



What's one of the greatest risks facing your clients? **Cyber Risk.**

Small Businesses Face Large Scale Cyber Exposures

When it comes to data breach incidents, it's true that large organizations tend to get all the headlines. Back-to-back news articles shed awareness on enormous cybercrime vulnerabilities and losses. This often results in the public believing that small organizations are immune from these risks. Many individuals and small businesses have a mindset that "it won't happen to me". However, industry statistics indicate the contrary. Small businesses are being attacked at alarming rates, in part, due to the relative ease of theft and abuse. And while large organizations get all the attention when a data breach or cyber event occurs, small businesses remain the most susceptible to these catastrophic events.



A recent National Cyber Security Alliance study found that 60 percent of small firms go out of business within six months of incurring a data breach.² Having protection for cyber risks is now a fundamental need and smart choice, that is, if it is not already being mandated by business vendor contracts. With data being easily lost and stolen (from insiders and out), insurance coverage is needed to help a business stay in business. It is no longer a question of "if" a business will have a cyber incident or data loss, but "when".

1. Symantec, 2014 Internet Security Threat Report, 6 (Apr. 2014), available at http://www.itu.int/en/ITU-D/Cybersecurity/Documents/Symantec_annual_internet_threat_report_ITU2014.pdf.

2. The Denver Post, 2016 60% of small companies that suffer a cyber attack are out of business within six months., 23 (Oct. 2016), available at <http://www.denverpost.com/2016/10/23/small-companies-cyber-attack-out-of-business/>

5 reasons small organizations need cybercrime protection from BIZLock.

1. Cyber threats are running rampant.

Small business organizations are being preyed upon by criminals as 'low hanging fruit'. Thieves are aware that small businesses lack cyber security sophistication, and may seek to profit off this. Risks and exposures exist wherever computers exist or information is collected. Sensitive, personally identifiable information (PII) of customers on computer systems, laptops, smart phones, external (thumb) drives, cloud data providers and paper office files all contain information that is very valuable to ID thieves and hackers. Loss can easily result from a simple accident, or data stolen in transit via email, web browsers and even the postal service. Data held by vendors, independent contractors or work-from-home employees are also exposures. Cyber incidents often occur as a result of negligence of trusted, experienced employees, the lack of data security and updates, and malicious hacking from ID thieves or rogue employees.

2. Small organizations need to optimize their time and money.

BIZLock delivers comprehensive, affordable protection that helps organizations maximize their investment in cyber protection. You don't need to spend six figures and all of your time on security to have prudent protection. Most organizations simply don't have the time or financial resources necessary to stop every attack. Rather, organizations need to focus on their customers, employees and generating revenues to sustain the business. That's why every BIZLock program maximizes its deliverables and provides three essential areas of risk management that help Prevent, Protect and Respond to the evolving cyber threats faced in our daily operations.

3. Cyber Insurance is essential for every business.

We live in the computer and information age and as large scale data breaches have proven, no organization can ever be 100% secure from fraud or negligence. When catastrophe does strike, there is no substitute for having cyber insurance as the final layer of security. Cyber Insurance can help protect and insure against the following:

- Third Party Cyber Liability & Expenses
- Regulatory Fines and Penalties
- Payment Card Industry (PCI) Fines and Penalties
- Media/Website liability
- Data destruction
- eBusiness Network Interruption
- Cyber Extortion
- Breach forensic investigations, Public Relations management, Legal Services, Incident Notifications and Credit Monitoring Services



4. Coverage can be bound instantly.

Time and money are valuable to small organizations and therefore, securing cyber insurance needs to be as simple as possible. Our quote/bind/print platform allows brokers to bind accounts in real time. Once bound, access to policy documents is provided immediately inside our agency dashboard. Because program pricing is pre-arranged based on the revenue size of an account and the desired limit of coverage, it makes securing coverage easy. For example, if a client has \$2MM in annual gross sales and desires a \$1 Million limit, BIZLock and all of its program benefits, costs about \$1,000 per year.

5. We've been managing cyber risks for more than 20 years.

Having an elite team 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 will seek to assess and contain the loss, preserve evidence, and support continuity of the business. Experienced in data forensics, investigators are able 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.

Cyber claims arise from many diverse angles.

- Malicious hacking of a system shutting down computer systems for an extended period of time resulting in loss of income and extra expenses
- A disgruntled employee spreads a virus into a computer system destroying data (and backup sources) resulting in expenses to investigate and recreate data
- Teenage hacker sabotages data network with Crypto-Locker type malware and demands an extortion fee of \$50,000 to unlock your own data
- Extortion demands of \$25,000 to prevent your sensitive customer data from being released on the internet to identity thieves and the general public
- Lost laptop containing sensitive personal information of customers results in a data breach requiring investigation, notification and credit monitoring expenses
- Lost patient health information results in a HIPAA regulatory fine
- Credit card processing encrypted POS payment system has a virus resulting in credit card data breach. Visa/MasterCard (PCI) fines and penalties mount
- Customer data is breached, class action lawsuit filed. Duty to defend policy responds

Cybercrime Protection and Insurance for Business



Broker Access and Tools	Customer (Insured) Risk Tools
<p>Visit www.bizlock.net/login (Or your sponsor site or contact us)</p>	<p>Insureds have access to our Customer Center at www.bizlock.net/login where important risk management tools are provided (at no additional cost).</p>
<p>Retrieve policy forms, applications, videos & webinars for training staff; brochures, videos and webinars to share with clients/prospects</p>	<p>The Human Resources Module (HR) provides unlimited access to Information Security related education for applicants, employees and management.</p>
<p>Solicit all accounts at one time and/or at each renewal term</p>	<p>The Information Security Module provides several risk assessments (Beginner to Advanced) and Information Security policy templates.</p>
<p>Visit www.aig.com/mobileapp</p>	<p>The Information Technology Module bundles important technologies. Higher limit programs obtain additional benefits (e.g. Bronze, Silver, Gold and Platinum), including the AIG e-Risk HUB.</p> <p>AIG's eRisk Hub is an online platform where up to three (3) executive staff will have access to i) risk manager tools, ii) law firm breach coach, iii) learning center, iv) eRisk resources, and v) news center - cyber risk stories, security and compliance blogs, news, events and more.</p>
<p>Call 844-432-LOCK (5625) for Q&A</p>	<p>The insured has the option to access their policy documents online.</p> <p>Incident Response On-Demand™ is available to the insured 24/7 by calling 844-432-LOCK (5625).</p> <p>All full-time employees are automatically enrolled in Core Identity Protection®, while part-time employees have access to VRS Elite Unlimited Fraud Resolution Services. For any questions about fraud or for any type of identity theft or fraud, - no matter how it is caused - employees should call 866-4-IDFRAUD (866-443-3728).</p>



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.

© 2017 Identity Fraud, Inc. All rights reserved. BIZLock is owned and exclusively administered by Identity Fraud, Inc. 05/17