



Michael S. George, CIC
317.735.4072
mgeorge@amj-ins.com

Cyber Claim Examples

Ransomware / Cyber Extortion

A company provides customers with hosting and connectivity solutions, including Internet access, hosted environments for internal and external facing websites, hosted application services, etc. Access is restricted to authorized users through assigned user identification with user-controlled passwords.

Situation: The company receives a threat from an unknown third party that will cause an interruption of the company's network and unauthorized access to the data stored on the company's servers. After investigating the threat, it's determined that the threat is credible and the company makes an extortion payment to the person or group making the threat.

Challenge: The cyber extortion threat results in the following expenses for the company:
\$25,000 cyber extortion expenses

Resolution: The total expenses incurred by the insurer were \$25,000.

Medical Records Hacked

When an insured hospital was notified by the United States Secret Service of a potential HIPAA breach that may have compromised data for 40,000 patients, our experienced team of dedicated cyber claims specialists quickly engaged a breach coach and a forensic investigator. As a result, the insured had knowledgeable partners to provide advice, handle notifications, create a call center, offer patients access to identity-monitoring products, and ensure the incident was properly reported to the state regulatory agencies.

Malware Data Breach

A regional retail computer system was compromised when a third party sent a malware program via email to a number of employees. The invasive software allowed the third party to access the system and capture the names, addresses and credit card numbers for more than 500,000 customers.

Stolen Laptop

An employee's company laptop containing private customer information is stolen from his home. As a result, customers sue the company for damages resulting from alleged failure to protect their private financial information.



eNetwork Interruption

When an insured with hundreds of outlets experienced a 48-hour systems failure at the start of a busy holiday weekend due to a hack, the insured could not process sales and payments quickly and its operations were disrupted. The response team added expertise, assisted the retailer in retaining a forensic accountant, and verified the lost sales calculation for the holiday weekend. The insured was also reimbursed for approximately \$200,000 of lost sales incurred after the waiting period applicable to the network interruption caused by a malicious attack.

"Our agency was targeted and hit by a cyber-attack a few weeks ago. BIZLock's response was immediate, comprehensive and heartwarming."
- Karen N., Owner, Insurance Agency

Rogue Employee


An employee stole a donor's credit card information from a non-profit that resulted in a forensics investigation, a lawsuit and a PCI fine. The per record insured cost for that incident was \$50,000.

Data Theft From Server

When a server and hard drive maintained by a company acquired by an insured were stolen, sensitive data for nearly 45,000 individuals was compromised. The insured was provided \$1 million to cover notification, public relations, and other incident-related services.

Cyber Claim Examples

Payment Card Industry (PCI) Related Fines and Penalties



A large movie theater operation had its transaction processing systems at a specific movie theater location hacked. Thieves collected card data from one machine over the course of one year before the Secret Service notified the movie theater owners. A forensic investigation ensued. Mastercard issued PCI related contractual fines and penalties in excess of \$250,000 to the payment processor, who in-turn contractually passed the obligation to the movie theater owners. The insurance aggregate limit was reached at \$100,000.

Pharmacy Procedural Error

A woman purchased a used computer from a pharmacy. The computer still contained the prescription records, including names, addresses, social security numbers, and medication lists of pharmacy customers. The cost of notifying affected parties per state law totaled nearly \$110,000. Two lawsuits were filed: one alleged damages in excess of \$200,000 from a party who claimed she lost her job as a result of the disclosure; the second alleged the plaintiff's identity was stolen, and the costs of correction and emotional distress exceeded \$100,000.

Media Liability Exposure

Two employees at a Pizza chain posted derogatory comments and a video online. The video captured their employee uniforms and work location.

"We were hacked and the hackers gained access to sensitive records. We called BIZLock and their Incident Response On-Demand was timely, effective and certainly comforting. We were very satisfied. We encourage every small business to purchase cyber insurance. It is sad how easy it is to suffer from a breach, which makes having cyber insurance a simple decision." - Dawn C., Michigan



Please Note: This document provides summary information only. Insurance coverage is provided by an A rated carrier(s) and is subject to specific terms, limitations and exclusions. Terms may also vary by state and may not be available in all states. Data extracted from industry cases, IFI cases and examples provided by industry insurers and players, including AIG.
©2017 Identity Fraud, Inc.



