Cyber Claim Examples

Cyber attacks and data breaches are occurring more frequently and at a larger cost. Small to medium sized organizations are being targeted because their security and protocols haven't kept pace with this trending risk. According to the 2018 Ponemon study on data breaches, the top industries paying the highest price as a result of a breach include: healthcare ($408/lost record), financial ($206), and pharmaceutical ($174). Their statistics show that 27% of all breaches are due to human error and 48% result from malicious or criminal activity.

The Ponemon Report also concludes that having an Incident Response Team on average lowers the cost per record by $14. The extensive use of encryption reduces the per record cost by $13.

There are many different ways to experience a data breach or business interruption event. The examples below demonstrate how organizations can be impacted by them and how Frank Cowan Company's Cyber Insurance policy may respond*.

Claim Example: Cloud Provider / Business Interruption

An Insured uses a third-party provider to host their corporate data via a cloud service. Due to an unforeseen incident, the cloud provider had an extended outage due to a system failure on their server The Insured, relying on the cloud provider, was unable to continue business operations without access to their corporate data which the cloud provider was hosting.

The Insured experienced lost business income while they could not access their data, had extra expenses to pay to try work around the problem, and suffered reputational damage.

Cyber Insurance Policy Response:

- Business Interruption losses paid – which now includes coverage systems or data in the cloud.
- Extra expense costs paid for continuing business during the outage.
- Crisis management provision to advise on how to mitigate the reputation damage.
- Legal costs and Network Security liability cover in case of 3rd party damages claims.

Claim Example: Network Breach

A facility experienced a network breach where several employees' information was compromised due to a computer virus that potentially affected employee data.

Cyber Risk Insurance Policy Response:

- Forensics costs paid, to investigate if employee data was breached and how.
- Privacy liability cover would respond to employee privacy claims.
- Cost of notifying individuals of the data breach whether or not it is required by legislation.
- Crisis management provision to advise on how to mitigate the reputation damage.
- Legal costs and potentially Regulatory Fines paid with respect to all major applicable privacy regulations

Claim Example: Lost Laptop

An employee was distracted as the commuter train pulled into the busy station. As a result, they accidentally left their laptop on the train. Despite calling the train office and looking in the lost and found area repeatedly, they were not able to recover their laptop. The laptop contained clients' personal information including: names, addresses, social insurance numbers and health card information.

Cyber Risk Insurance Policy Response:

- Crisis management costs to advise on how to mitigate the reputation damage
- Cost of notifying individuals of the data breach whether or not it is required by legislation.
- Legal costs and potentially Regulatory Fines paid with respect to all major applicable privacy regulations.
- Privacy liability cover, for any 3rd party client claims.

Claim Example: Malicious Online Post

A hacker obtained damaging and sensitive information regarding the Insured's clients by gaining access to their systems. The hacker posted the information online for everyone to see. The client's reputation was damaged and eventually brought suit against the Insured.

Cyber Risk Insurance Policy Response:

- Privacy liability cover, for any 3rd party client claims
- Forensics costs to investigate how the insured was hacked and what was done.
- Cost of notifying individuals of the data breach whether or not it is required by legislation.

Claim Example: Media / Online Posting

An Insured operates a Facebook page to advertise their local services. A disgruntled employee had access to the Facebook page and posted public and derogatory/slandering comments on the pages of similar service providers.

It was determined that the Insured didn't have adequate internal procedures to monitor and clear any content posted on the Facebook page, including inadequate procedures to remove access for ex-employees.

Cyber Risk Insurance Policy Response:

- Multimedia liability cover including slander, defamation, breach of confidence/misuse of information.
- Crisis management costs to advise on how to mitigate the reputation damage.

Claim Example: Computer Virus / Ransomware

An Insured experienced a system outage Where the incident was determined to be caused by a virus spread when an employee of the Insured clicked on an external link found in an email which then spread the virus across the insureds network.

The email posed as an authentic HR email asking for the employee to click a link to review updated HR policies and procedures.

The virus locked all essential files and applications stopping day-to-day business until a ransom was paid in order to regain access. The Insured was not adequately backing up their information on a regular basis causing them to feel obligated to pay the ransom as they had no other avenues for recovery.

Cyber Risk Insurance Policy Response:

- Extortion expenses to pay the ransom, potentially in bitcoins, if legally permissible.
- Data restoration would apply for files that were destroyed in the process if possible.
- Crisis management costs to advise on how to mitigate the reputation damage.
- Forensics costs to investigate what the virus was, how it got into the system, what damage it has done and to investigate if it can be removed, reversed or wiped and replaced.

Claim Example: Payment Card Industry (PCI)

An Insured experienced a cyber incident and after an investigation it was determined that their Point-of-Sale system was breached. The investigation found that they were unintentionally logging credit card numbers and sharing them with an unknown 3rd party hacker.

The Insured incurred fraud assessments, card reissuance costs, case management fees and were subject to regulatory fines as mandated by the Payment Card Industry Data Security Standards (PCI DSS). These fines posed a significant business impact due to the small nature of their operations and inability to absorb the penalties incurred.

Cyber Risk Insurance Policy Response:

- PCI DSS Extension Endorsement is available and is required to respond in this example
- Cost of notifying individuals of the data breach whether or not it is required by legislation.
- Crisis management costs to advise on how to mitigate the reputation damage.
- Forensics costs to investigate what was hacked, how, and what was stolen.
- PCI DSS fines, penalties, assessments, fraud recovery and operational expense.
- Legal costs and potentially Regulatory Fines paid with respect to all major applicable privacy regulations