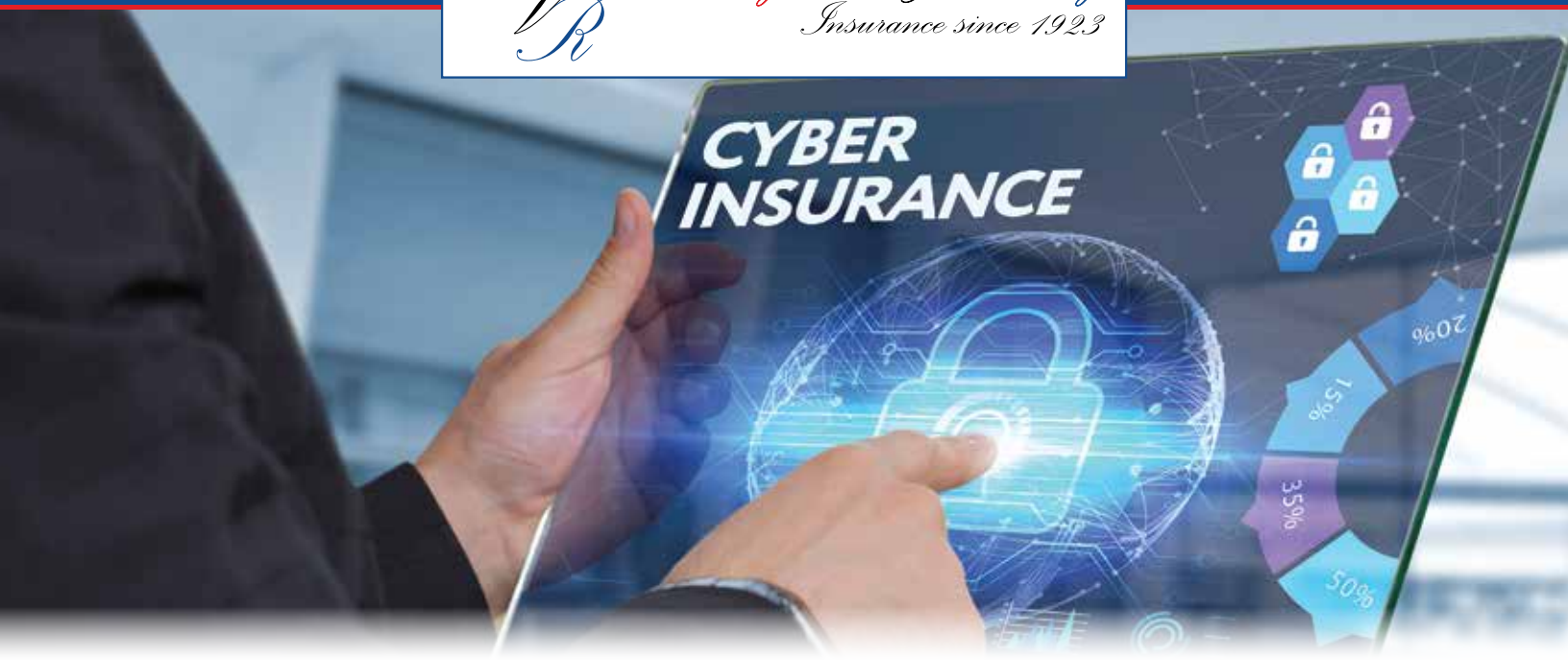
McCartney, Verrino & Rosenberry
Insurance since 1923



Cyber Insurance Solutions For Your Business

Does your company collect credit card information for online sales or maintain a data base of personal information for lead generation? With new threats to computer systems and data emerging every day, it pays to be prepared. Even if your business or organization has taken steps to maintain the security of your data, you may not be keeping up with today's increasingly sophisticated threats.

ONLY 55% of businesses have purchased a cyber insurance policy

What is Cyber Liability Insurance:

Cyber insurance generally covers your business' liability for a data breach involving sensitive customer information, such as Social Security numbers, credit card numbers, account numbers, driver's license numbers and health records. It can also cover:

- Information Security & Privacy Liability
- Privacy Breach Response Services
- Website Media Content Liability
- Cyber Extortion
- First Party Data Protection
- First Party Network Business Interruption
- Fraudulent Instruction
- Electronic Crime

Who Needs Data & Cyber Liability Coverage?

- Accountants
- Consultants
- Contractors
- Hair Salons / Barbers
- Law Firms
- Marketing Companies
- Financial Firms
- Real Estate Agents
- Retailers
- Restaurants

Contact MVR Insurance today to discuss your policy needs

(914) 693-3500

MVRAgency.com

Independent Insurance Agent

MVR Insurance Agency
477 Ashford Avenue
Ardsley, NY 10502

The hard realities of a cyber event:

Phishing Email: Medical Group

An employee of a medical group opened a phishing e-mail that infiltrated their centralized network. Anti-virus software failed to keep out the malicious code, exposing names, addresses, dates-of-birth, medical record numbers, medication, dates of service and diagnoses of 1200 patients. A computer forensics investigator was hired, who determined that PHI (protected health information) had been compromised. The medical group notified the affected individuals and hired a public relations firm in anticipation of bad publicity. Thereafter, The Office for Civil Rights launched an investigation and the medical group was fined as a result of a HIPAA violation for having unsecured access to the network.

An average event of this type could drive the average costs up to $2,810,000 for a business.

Risk Management Tips:

- Specific phishing training program could be implemented to educated employees to recognize a suspicious email.
- Conduct more frequent vulnerability assessments and penetration testing.
- Create, implement and test an incident response plan.

Website Vulnerability: Non-Profit

A Non-Profit experienced a cybersecurity breach that resulted in the inadvertent disclosure of 10,000 donors' personal information. Due to malware on their website server the unauthorized individual was able to gain access to donor information including names, addresses, emails, credit and debit card numbers, security codes and expiration dates.

Computer forensic experts were retained to assist with the investigation. Corrective measures were taken including changing all passwords, implementing additional monitoring and reviewing policies and procedures to ensure that all information was appropriately protected moving forward..

An average event of this type could drive the average costs up to $1,728,000 for a business.

Risk Management Tips:

- Encrypt data at rest on network server.
- Implement more frequent vulnerability assessments and penetration tests.
- Create, implement and test an incident response plan.

Broad economic uncertainty is now the top business concern, jumping from #6 in 2019

47%
said the business environment is becoming riskier

The #2 business concern is cyber risk, and the percentage of business reporting this concern has increased.

BIGGEST CYBER-RELATED BUSINESS CONCERNS:

Security breach

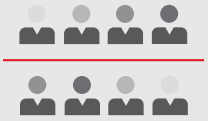
Hacker gaining access to financial systems

Employees putting information at risk

EMERGING CYBER CONCERNS INCLUDE:

Suffering a cyber event, security breach due to employees working remotely

COVID-19 PANDEMIC RAISES NEW REMOTE WORK CONCERNS



The percentage of businesses with at least **40% of employees** working remotely has more than doubled.

Despite heighted concerns about remote working, many businesses admit **NOT IMPLEMENTING BASIC PREVENTION PRACTICES**, such as:

Conducting focused cyber security awareness training

Using Virtual Private Networks (VPN) with multi-factor authentication for remote access

Enhancing cyber security monitoring and early warning protocols

Implementing an Endpoint Detection and Response (EDR) Solution