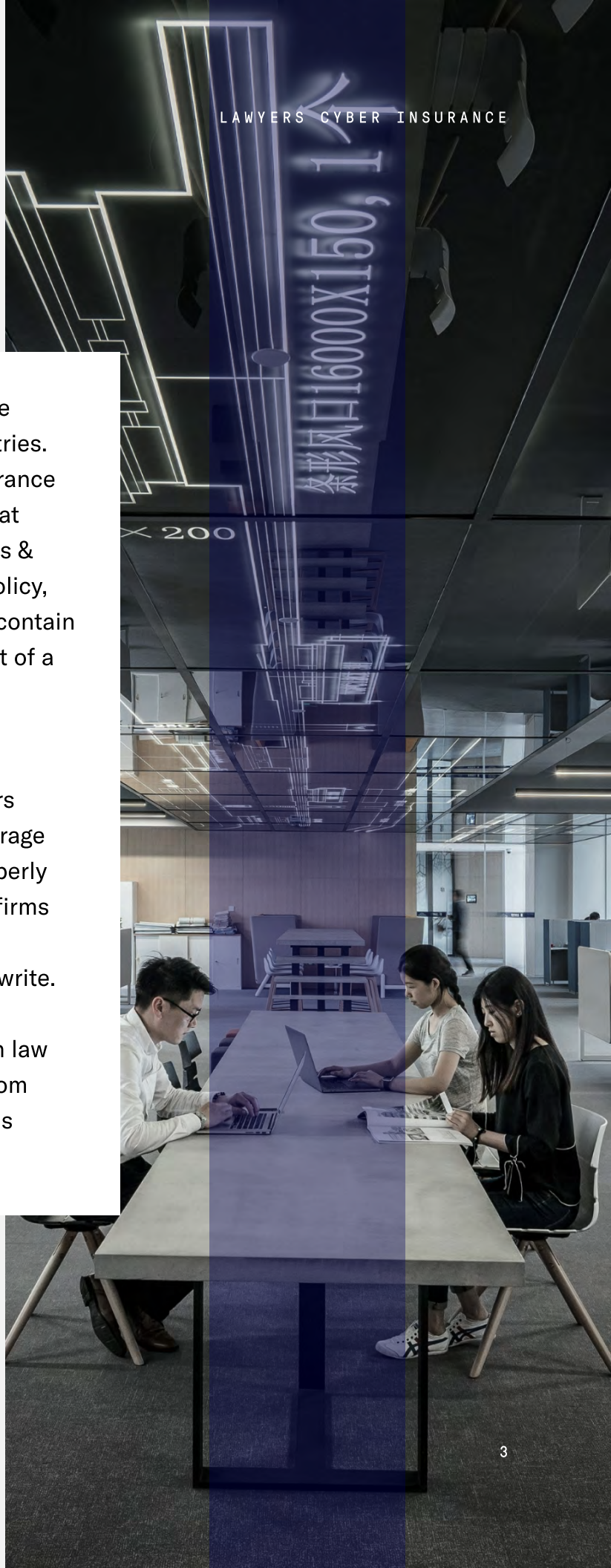
at bay

Lawyers Cyber Insurance

Contents

©2020 At-Bay. All rights reserved. This document is intended for information purposes only and does not modify or invalidate any of the provisions, exclusions, terms or conditions of the policy and endorsements. For specific terms and conditions, please refer to the coverage form.

