Innovation Growth Partners Specialty®

CONTACT US

Dave Perkins, RPLU
(508) 848-4263
dave.perkins@igpspecialty.com

Understanding the Most Common Cyber Insurance Claims, with Sample Claims

Cyber incidents are one of the fastest-growing sources of financial loss for organizations of all sizes. While attacks vary, most claims fall into a few core categories. Understanding these helps illustrate where your organization is most exposed—and how cyber insurance responds.

1. Ransomware Attacks

WHAT IT IS:
Cybercriminals gain access to your systems, encrypt your data, and demand payment to restore access or prevent public release of sensitive information.

REAL-WORLD IMPACT:
- Operations can be shut down for days or weeks
- Significant costs to restore systems and data
- Potential reputational damage if data is leaked

SAMPLE CLAIM SCENARIO:
A manufacturing company is hit with ransomware after an employee clicks a phishing email. Their systems are down for 10 days.

- Ransom payment: $750,000
- Business interruption loss: $1,200,000
- Forensics and restoration: $350,000
- **Total Loss: ~$2.3M**

2. Social Engineering / Business Email Compromise (BEC)

WHAT IT IS:
Fraudsters impersonate executives or vendors to trick your organization into transferring funds.

REAL-WORLD IMPACT:
- Unauthorized wire transfers
- Direct financial loss
- Operational disruption

SAMPLE CLAIM SCENARIO:
An accounts payable employee receives an email appearing to be from a trusted vendor requesting updated payment instructions. Funds are wired to a fraudulent account.

- Fraudulent transfer: $480,000
- Recovery/legal costs: $75,000
- **Total Loss: ~$555,000**

3. Phishing and Credential Theft

WHAT IT IS:
Employees unknowingly provide login credentials, allowing attackers to access systems.

REAL-WORLD IMPACT:
- Unauthorized system access
- Potential escalation to ransomware or fraud
- Investigation costs

SAMPLE CLAIM SCENARIO:
An employee's Office 365 credentials are compromised. The attacker accesses email accounts and launches internal phishing campaigns.

- Forensic investigation: $85,000
- System remediation: $40,000
- Legal consultation: $25,000
- **Total Loss: ~$150,000**

4. Data Breaches

WHAT IT IS:
Sensitive data (customer, employee, financial, healthcare) is exposed or stolen.

REAL-WORLD IMPACT:
- Notification requirements
- Regulatory scrutiny
- Lawsuits and reputational harm

SAMPLE CLAIM SCENARIO:
A healthcare provider experiences a breach exposing 75,000 patient records.

- Notification and credit monitoring: $375,000
- Legal and regulatory costs: $600,000
- Settlement: $1,000,000
- **Total Loss: ~$2.0M**

5. Business Interruption

WHAT IT IS:
A cyber event causes a disruption to normal operations.

REAL-WORLD IMPACT:
- Lost revenue
- Ongoing expenses
- Service delivery delays

SAMPLE CLAIM SCENARIO:
A SaaS company experiences a system outage due to a cyberattack affecting its cloud provider.

- Lost revenue: $900,000
- Extra expense to restore operations: $250,000
- **Total Loss: ~$1.15M**

6. Funds Transfer Fraud

WHAT IT IS:
Cybercriminals gain access to banking credentials and initiate unauthorized transfers.

REAL-WORLD IMPACT:
- Direct financial theft
- Limited recovery options

SAMPLE CLAIM SCENARIO:
An attacker gains access to a company's banking platform via compromised credentials and initiates multiple transfers overnight.

- Stolen funds: $620,000
- Recovery/legal costs: $80,000
- **Total Loss: ~$700,000**

7. Cyber Extortion (Non-Ransomware)

WHAT IT IS:
Threat actors demand payment to avoid an attack, data leak, or disruption.

REAL-WORLD IMPACT:
- Pressure to pay to avoid harm
- Response and negotiation costs

SAMPLE CLAIM SCENARIO:
A professional services firm is threatened with the release of stolen client data unless payment is made.

- Extortion payment: $150,000
- Incident response and negotiation: $60,000
- **Total Loss: ~$210,000**

8. Denial of Service (DDoS) Attacks

WHAT IT IS:
Attackers overwhelm systems, causing outages.

REAL-WORLD IMPACT:
- Website downtime
- Lost revenue
- Customer dissatisfaction

SAMPLE CLAIM SCENARIO:
An e-commerce company experiences a multi-day DDoS attack during peak sales season.

- Lost sales: $300,000
- Mitigation services: $75,000
- **Total Loss: ~$375,000**

9. Employee Error or Insider Incidents

WHAT IT IS:
An employee accidentally or intentionally exposes sensitive data.

REAL-WORLD IMPACT:
- Data leaks
- Compliance and legal costs

SAMPLE CLAIM SCENARIO:
An employee mistakenly sends a spreadsheet containing sensitive customer data to the wrong external recipient.

- Notification costs: $120,000
- Legal and consulting fees: $80,000
- **Total Loss: ~$200,000**

10. Third-Party / Vendor Breaches

WHAT IT IS:
A vendor or service provider is compromised, impacting your organization.

REAL-WORLD IMPACT:
- Indirect data exposure
- Operational disruption
- Limited control over response

SAMPLE CLAIM SCENARIO:
A payroll provider suffers a breach exposing employee data of multiple clients.

- Notification and monitoring: $220,000
- Legal expenses: $130,000
- **Total Loss: ~$350,000**

Key Takeaways

- Most cyber incidents stem from **human error or compromised credentials**
- The primary areas of exposure are:
  - Operational disruption (ransomware, outages)
  - Financial fraud (social engineering, funds transfer)
  - Data exposure (breaches, privacy events)
- Losses can range from **six figures to several million dollars,** depending on severity and response time

How Cyber Insurance Helps

A well-structured cyber insurance program can:

- Cover ransomware, fraud, and incident response costs
- Protect against business interruption losses
- Provide expert legal, forensic, and crisis management support
- Help your organization recover quickly and minimize long-term impact

©2026 Innovation Growth Partners Specialty, LLC | igpspecialty.com