Cyber, Privacy & Technology Insurance FAQ's

1. What is "cyber liability"?

Cyber liability is the risk posed by conducting business over the Internet, over other networks or using electronic storage technology. Cyber liability includes first and third-party risks associated with the use of computer hardware and software systems, the Internet, networks, mobile computing devices, and other electronic information assets. In addition to electronic hacking or online activities, Cyber Liability Insurance provides coverage for private data and communications in many different formats – paper, digital or otherwise.

Examples include:

- Data privacy issues
- Virus/malicious software (malware) transmission to a third party
- Business interruption and data recovery
- Regulatory defense and fines
- Cyber extortion
- Website or media misuse
- Infringement of intellectual property

Common first-party costs when a security failure or data breach occurs include:

- Forensic investigation of the breach.
- Legal advice to determine your notification and regulatory obligations.
- Notification costs of communicating the breach.
- Credit monitoring to customers as a result of the breach
- Public relations expenses.
- Loss of profits and extra expense during the time that your network is down (business interruption).

Common third-party costs include:

- Legal defense.
- Settlements, damages and judgments related to the breach.
- Liability to banks for re-issuing credit cards.
- Cost of responding to regulatory inquiries.
- Regulatory fines and penalties (including Payment Card Industry fines).

2. What are the potential cyber risk exposures?

Potential Risk

- Breach of Personal Protected Information (PPI)/ Hacker
- Lost or Stolen Laptop/ Smartphone/ Tablets
- Employee Negligence/ Human Error/ Rogue Employee
- Thumb Drives / Flash Drives
- Servers and Cloud Storage
- Dropbox
- Paper Files
- Copy Machines

Potential Exposures

- Citizens' Records
- National Security Intercepts (e.g. telephone/email)
- Social Security Numbers
- Health Records
- Tax Data
- State Contracting, Purchasing
- Employee Records
- Student Enrollment Records
- DMV Records
- Credit Card Numbers
- Fines/Penalties coming from a regulatory claim alleging a privacy breach or violation of a Federal, State, local or foreign statute or regulation with respect to privacy regulations.

3. What does cyber liability cover?

Breach Response Expenses- Covers crisis management, including notification cost, credit monitoring service, and public relations expenses incurred resulting from a security or privacy breach.
Data Restoration- Pays the costs for the restoration of any data stored.
Network Security Liability- Provides liability coverage for damages and claim expenses arising out of an actual or alleged act.
Privacy Liability- Provides liability coverage if an insured fails to protect personal protected information.
Privacy Regulatory Proceeding- Provides coverage for defense expenses from a regulatory proceeding resulting from a violation of a privacy law caused by a covered security breach.
Media Liability- Covers the insured for Intellectual Property and Personal Injury perils that result from an error or omission in content on their website.
Cyber Extortion- Provides coverage for expenses and/or losses incurred as the result of an extortion threat.
Business Interruption- Provides coverage for business interruption loss and/or business restoration expense as result of a security breach that caused system failure.

4. How would my coverage respond in the event of a cyber liability claim?

Breach Response Timeline

1. Notify the Office of Risk Management once your organization is made aware of a possible breach.
2. Risk Management will notify the cyber liability carrier once your agency reports the possible breach to Risk Management
3. The carrier will assign a Breach Coach to your agency who will help select the proper breach counsel and forensic team.
4. The Breach Coach and you're the agency will select a notification service provider to notify the affected individuals ensuring all regulatory requirements are met.
5. Your agency will approve the notification letters to be mailed to the affected individuals

6. The Breach Coach will contract a call center service provider to handle any questions on your agency's behalf.
7. Affected individuals receive their notification letters and may enroll in the credit monitoring service.
8. Your agency will receive reports on the progress of the notification letters and credit monitoring enrollment for continuous monitoring of the event.
9. Your agency will be responsible for the first $10,000 for each claim.

5. Top 5 Leading Causes of Cyber Claims?

1. Lost employee laptop or other computing devices
2. Malicious acts by a rogue employee or ex-employee
3. Improperly disposed sensitive information
4. Media campaign gone wrong
5. Subcontractor error or omission (including breaches on those subcontracting vendors that are holding your data)

6. Does the State of Idaho have cyber liability insurance?

Yes, coverage was bound effective 12/1/16. This policy is to help cover costs associated with the financial impact from information technology (IT) security incidents. This coverage is provided as a standalone insurance policy that the state carries. For an agency to access this coverage, it must also be covered by our self-retained liability coverage. The underlying insurance would be provided by the Barbican Insurance Group a Syndicate of Lloyds.

