Texas Council Risk Management Fund

# Anatomy of a Cyber Claim

Cyber claims often require the involvement of many specialized resources, including computer forensic experts, privacy lawyers, credit monitoring services, and call centers. Because cyber claims are altogether different from typical claims, it's vital to have the resources and expertise to handle the complexities of cyber claims. Understanding the importance of having a Claims Protocol and getting the notification process correct from day one is important. Understanding how to respond to a cyber incident and the interactions between various party and vendor roles is also beneficial.

First; let's discuss what can you do to protect your organization. The first step would be to make sure your organization is covered by a cyber insurance policy. Cyber coverage is available on the market and can be included as an add-on to most excess coverage. Cyber coverage offers protection from threats posed by cyberattacks and data breaches including losses to an organization's finances, reputation, and operational capabilities.

In addition to ensuring the entity has coverage for these events, it is also important to make sure they take appropriate steps to reduce the risk of data loss. The following steps are provided so entities can reduce the risk of cyberattacks.

- **Incident Response Planning**. Develop an incident response plan, designate an incident response team, and practice and update the plan regularly.
- **Employee Training**. Train employees on security awareness throughout the year; consider phishing tests to maintain employee vigilance.
- **IT Risk Assessment**. Conduct a risk analysis to identify what sensitive data your entity holds and where, and to evaluate your risks and the effectiveness of mitigating controls. Consider employing an experienced IT Risk Control Specialist, provided by the Texas Council Risk Management Fund, to conduct the IT risk assessment. If interested, contact Lee Cain at Lee.Cain@sedgwick.com or (512) 427-2322 to schedule an IT Risk Control Visit.
- **Encryption.** Implement full device encryption on all portable devices and consider secure email solutions.
- **Two-factor Authentication**. Set up two-factor authentication for remote access and for administrator access to key resources. Provide remote access only through secure channels, such as a well-configured virtual private network (VPN) connection. Require strong passwords.
- **Backups**. Implement a data backup and recovery plan; maintain copies of sensitive or proprietary data in a separate and secure location not readily accessible from local networks.
- **Document Retention Policy**. Develop a document retention policy and properly dispose of sensitive data accordingly.
- **Penetration Testing**. Retain a security firm to evaluate the risk that an attacker can compromise the IT assets and remediate accordingly.

- **Antivirus and Patching**. Regularly update antivirus definitions for all users and ensure timely patching of operating systems and software.
- **Intrusion Prevention and Detection**. Deploy an intrusion detection system (IDS) and an intrusion prevention system (IPS) that aggregate logs to a Security Information and Event Management (SIEM) tool that sends real-time alerts.
- **Vendor Risk Management**. Ensure vendors are contractually obligated to protect sensitive data, provide timely notice of a breach, return, or destroy data at termination, and maintain cyber liability insurance.

If a cyber incident or potential cyber breach does occur and you have cyber coverage with Beazley, report it immediately by sending an email to both of the following email addresses; bbr.claims@beazley.com and Shela.Ferrell@sedgwick.com. When reporting a claim or loss, please provide the following information:

- Name of the organization and insurance policy number;
- Short description of the incident;
- Date the incident occurred (if known);
- Date the insured discovered the incident; and
- Contact information for the point person handling the investigation at the insured level.

The insured should not appoint their own external law firm or forensics team to provide them with assistance. It can get very complicated adhering to each state's cyber breach laws. All of these details should be assessed and pre-approved by the Insurance provider's Claims Department first. If they determine a breach of privacy has occurred, a Cyber Breach Coach or Privacy Attorney will be appointed to the insured.