at bay

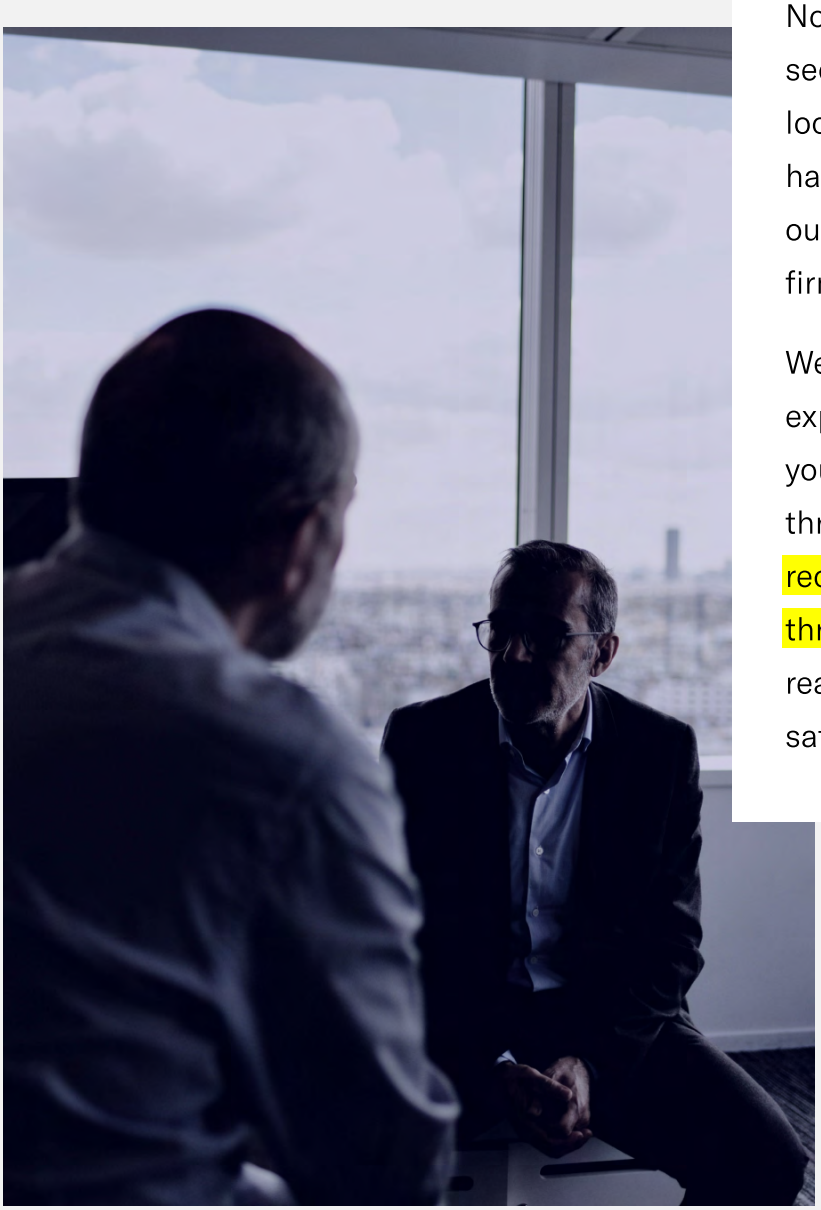


Cyber risk has been ranked the number one concern for risk managers across all industries. However, it is a commonly overlooked insurance purchase because of the misconception that cyber risk is always covered under an Errors & Omissions, General Liability, or Property policy, when it isn't. These policies nearly always contain affirmative exclusions for claims arising out of a cyber-related incident.

Law firms are not favorable cyber risks for traditional insurance carriers. Many insurers refuse or are reluctant to offer crucial coverage because they don't understand how to properly evaluate the cyber security posture of law firms and are unable to recommend security improvements that make it a better risk to write.

This white paper outlines the threats which law firms face, the coverage that is available from At-Bay, and claims examples specific to this industry.

Law firms surprisingly, and typically, have weak cyber security.



Not all firms have weak cyber security practices, but our ability to look at a company's security from a hacker's perspective, coupled with our analysis of thousands of law firms, has confirmed that most do.

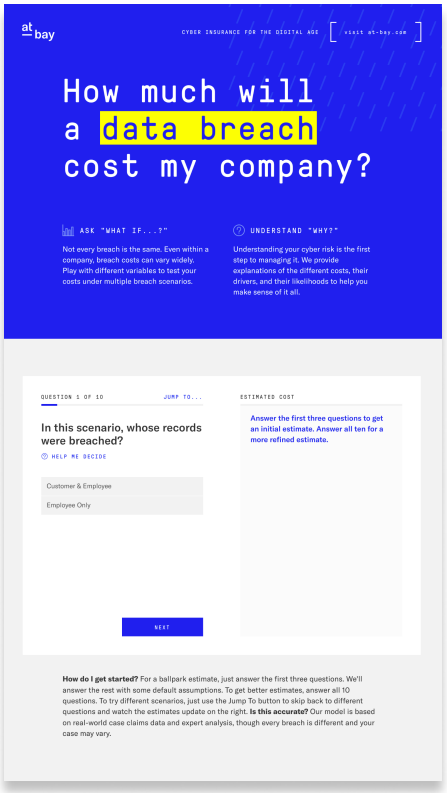
We use our deep bench in security expertise to continuously monitor your technology stack for potential threats. By making recommendations and talking through your vulnerabilities in real-time, we're able to keep you safe and informed.

Confidential Information

Keeping the personally identifiable information (PII) of your clients and even employees comes with risk—losing extremely sensitive case information could be disastrous.

Do you collect and store email addresses, Social Security numbers, payment data, passports, drivers' licenses, etc.? This confidential information is most prone to identity attacks. If these records are lost or compromised by any means, you are legally required to notify these individuals, and the costs can be devastating to your bottom line.

