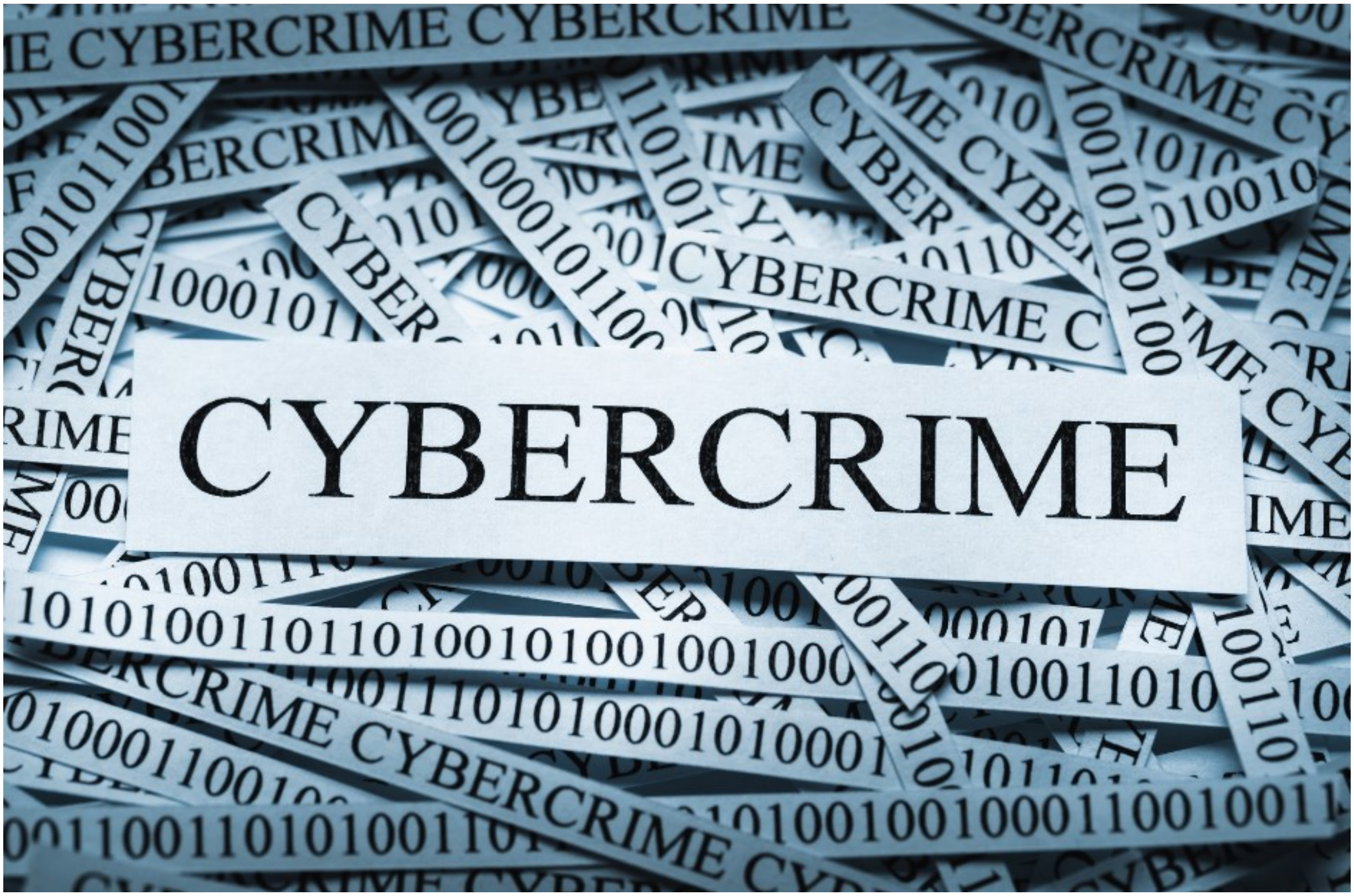
PROFESSIONAL INSURORS
AGENCY, LLC

Cybercrime:
What You Need To Know



Small Businesses Are 400% More Likely to Be Affected By a Cyber Crime than a Natural Disaster

Cybercrime is **criminal activity that either targets or uses a computer, a computer network, or a networked device**. According to the 2021 Thales Data Threat Report, 45% of US companies have experienced a data breach. As companies continue to expand their digital presence the amount of cyber-attacks has grown exponentially, making cybercrime one of the top-rated risks for all companies.

Who needs to be prepared for a cyber attack?

Who is being affected?