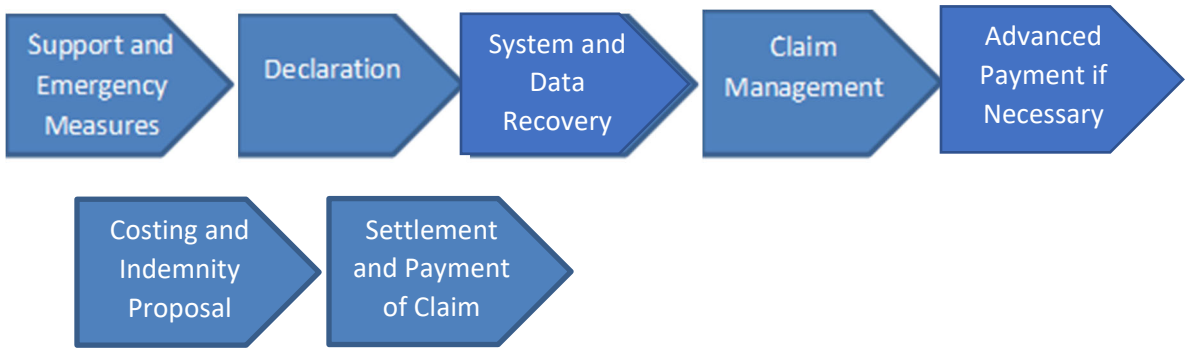
An investigation will then take place to:

- Gather all the facts surrounding the incident;
- Determine what systems have been impacted;
- What potential data has been impacted;
- Who knew about the incident;
- When was the incident discovered;
- When did it actually occur;
- Has the broker been notified;
- Who will perform the forensics analysis; and
- Who will provide legal services.

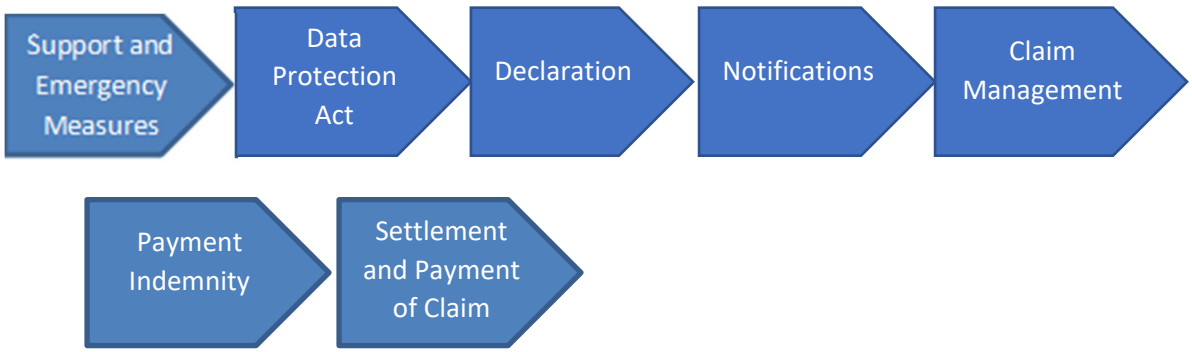
**Incident and Claims Management Steps**

Below are the various steps that occur in incident and claims management. In the first phase, Incident Management will occur. Internal and external expertise is required by IT, legal, and public relations. In the second phase, Claims Management will occur. Facilitation of adequate reimbursement of costs from the insurance policy, loss adjusters, loss assessors, and claims advocates is required.

**Disruption of IT System(s)**




**Breach of Confidentiality of Personal Data**




**Cyber Extortion**
Extortion is part of a cyber policy. It will cover the ransom, the costs for a negotiator, and it will cover a reward if someone is able to provide information that will lead to the capture of the extortionist. Unfortunately, it's not often that these extortionists are caught.

**Forensics Team**
After the extortion has been dealt with and the files have been recovered, the insured will want to bring in a Forensics team. They'll evaluate the breach to determine, how the cybercriminal got in, what access they had while they were in the system(s), what information was taken, how long has the cybercriminal been in the system(s), are they still present, and how to get them out to stop any further issues. Forensics are very good at what they do and can be costly.

