Cyber Risk & Cyber Insurance

PROTECTING BUSINESS, FAMILY, WEALTH, AND REPUTATION IN A CONNECTED WORLD

The digital transformation of the global economy has created unprecedented opportunities, but it has also introduced a new category of risk capable of threatening businesses, families, and personal wealth in ways that would have been unimaginable a decade ago.

Cyber risk is no longer limited to technology departments or large corporations. It has become a financial, operational, reputational, and strategic risk affecting organizations of every size and individuals across every segment of wealth.

A single compromised email account can result in a fraudulent wire transfer. A ransomware attack can halt operations for weeks. A stolen database can trigger regulatory investigations, litigation, and lasting reputational damage. A convincing AI-generated voice or video can deceive even the most experienced professionals.

BUSINESS IMPACTS

- Revenue
- Operations
- Customer relationships
- Employee productivity
- Regulatory obligations
- Brand reputation
- Enterprise value

INDIVIDUAL & FAMILY IMPACTS

- Personal identity
- Investment accounts
- Digital assets
- Reputation
- Family privacy
- Financial security

Cyber insurance has evolved from a specialized coverage into a critical component of a comprehensive risk management strategy. Properly structured cyber insurance provides not only financial protection but also access to specialized resources—including forensic investigators, legal counsel, breach response professionals, crisis communications specialists, and cybersecurity experts.

The most effective cyber strategy combines: prevention + preparedness + protection + recovery

Continued

0826 1666400

THE NEW REALITY: CYBER RISK IS BUSINESS RISK

Historically, organizations viewed cybersecurity as an information technology concern. Today, it belongs in the boardroom.

A cyber event can stop manufacturing lines, lock employees out of critical systems, interrupt revenue collection, expose confidential data, and trigger regulatory obligations—all while eroding the stakeholder confidence that takes years to build.

Cybersecurity failures have grown beyond mere technical problems and become business continuity events with direct financial and reputational consequences.

WHY CYBERCRIMINALS TARGET EVERY ORGANIZATION

Many business owners operate under the assumption that their organization is too small to attract the attention of sophisticated attackers. This assumption creates substantial vulnerability.

Attackers frequently target smaller organizations precisely because they hold valuable financial data, customer records, and banking relationships—while often presenting fewer security barriers than larger enterprises.

THE EVOLUTION OF CYBER THREATS

Ransomware

Ransomware occurs when criminals encrypt systems or data and demand payment for restoration. The consequences extend well beyond the ransom itself:

- Operational shutdown and lost revenue
- Costly data recovery and system restoration
- Customer disruption and lasting reputation damage

Business email compromise

One of the most financially damaging cyber exposures involves fraudulent emails designed to manipulate employees into transferring funds or releasing sensitive information. Common examples include:

- Fake executive wire requests
- Vendor payment changes
- Payroll diversion
- Fraudulent invoices

Continued

Artificial intelligence-enabled fraud

Artificial intelligence has fundamentally changed the threat landscape. Threat actors no longer need to simply steal credentials, they can convincingly impersonate a trusted executive, family member, or advisor.

Modern attacks may include:

- Voice cloning
- Deepfake video
- Sophisticated phishing
- Automated social engineering
- Synthetic identities

Third-party vendor risk

Organizations increasingly depend on external parties—cloud providers, software vendors, payment processors, and supply chain partners—whose security posture directly affects their own.

A company may have strong internal controls and still suffer a significant loss because of a compromised third party.

Cyber risk and enterprise value

For business owners, the most important question is not only: "Can we survive a cyberattack?"

It is: "How will a cyber event impact the value we have spent years building?"

Cyber incidents can affect EBITDA, customer retention, business valuation, financing relationships, acquisition opportunities, and employee confidence. Cyber protection is therefore not just a security decision; it's a component of enterprise preservation.

No single cybersecurity measure eliminates risk entirely. Resilient organizations prepare for the possibility that an incident will occur and build a plan to respond quickly and effectively.

THE ROLE OF CYBER INSURANCE

When prevention is not enough, cyber insurance is designed to help organizations and individuals respond with speed, expertise, and financial support.

A comprehensive cyber policy may provide:

Continued

Financial protection

- Incident response expenses
- Data restoration costs
- Business interruption losses
- Cyber extortion expenses
- Legal defense costs
- Liability claims

Expert response resources

- Digital forensics
- Breach counsel
- Public relations support
- Notification services
- Crisis management professionals

Strategic support

The value of cyber insurance extends beyond reimbursement. In the hours following a cyber event, access to experienced professionals can significantly influence the speed and effectiveness of recovery.

CONCLUSION

Cyber risk is not a technology issue. It is a financial risk, an operational risk, a reputational risk, and—for high-net-worth individuals and families—a deeply personal one.

The assets, relationships, and reputation that take decades to build can be materially impacted by a single event. Organizations and families that invest in preparation before an incident occurs are meaningfully better positioned to protect what matters most.

We encourage you to speak with your advisor to assess your current cyber exposure, review your insurance coverage, and ensure that a response plan is in place before it is needed.

0826 1666400