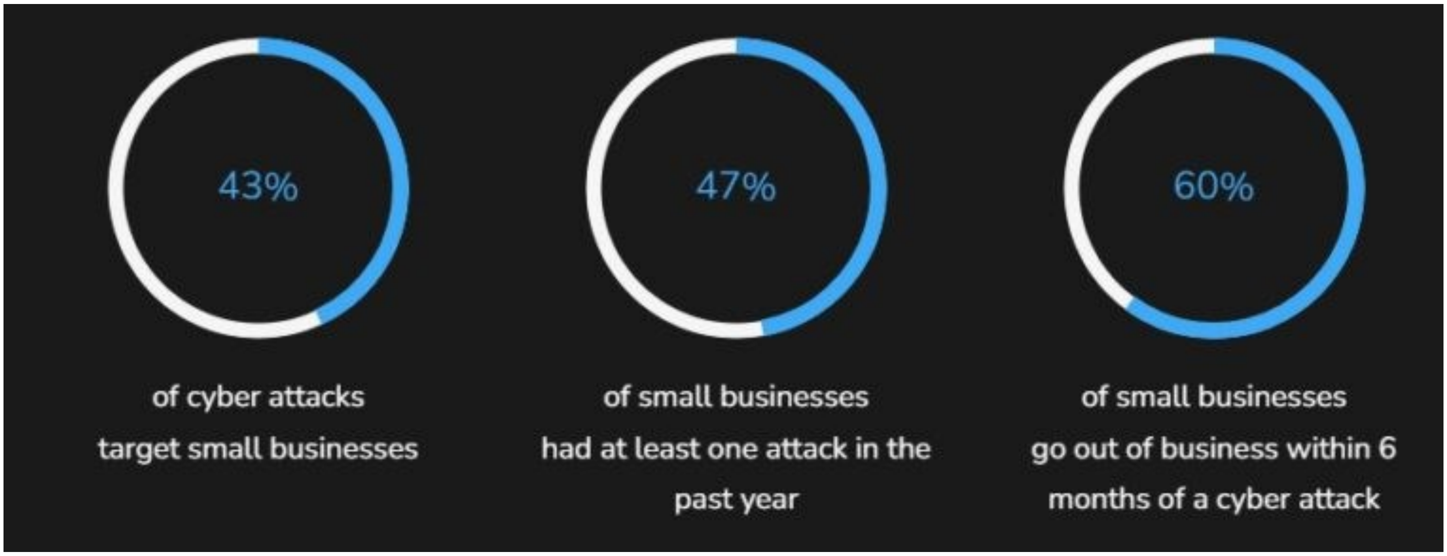
A cyber attack can have devastating effects on any size of business. Still, recently large and even medium-sized companies have amped up their cyber security leaving **small businesses** at the most risk for their digital platforms to be compromised by cybercrime. It is reported that 43% of all cyber and data breaches are targeted at small businesses and about 60% of small businesses effected will be out of business within six months.

Who is being Impacted?

Having a data breach does not only risk your company and employee information being compromised, it can bring about negative ramifications to anyone you have information or data on.

Potentially impacted parties:

- Customers/ Employees
- Competitors
- Vendors
- Patients
- Insureds/ Claimants/ Beneficiaries
- Business Partners



What would cyber insurance cover?

Here is a look at different coverages that would be included in cyber insurance:

Network and Information Security Liability

Coverage for claims arising from unauthorized access to data, failure to provide notification of a data breach when required by law, the transmission of a computer virus, or failure to provide authorized users with access to the company website. This policy includes first-party costs and direct expenses incurred due to the cyber attack such as legal expenses, data restoration, public data expertise, etc..

Communications & Media Liability

Coverage for claims arising from copyright infringement, plagiarism, defamation, libel and slander in electronic content. Media liability also covers both digital advertising (like social media posts) and printed advertising.

Regulatory Defense Expenses

Coverage for governmental claims made as a result of network and information security liability or communications and media liability.

Crisis Management Event Expenses

Coverage for public relations services to mitigate negative publicity.

Security Breach Remediation &
Notification Expense

Coverage for costs associated with notification of individuals breached, credit monitoring, fraud expense reimbursement, and a call center with an optional per person notification available. Computer Program & Electronic Data Restoration Expense Coverage for expenses to restore data lost from system damage due to computer virus or unauthorized access.

Computer Fraud

Coverage for loss of money, securities, or other property due to unauthorized system access.

Funds Transfer Fraud

Coverage for loss of money or securities due to fraudulent transfer instructions to financial institution.
E-commerce Extortion Coverage for money paid as a result of threats made to fraudulently transferred funds, destroyed data, an introduced virus, attack on a system, or disclosure of electronic customer information.

Is your business prepared for a cyber attack?

Risk Prevention

Cyber security audits are a risk prevention measure that help to decrease the likelihood of a future cyber attack. The audit will help detect vulnerabilities and threats within the IT infrastructure and provide a comprehensive analysis and review for your company that will in turn assist in the creation of a preventative plan for your cyber security efforts. **Some cyber security advising services would include Network Security, System Security, Physical Security, and Operational Security.**

Services provided by carriers:

Cyber Insurance carriers will often provide services to clients that will help prevent cybercrime. These services include:

- Discounts on Cyber Protection and Prevention Software
- Tools to build privacy controls, information and IT security programs
- Listing of experts who help customers build/ improve cyber programs
- Data Breach Coaches & Attorney Consultations in the event of a breach
- Statutory, regulatory & case law updates on privacy liability and notification

Average cost of a cyber attack in the U.S.

- Small Business (1- 49 Employees)
  - Average cost recorded: $24K (2021 McAfee Report)
- Small/Medium Business (50-249 Employees)
  - Average cost recorded: $50K
- Medium Business (250-999)
  - Average cost recorded: $133K (2021 McAfee Report)
- Large Business (1,000+ Employees)
  - Average cost recorded: $9.44 million (IBM 2022)

Cybercrime statistics

- The likelihood of a small business being effected by a natural disaster is 14% while the likelihood of a small business being effected by a **cyber attack is 47%.**
- The average cost of a data breach was **$4.24 million in 2021**, the highest average on record.
- Breach costs for companies using strong encryption costs **$1.25 Million less** on average.
- The global cost of cyber crime will be **10.5 trillion by 2025.**