**Notification**
What the Forensics team finds determines the type of notification(s) that will occur. Affected parties will be notified in accordance with applicable State and Federal Law. Laws concerning medical information can be more stringent. Typically, notifications will be sent in the form of a letter. They can also be completed via website. Sometimes call centers will need to set up to manage the questions coming in after the notifications occur. These are all First Party expenses that would be covered on a cyber policy including data restoration. A question to ask is, "Does the policy cover voluntary notification?" It's

possible that only telephone numbers were taken, for example, but the insured still wants to notify those parties.

**Credit Monitoring**
When the affected parties have been notified that there's been a breach, the insured will want to provide them with credit monitoring. This will occur usually within one year or more depending on the nature of the data that was breached so the length can vary. A question to ask is, "Is credit monitoring only covered up to one year or does it cover whatever the state mandates?" As more breaches occur, it's highly likely that states will change their laws in accordance with this trend and increase that time. Credit Monitoring is used as a tool to mitigate potential liability and class actions arising from data breach.

**Public Relations**
Perhaps the insured will want to initiate public relations to assure the affected parties that their information is secure. This is also covered on a cyber policy to effectively respond to the data breach and reduce the reputational harm along with mitigating the liability. Reputational harm is different because it's the goodwill lost by the insured after a data breach. It's typically not insured on cyber policies. Because of that, it can be devastating if a cyber breach is mishandled. Even if it is included in the cyber policy, the insured is most likely going to reach the limit before Reputational Harm coverage even gets triggered. If the systems were down because of a virus or ransomware and business continuity is paused, there's going to be a waiting period and a limit.

**Reimbursement vs. Pay on Behalf**
Odds are the insured most likely doesn't have $30,000 or more sitting around exclusively to pay a ransom. Because of this, pay on behalf is most likely what is wanted in a cyber policy instead of choosing the reimbursement option.

**First Party vs. Third Party**
After all the expenses are paid, now come the claims. Entities with First Party exposure (damage to the member) almost always have Third Party exposures (damage to others) as well. After notifications to the affected parties of the cyber breach, various liabilities follow. The State Attorney General may come after the insured. If HIPAA violation occurs, U.S. Department of Health and Human Services Office for Civil Rights will most likely contact the insured. This all falls under regulatory action. The insured could experience class action lawsuits and/or fines and penalties assessed by the Payment Card Industry. These are all the Third Party exposures the insured may have.

**Policy Aggregate**
Another question to ask is "What's the Cyber Policy Aggregate Limit?" Is there a separate limit for the First Party expenses and the Third Party claims? For example; If the insured has a $500,000 policy and they spend $400,000 on forensics, notification, credit monitoring, and public relations, is there another $500,000 limit for claims or is there only a $100,000 limit remaining? This is something to pay attention to. Does the cyber policy have separate limits for the first and third parties or does it have a Shared Policy Limit?

Data Breach Coverage, Cyber Liability Coverage, and Cyber Privacy and Security Coverage all help protect the entity from the direct costs and fallout faced when a data breach occurs. Coverage is offered as part of a convenient suite of management liability products for seamless protection. Global reinsurance rates have increased by up to 40% in the July 2021 renewal season as ransomware attacks increase in number and severity. The average ransomware payment to restore data after a cyber attack was $220,000 in the first quarter, up 43% from the last quarter of 2020. Reinsurers insure the insurance companies, and a rise in reinsurance rates feeds through into higher insurance costs. The costly attacks are not going to stop. This, in all likelihood, means the costs of cyber coverage will continue to increase and/or terms of the policy will change to limit coverage.

To combat cyber risk, an IT risk assessment is a great method to conduct a risk analysis and the effectiveness of mitigating controls. Consider scheduling an experienced IT Risk Control Specialist, provided by the Texas Council Risk Management Fund. If interested, contact Lee Cain at Lee.Cain@sedgwick.com or (512) 427-2322 to schedule an IT Risk Control visit.