber Extortion Support

Case Study: Okanogan County

Derek Bryan, Executive Director
Washington Counties Risk Pool
360-292-4497
derekb@wcrp.wa.gov

What happened?

- On a Saturday morning, County discovered their system had been hacked and was being held for ransom.
- County contacted WCRP and reported the breach and a claim was immediately opened.
- Claim was also reported to Cyber Re-Insurer and Incident Response Team was assembled.

What happened?

- Incident Response Team was the direct contact for the “bad actors” and coordinated settlement offers and eventual resolution.
- Ransom was eventually negotiated and paid.
- Encryption “key” was provided after money wired.
- Over many weeks following, the County was able to recover data, restore systems and is returning to “normal”.

Key Takeaways…

- ❑ Are your back-up servers through a third-party and standalone?
- ❑ Is your VPN access secure?
- ❑ Are employees using personal equipment to login?
- ❑ Do you require multi-factor authentication?
- ❑ Do you use a third-party cyber security vendor/consultant?

WASHINGTON COUNTIES RISK POOL

Created *by* Counties *for* Counties

Thank you!

Derek Bryan, Executive Director
Washington Counties Risk Pool
360-292-4497
derekb@wcrp.wa.gov