Cyber Risk Management & Insurance Overview

Contents

1. **Prevent** - Essential Risk Management [1]
2. **Protect** - Cyber Insurance Coverage [3]
3. **Respond** - Incident Response On-Demand [4]

BIZLock® is the nation's premier cyber insurance and risk management suite empowering small businesses to better **prevent, protect against and respond** to cybercrime. The program is aimed at addressing what most small businesses need, which is an affordable solution that delivers essential risk management tools to mitigate exposures, 24/7 access to experts to respond to incidents and the financial protection provided by the industry's largest insurer of cyber insurance - AIG.

Prevent - Essential Risk Management

Small businesses face an array of cyber security challenges daily. Every BIZLock program includes important risk management tools tailored for small businesses. Best practices, compliance and contractual obligations require prevention practices to help address and mitigate cyber risks. With BIZLock, depending on the limit of insurance you secure, you can take advantage of the following benefits:

24/7 Tech Support Hotline

Tech support for your office is just a phone call away! Remote support allows users to get technical problems resolved immediately and affordably. Support is provided for more than just computers. Technicians are available 24 hours a day, 7 days a week to help resolve the following types of issues:

- Diagnostics
- Basic Network Setup & Support
- PC & Mac Maintenance & Optimization
- Virus & Spyware Removal
- Data Backup Assistance
- Operating System Issues
- Software Setup & Troubleshoot
- Printers & Scanners Support
- Internet & Email Issues
- WiFi & Router Setup
- & More!

Keystroke Encryption Software

Keystroke Encryption Software helps protect your identity and sensitive business activities by encrypting your computer keystrokes and hiding them from hackers, malware and keylogger's intent on stealing your sensitive credentials while using the internet.

Human Resources Module

Every BIZLock program includes unlimited access to education and training that focuses on cyber security, privacy and identity theft. Applicants, employees and managers each have separate levels of modules. **BIZLock Pro** includes pre-employment screening and behavioral assessments.



Risk Assessments / Written Policies / Templates / Incident Response Plan

To support information security efforts, we provide our guides, templates and self-assessments for your unlimited use. We understand that information security is complex and that some companies are just beginning their information security efforts, while others are more mature. That's why we provide our self-assessment protocols in four distinct levels, Beginner I/ II, Intermediate and Advanced. Because not all businesses have the same exposures or experience, our protocols are designed to add value and meet your specific level of need.

"We built BIZLock to deliver the peace of mind, resources and insurance protection you need to reinforce your prudence and to help ensure you survive a cyber incident."
–Tom Widman, Founder, CEO

Cyber Edge Risk Tool

Certain BIZLock programs with higher limits include access to the Cyber Edge Risk Tool providing access to advanced information security and compliance education and discounts on Risk Analytics' AutoShun® crime fighting technology.

E-Risk Hub

Sponsored by AIG, the E-Risk Hub provides advanced risk management tools, policies, procedures, risk assessments and more...

Protect - Cyber Insurance Coverage

Does your small business collect, use and/or disclose personal information? Do you operate a website? If so, it is entirely appropriate to have insurance to defend and cover the specialty cyber, privacy and information related liability exposures that exist. When it comes to data risks, our primary message is *"Do your best, and insure the rest"*. We understand that protecting computers and information against loss or theft is difficult. Because data risks will always remain, no matter how diligent your defenses, insurance presents a cost effective vehicle to transfer risk. We believe that cyber liability insurance is a fundamental need of every business, especially in today's risk environment.

Cyber Liability Insurance

Coverage is provided for any failure to protect private information in the care, custody or control of the insured, its information holder, or for which the insured is legally responsible, including costs/forensic costs to investigate. Private information includes personal and non-public business information (e.g. trade secrets). Information can be paper, electronic, unencrypted, mobile, in the cloud or with contractors.

Regulatory Fines & Penalties

Coverage is provided for defending against regulatory actions and resulting fines and penalties arising from a covered privacy event.

Cyber Extortion / Ransomware

Coverage for costs to end, terminate or investigate cyber extortion threats.



Media Liability

Coverage for wrongful acts (an act, error, omission, negligent supervision, misstatement or misleading statement by an insured) in connection with material on an internet site owned by the insured or related social media.

