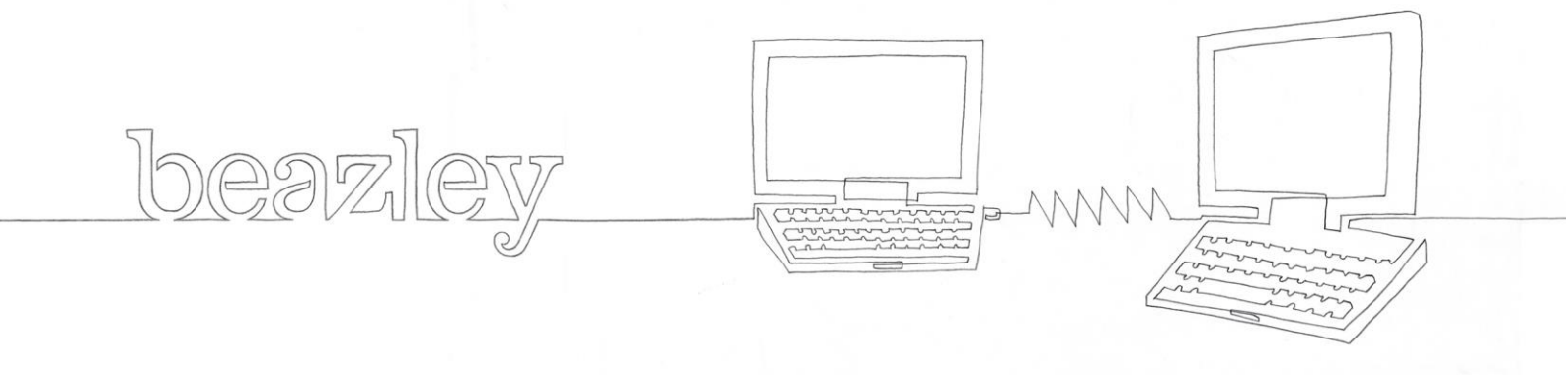
Beazley Breach Response

Executive summary



BBR – Executive summary

If a business has a company website or handles customer or employee data, then it has the real exposure of a potential breach of data. Having handled over 6,000 data breach incidents, Beazley are unparalleled in terms of experience and understand the steps necessary to handle a data breach efficiently, preserving the reputation of the business.

BBR Services

Fundamental to our coverage is the facilitation of the provision of Beazley Breach Response (BBR) services, supplied by our vendors and paid for by us, not the insured. The BBR limit is expressed as a number of individuals (rather than GBP) covered making it easier to choose the appropriate limit size. BBR encompasses a wide range of services, from legal and forensics to credit monitoring and Data Patrol, which is an especially useful service for companies to show their affected customers they care. It is also a completely separate column of cover so you can use all the services cover and still have a financial limit left for the liability claims.

Cyber Liability

When looking at the liability side of cover, as standard we have the usual information security and privacy coverage for claims brought against the insured as a result of their third party cyber liability. This includes coverage for regulatory actions, website and offline media liability, and payment card industry (PCI) coverage for credit card breaches. As well as network/system data, we also cover the exposure of data on paper, and we will cover legal defence costs.

Extensions

On top of this, we can extend our policy with our First Party Computer Security Coverage endorsement which offers protection for Cyber Business Interruption, Cyber Extortion and Data Protection. In the event of a ransomware attack (for example), this would cover the loss of income or increased working costs, any costs/values involved as a result of the ransom demanded and, arguably more vitally, the cost of data recovery. As well as this, our Fraudulent Instruction Coverage endorsement covers the value of any fund transfer made in good faith which subsequently turns out to be a hacker. Lastly, our Telecommunications endorsement covers the charges for fraudulent use of a telephone network.

To summarise, our standard policy includes coverage for:

Breach Response services:

- Computer expert services and legal services to help determine the extent of the breach and the steps needed to comply with applicable breach notice laws
- Crisis management and public relations
- Access to educational and loss control information at no charge
- Notification services provided on a number of affected individuals basis, not capped by a monetary amount
- Call centre services for notified individuals
- Breach resolution and mitigation services including
    - credit monitoring
    - Data Patrol services which allows the insured to choose what personal information they want peace of mind about

- Third party liability:

  - Third party information security and privacy coverage
  - Regulatory defence and penalties
  - Website and offline media liability
  - PCI fines, penalties and assessments

Optional extensions available to be added on by endorsement are:

  - First Party Network Cyber BI / Extortion: covers the loss of revenue, the cost of data recovery and investigation of an extortion (or ransomware) attack
  - Fraudulent Transfer: if the insured receives a request for a transfer of funds and processes the payment in good faith but it is in fact a request from a criminal impersonating clients/suppliers then we cover the value of the transfer
  - Telecommunications Fraud: covers the telephone bill for unauthorised charges if someone fraudulently uses your phones (e.g. a cleaner making international calls)

Some limitations of our policy:

  - It is not designed for cyber-crime, it is focused on service provision
  - We do not pay:
    - an actual or alleged breach of your organisation's professional duty
    - a data breach of information that involves information that is collected without explicit consent
    - actual/alleged infringement of any patent, patent rights or trade secret(s)
    - a breach of a merchant services agreement, however this does not apply to PCI fines and penalties
    - loss of funds for transfers unless duped by a hacker
    - bodily injury or property damage
    - war and nuclear risks (but there is no terrorism exclusion)
    - media content which the insured has knowingly published
    - fines, other than PCI fines as per the schedule
    - unencrypted mobile devices
    - sanctioned persons/countries

  - However, there are not exclusions for:
    - terrorism
    - warranties or conditions regarding maintaining security patches or software updates
    - failure of an internet service provider