7. What is the deductible for the current cyber liability insurance policy?

The self-insurance retention (SIR) amount is $1,000,000 per occurrence. The terms SIR, retention, and deductible mean the same thing. The insurance covers costs over this limit. The agency deductible is $10,000 per occurrence.

8. What are the policy limits?

The State of Idaho has a limit of $25,000,000 per claim and a $25,000,000 annual aggregate (the maximum that the insurance company will pay in any policy period) in the current policy year.

9. Are all state agencies covered by the cyber liability insurance policy?

All agencies that are covered by Idaho's self-retained liability program have the current cyber liability insurance coverage.

10. How do we know the cyber liability policy will pay out when we need it?

Risk Management requires our insurance broker to only offer us insurance from insurance firms with a rating of "A" or better. This designation refers to the international ratings by AM Best. Our current cyber liability Insurance is provided by the Barbican Insurance Group a Syndicate of Lloyds. Barbican is backed by the financial security of Lloyds which is rated A+ (Strong) from Standard's and Poor's.

- The State of West Virginia purchased coverage with Lloyds in August 2014. They have had several incidents and have used the breach counselor and credit monitoring services. The Risk Manager reported that they have had excellent service and immediate responses from the breach counselor assigned.
- The Cyber Liability Insurance policy is NOT based on any assessment of compliance to the state Office of the Chief Information Officer (OCIO) or other IT security standards at the time of a loss.

11. What should agencies that are included in the statewide cyber policy report to Risk Management.

This policy requires that the state provide notice of claim, loss, or circumstance that might lead to a claim as soon as practicable. Keep the Office of Risk Management up-to-date regarding your agency cyber liability risk exposure.

12. How do we find out more about this policy or report a claim or incident?

Contact the Office of Risk Management by phone or email. Cyber liability contacts are:

Faith Cox, Statewide Risk Manager, 208-332-1871, faith.cox@adm.idaho.gov
Kris Coffman, Senior Adjudicator, 208-332-1870, kris.coffman@adm.idaho.gov
Glen Goff, Claims Adjudicator, 208-332-1868, glen.goff@adm.idaho.gov
Joan Compton, Risk Management Analyst, 208-332-1872 joan.compton@adm.idaho.gov

13. Is this different than the OCIO Incident Communication Policy?

The OCIO Incident Communication Policy deals with the operational communication needs during an IT Security incident. Risk will coordinate with the OCIO and have access to the OCIO incident database. All incidents should be reported through the OCIO portal to assure proper reporting protocols are followed. If an agency fails to notify the OCIO and Risk of an incident that gives rise to a claim within 30 days, coverage may be denied. An official claim with Risk will be opened once an incident turns into a claim for damages. Agency IT leadership should work closely with their Risk Manager and the OCIO to develop procedures for these reporting requirements. Our obligation is to report claims and incidents as soon as practicable but no later than 30 days from when they are known.

14. How will the policy respond if the date of breach cannot be determined?

The date of the actual breach does not matter. The policy requires Risk Management to notify the insurance carrier once a "controlling member" is made aware of the breach. A controlling member is defined as Chief Executive Officer, Chief Financial Officer, General Counsel, Risk Manager, Chief Operating Officer, Chief Information Officer, Chief Privacy Officer, President and Chief Technology Officer and their functional equivalents.

For example, if there was a data breach in 2012, which went undetected until 2016. The Insured reported the breach to the carrier once the Manager, Risk Manager, or CIO became aware in 2016. The event would be covered.

There will not be retroactive coverage for events that are known prior to the policy effective date. For example, Fish and Game had a known 3rd party vendor data breach in August 2016. The policy and coverage was effective on December 1, 2016. This event will not be covered.

15. When we have a third-party breach will our policy respond even if they have a contractual obligation to provide some cyber coverage?

Yes, the coverage would respond. The State's coverage would be secondary to the third-party vendor's coverage. The State's coverage would also apply if the third-party vendor did not have cyber coverage or their limits were exhausted.

For example, the State utilizes a third-party vendor to process its credit payments. The third-party vendor has a data breach, which includes the State's data, costing $10M in expenses. The third-party vendor has a cyber liability policy of $5M. The third-party vendor's coverage would be primary, covering the first $5M. The State's coverage would be secondary covering the remaining expenses, in this example $5M.

16. Are there special requirements before the policy will respond to third-party vendor losses?

No. The only special requirement is that the breach must affect the State. In other words, the cyber policy will only cover the expenses for the State of Idaho loss.