Click below to calculate the amount a data breach could cost your firm:



https://www.at-bay.com/data-breach-calculator/

Social Engineering

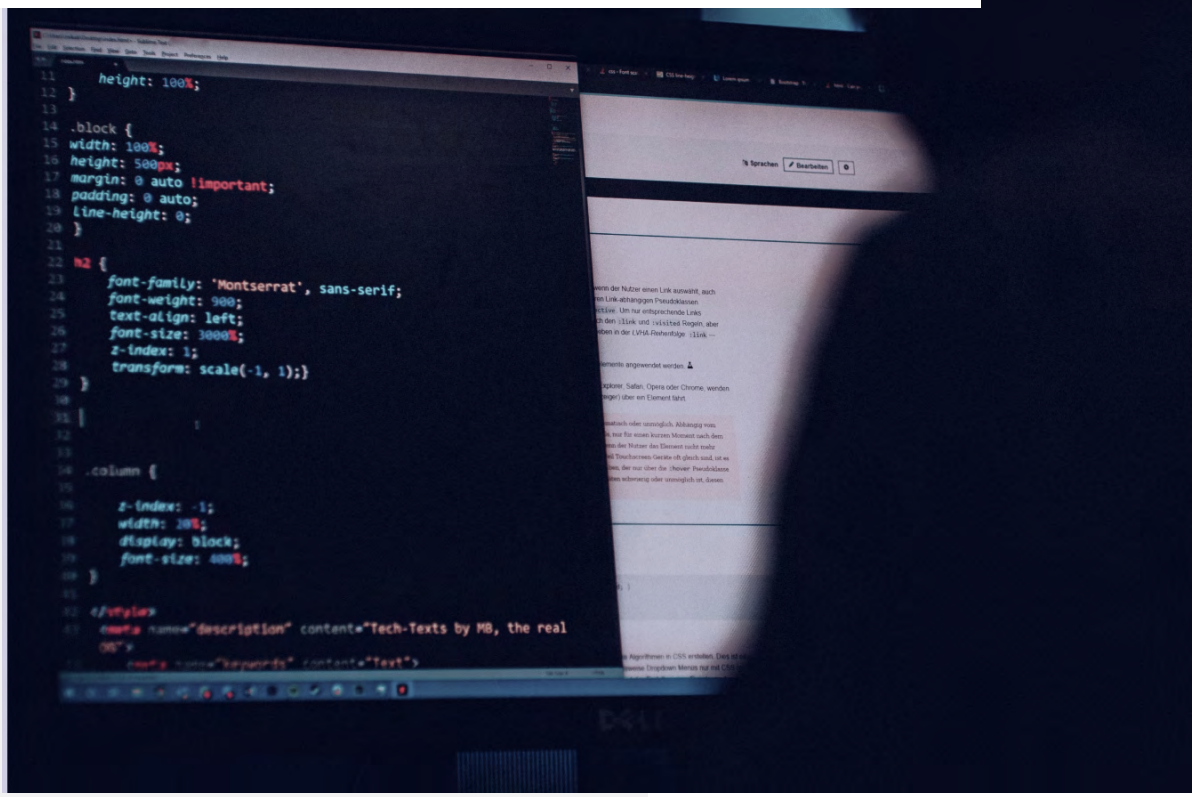
Social engineering insurance covers scenarios in which an attacker tricks an employee into transferring funds, securities, or protected personal information to someone the employee believes to be the intended recipient—normally a client, vendor, or executive. Considering the human response involved in these situations, most insurers will not offer social engineering coverage to law firms because the risk is simply too high. At-Bay looks at your exposures differently.

When was the last time you trained all employees on phishing, social engineering, suspicious emails, and malware infested email attachments? All it takes is one employee to click on the wrong attachment and in an instant, your systems have been breached. Do you always check the validity of your client's banking information when wiring funds? If not, you could be inadvertently transferring funds to a bad actor. The average amount of fraudulent wire transfers we see on the front lines exceeds $100,000.

Ransomware

Ransomware is the latest buzz in insurance and is most commonly tied to extortion. Ransomware generally occurs when an attacker infiltrates your systems, finds your critical data, and encrypts it so you can't access it. To access your critical data, the attacker demands a ransom in crypto currency. The industry has learned that those who pay ransoms frequently get added to a list titled 'These Companies Have Insurance and Will Pay Ransoms' sold by the bad actor on the dark web.

These ransomware demands come with various degrees of legitimacy. At-Bay is able to assess the threat and mobilize the experts you need to appropriately respond to the situation.



