Arlington/ Roe Big “I” Program

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

68%
of cyber incidents involved a human element [1]

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

The average cost of a business interruption incident for smaller firms is
US $467K [2]

After CrowdStrike, we saw how vulnerable businesses are in a globally connected economy. We also saw that businesses with strong cyber security had limited business interruption.

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 smaller firms 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 [3] suffer a cyber attack are out of business within six months. Firms that build their cyber resilience and have comprehensive cyber insurance can minimise 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 attack.

A cyber attack happens every
39 seconds [4]

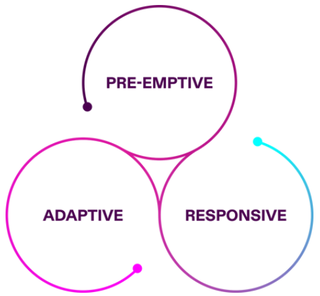
How am I liable? I’m the victim

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 based on whether 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.

Minimize risk
To minimize risk against cyber threats, our Full Spectrum Cyber solution helps pre-empt emerging cyber threats, respond to them, and adapt to new threats as they emerge.



How does Full Spectrum Cyber protect businesses from a cyber incident?

Full Spectrum Cyber includes our flagship cyber product, Beazley Breach Response (BBR) that protects against 1st & 3rd party loss and eCrime.

No-one wants to be at the sharp end of a cyber attack, when your clients partner with us they instantly multiply their own cyber strength.

- 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 defence 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
Your client needs more than the main aggregate to respond to a cyber incident.
We have included an additional limit: Breach Response to help get your client back in the game. The sub limits of this tower include: a) Legal Services b) Digital Forensics c) Call Center d) PR Firm e) Credit Monitoring

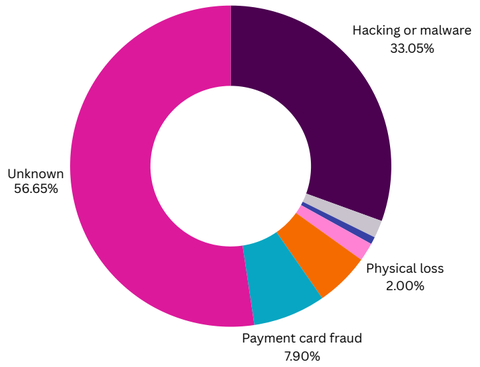
BBR offers more coverage per dollar of premium through multiple towers of coverage.
The benefit of having the services in the breach response tower fall under a separate limit means the services costs won’t erode the main aggregate.

[1] Verizon Data Breach Investigation Report DBIR Report 2024 - Results and Analysis - Not the Human Element | Verizon Business
[2] https://netdiligence.com/cyber-claims-study-2024-report/
[3] https://www.vodafone.co.uk/newscentre/press-release/half-of-smes-experience-surge-in-cyber-attacks-vodafone-research-reveals/
[4] https://www.business2community.com/statistics/how-many-cyber-attacks-happen-per-day

beazley

Full Spectrum Cyber protects businesses against cyber risks

Records Breached



https://privacyrights.org/data-breaches

6.61bn[5]

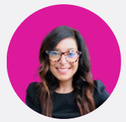
Records breached from 2005-2024

- 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 Full Spectrum Cyber product.**

Ian Fantozzi
CEO - Beazley Digital

> **"Insurance Agents are unique and have intricate day to day operations; it's important to include Full Spectrum Cyber in todays era or accelerating risk to reduce the impact of a potential cyber incident.**



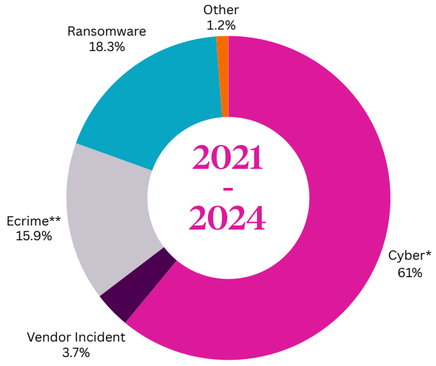
Sarah Lamberg
Head of US Underwriting,
Beazley Digital

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 $300 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[6]



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

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

[5] https://privacyrights.org/data-breaches
[6] Beazley Claims Data- Big 'I' Program

beazley