IIA Cyber Big “I” Program

Does your insurance agency have what it takes to manage a cyber incident?

82%
of cyber incidents involved a human element [1]

Businesses need to be prepared for when a cyber incident occurs.

The average cost of an incident for SMEs is
US $643k [2]

The best way to ensure that you are covered by cyber threats is to have the right cyber insurance for your business.

Why would a cyber-criminal want to hack my small business?

01
Basic IT infrastructure
Very few small businesses have in house IT support; they use an external provider that focuses on setup and server maintenance. Without a cybersecurity plan they can easily be hacked.

02
Easy target
Businesses of all sizes are likely to suffer a cyber incident either due to human element or cyber crime. Many do not recover - 60% of small businesses that suffer a cyber attack are out of business within six months. Firms that build their cyber resilience and have cyber insurance can minimize that risk.

03
Untrained staff
Businesses that don’t train staff on basic Cybersecurity hygiene are more likely to fall victim to a phishing attack or social engineering.

A cyber attack happens every
39 seconds [3]

How am I liable? I’m the victim

Liable for data
You are still liable even if you outsource data handling to a third party. Once a cyber incident occurs as the owner of the data you are obligated to report it and pay the necessary fines and penalties for the negligence.

Legal obligation
You may be legally obligated to notify the affected individuals pursuant to state or federal laws if their personal information or confidential information was taken due to a data breach or security breach.

Human element
The majority of cyber incidents involve a human element; the common tactics are stolen credentials, clicking on a phishing email and simple error. Examples are: Employees working at home or in shared accommodation makes protecting confidential data much harder, as the wi-fi connection is often not fully secure creating an easy path for a cyber criminal to follow.

Packaged policies aren’t up to the task
Your commercial package may have a cyber liability extension, but take a hard look at the coverage it provides. Endorsements typically carry low limits and few options. If first party coverage is provided, limits may be inadequate for the exposure. For third party liability, coverage may fall short in key areas, such as responding to a lawsuit due to cyber incident. Does it address regulatory fines and penalties?

Minimize risk
To minimize risk against cyber threats, we recommend our market leading cyber insurance product, Beazley Breach Response (BBR)

How does BBR protect my business from a cyber incident?

Our product protects against First & Third party loss and eCrime
No one can anticipate the impact of a cyber incident; the coverage that BBR provides your clients is more flexible than most cyber insurance, therefore it minimizes their exposure to cyber risk.

- First party protections consist of a) Business Interruption: financial losses due to a security breach or system failure; b) Data Recovery costs; and c) Cyber Extortion: Negotiation costs and extortion payments associated with a ransomware attack.
- Third party protections consist of claims expenses and damages from a) lawsuits based on a cyber incident; b) regulatory defense and penalties; c) payment card liabilities; and d) media liability
- eCrime provides first party protections against loss of funds due to fraudulent instruction or funds transfer fraud.

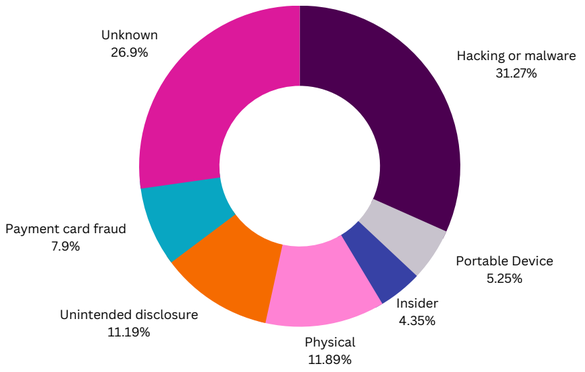
Incident response
Responding to a cyber incident can be costly and complex; incident response is a tower of cover included in our policy. Our incident response includes access to state of the art vendors versed in dealing with the incident. Vendors include: legal services, digital forensics investigators, public relations firms, notification centers and credit monitoring.

beazley

[1] Verizon Data Breach Investigation Report DBIR Report 2022 - Results and Analysis - Not the Human Element | Verizon Business
[2] https://netdiligence.com/cyber-claims-study-2022-report/
[3] https://www.business2community.com/statistics/how-many-cyber-attacks-happen-per-day

BBR helps to protect businesses against cyber risks

Records Breached



https://privacyrights.org/data-breaches

1.993bn
Records breached from 2005-2022

- Hacking or malware- Electronic entry by an outside party
- Portable Device- Lost, discarded or stolen laptop, phone or external hard drive
- Insider- Someone with legitimate access intentionally breaches information- such as an employee or contractor
- Physical loss- Lost, discarded or stolen non- electronic records such as paper documents
- Unintended disclosure- Sensitive information posted publicly on a website, mishandled or sent to the wrong party via email or mail
- Payment card fraud- Fraud involving debit and credit cards that is not accomplished via hacking, eg. Skimming devices
- Unknown

> **"Small businesses believe that their cyber risk will decrease in the future. This perception seems to rely on SMEs evolving their businesses while cybercriminal's approaches remain static, Unfortunately, this is not the case. That's why we recommend our BBR product.**

Ian Fantozzi
CEO - Beazley Digital

> **"Insurance Agents are unique and have intricate day to day operations; it's important to include BBR as a proactive measure in today's digital age to reduce the impact of a potential cyber incident.**

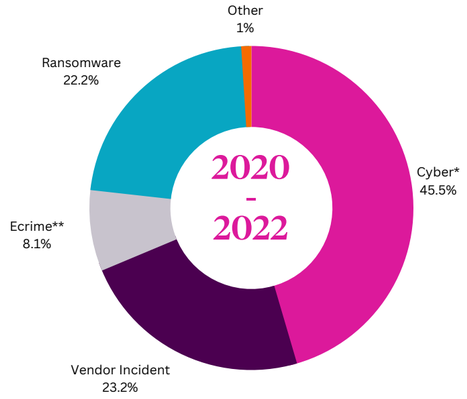
Bolanle Akinrimisi
Claims Focus Group Leader - Small Business Cyber & Technology

Big "I" program

Aside from the competitive pricing, below are the key differences:

- Slot rated coverage for ease of new and renewal business
- Aggressive pricing for risks <$10m revenue including annual premium options less than $600 for risks <$1m revenue
- Flexibility on post bind implementation for required cyber risk controls.
- Dependent Business Interruption/Dependent System failure provided at $250k (standard open market default $100k)
- Three towers of coverage
  - Notification costs based on per person basis
  - Incident response services (legal, forensics, PR/Crisis Management)
  - Third party liability
- Additional Breach Response Limit for additional costs exceeding notification or incident response
- Bespoke fraudulent instruction coverage for Big "I" Program members
- Cyber Extortion retentions at $1,000 (standard open market default $2,500)
- Computer Hardware Replacement Cost, Cryptojacking, and Reputation Loss endorsements are given in each policy to match the overall policy limit

Claims data



*Cyber includes:
- Portable Device
- Insider
- Physical Loss
- Unintended Disclosure

**eCrime Includes:
- Fraudulent instruction
- Funds transfer fraud

beazley