Insurance for the digital age.

We at **At-Bay** are proud to be the only insurer with the technical expertise to manage risk across your entire technology stack, to take an unbiased view in navigating security solutions, and most importantly to align financially with your business through our motivation to keep you secure.

At-Bay is building a new kind of insurance company, designed from the ground up to manage the unique risks associated with doing business in the digital age. We employ a team of security professionals who complement our skilled insurance team. We built a fully automated reconnaissance engine which maps out all of your externally facing technology assets, running each one against thousands of vulnerabilities, updated continuously to stay ahead of the newest attacks. Any time a new vulnerability is found in any one of the hundreds of technologies in your stack, At-Bay is there to notify you of the issue and help you address it. This service is free for every client as part of your insurance coverage. As your partner, we have clearly aligned incentives to help you avoid risk and empower you to **embrace technology fearlessly.**

Our Coverage

Full prior acts (Retroactive Date scheduled as "Not Applicable"

Full limits Coverage for both Direct and Contingent System Failure

Full limits Reputational Harm for both real and "fake news"

Pollution Liability Coverage

Enhanced Settlement Provision (90/10)

$100k Affirmative Voluntary Notification Costs

Affirmative Pay-On-Behalf Intent (First-Party)

$25k HIPAA/HiTECH Betterment Coverage

$250k Invoice Manipulation Coverage

***$250k Coverage for Financial Fraud,** including Social Engineering Crime and Computer Crime

$250k Contingent Bodily Injury Coverage

$1M Additional Breach Costs Outside the Aggregate

Cryptojacking & Utility Coverage up to full limits of insurance

Voluntary Shutdown

No hourly waiting or qualifying periods for our Direct and Contingent Business Interruption coverages

Explicit GDPR and CCPA Coverage

Hardware Replacement (also known as Bricking) up to the full limits of insurance

Full limits for Information Privacy, Regulatory Fines, Breach Response, PCI Fines and Penalties, Business Interruption, Contingent Business Interruption, Cyber Extortion, and Media Liability.

Coverage underwritten by HSB Specialty Insurance company, rated A++ Superior by A.M. Best Company.

*** coverage depdendent on applicant's security controls.

©2020 At-Bay. All rights reserved. This document is intended for information purposes only and does not modify or invalidate any of the provisions, exclusions, terms or conditions of the policy and endorsements. For specific 7 terms and conditions, please refer to the coverage form.

Claims Examples

CONFIDENTIAL INFORMATION

A partner in a law firm accidentally distributed an excel file containing confidential litigation logs of 1,000 cases to the wrong email chain and inadvertently emailed this document to an unintended recipient. This excel file contained the names, date of birth, SSN, and confidential case information of the firm's clients. The law firm did not realize their mistake until the recipient of the email notified the law firm of the error.

TOTAL COST TO THE CLIENT:

$25,000	Breach Coach
$60,000	Forensics
$30,000	Crisis Management
$4,500	Notification
$1,800	Call Center
$900	Credit Monitoring
$280,000	Regulatory Fines & Defense
$402,200	$366 per record

Claims Examples

WIRE TRANSFER

An employee at a law firm received an email from someone they believed to be the Chief Financial Officer requesting the company transfer $95,000 to an overseas bank account to pay a third-party vendor. The email did not look suspicious to the employee, and the location of the bank account was familiar. A few days later, the employee followed up with the CFO finding it strange that the CFO had not mentioned the transfer to them, only to discover that the CFO had no knowledge of the wire transfer. The CFO's email had been compromised. The bad actor meticulously monitored the behavior, tone, and activities of the CFO before perfectly executing the phishing scam!

TOTAL COST TO THE CLIENT:

$95,000	Wire Transfer
$35,000	Forensics
$130,000	

Claims Examples

RANSOMWARE

Every employee at a medium to large law firm received an email titled “I love you” with an attachment that looked like a PDF. The law firm did not have adequate email security in place to filter these types of emails, so a few employees clicked on the attachment to see what the email was about. Once the attachment was opened, a form of malicious malware was downloaded onto the law firm’s servers. The malware immediately sent a message to the IT department, demanding the company to pay 10 BTC in the next 12 hours otherwise their systems would be locked down forever and no employee would be able to access the firm’s data. Because the law firm had not backed up their sensitive data, they were forced to pay the ransom. The firm coordinated with their insurer, who negotiated with the bad actor to receive the encryption key that allowed them to recover their files.

TOTAL COST TO THE CLIENT:

$100,000	Ransom
$58,000	Forensics
$9,000	Legal Consultant Fees
$6,000	Breach Coach
$18,000	Reconstitution of Data
$191,000	