Incident Response / Event Management / Mitigation Expenses

Coverage is provided for law firm/breach coach, PR firm, forensics, consumer notifications and remedies including education, assistance, insurance and credit file or identity monitoring. Mitigation expenses are provided up to 50% of the liability limit.

Payment Card Industry (PCI)

Coverage for PCI-DSS assessment from payment card association members as a result of an organization's failure to comply with PCI-DSS. Limits provided up to \$250,000.

eNetwork Interruption / Data Reconstruction

Separate breach expense coverage is provided for e-business network interruption and reconstruction of data. (Separate Limits)

Business Identity Fraud Insurance

Provides expense reimbursement to protect against the abuse and fraudulent use of sensitive Business Identity Information or BII. (Available with BIZLock Pro)

Employee Personal Identity Protection

Automatic identity protection includes VRS Elite Unlimited fraud victim resolution services, risk management education, and discounts on upgrades, all combined with \$15,000 identity insurance. No enrollment necessary. VRS Hotline: 1-844-432-LOCK (1-844-432-5625)

Respond - Incident Response On-Demand™

Having an elite team of experts available via our **Incident Response On-Demand™** is indispensable when faced with a data catastrophe or cyber event. Whether the business has 5 customers or 5 million, our capabilities to respond to a data breach are seasoned and flexible. Our team of experts will seek to assess and contain the loss, preserve evidence, and support continuity of the business. Experienced in data forensics, investigators have the ability to support law enforcement and pursue independent investigations, while our notification, victim assistance and identity protection monitoring programs can be activated nationwide within 24-hours.





Program Summary

(For organizations having
less than 51 FTE employees
and \$10 Million in sales)



Data Theft Risk Management and Insurance

Organizations are at risk of having a data breach on multiple fronts — negligence, a rogue employee, stolen equipment, or a network security failure. If the proper insurance protection is not secured before a data breach occurs, the future of the business could be in jeopardy due to extensive recovery and reimbursement costs as well as damage to its reputation.

BIZLock provides organizations the expert assistance and financial relief needed to confront a data breach head on. With a host of value-added consultancy services available before, during and after a data breach incident; and financial assistance in the event a covered breach occurs, BIZLock is the comprehensive solution organizations need to ensure a data breach incident does not challenge their future.

Program Highlights:

Prevention

- Mobile security app (for ios and Android devices)
- Computer Vulnerability Scans (Internal)
- Unlimited Access to Employee Education Modules
- Risk Assessments, Written Policies/Templates, Incident Response Plan
- Keystroke Encryption Software
- Loss Mitigation / Event Management including Law Firm/Breach Coach, PR Firm, Forensics, Consumer Notifications and Consumer Remedies for identity theft education and assistance, victim cost reimbursement insurance and credit file or identity monitoring (sub limit 50% of liability limit).

Protection

- Cyber / Breach / Privacy Legal Liability and Defense Coverage
 - Limit: up to \$1 million aggregate / year
 - Retention: \$1,000 per incident
 - Loss/Theft of Personal and/or Business Data
 - Failure to Disclose/Notify
 - Regulatory Fines and Penalties
 - Cyber Extortion
 - PCI DSS Fines and Related Contractual Obligations (\$250,000 sublimit)
 - Web Site / Media Liability for libel, slander and certain related web site risks
- Breach Expense Protection for eBusiness Network Interruption and Data Reconstruction. Separate limits provided up to \$500,000 (Retention: \$1,000).
- Employee Personal Identity Protection (Automatic)
 - Victim Resolution Services (VRS) and more
 - \$15,000 limit / \$0 deductible

Response

- Data Breach Incident Response On-Demand™ (iROD) 24/7

BIZLock® is owned and exclusively administered by Identity Fraud, Inc.

Please Note: This document provides summary information only. The program is provided pursuant to the IFI Customer Agreement and may not be available in all states. Terms may also vary by state. Insurance coverage is provided by an A rated carrier(s) and is subject to specific terms, limitations and exclusions. Liability insurance is provided pursuant to your active membership in the Data Theft Risk Purchasing Group (RPG) on a claims made basis, covering valid claims first occurring after the original policy inception date (retroactive date). Please note there is a nominal fee of \$1.00 per term for the RPG that is allocated to the RPG by the program administrator, Identity Fraud, Inc. from the proceeds of your purchase.

Michael S. George, CIC
317.735.4072
mgeorge@amj-ins.com

