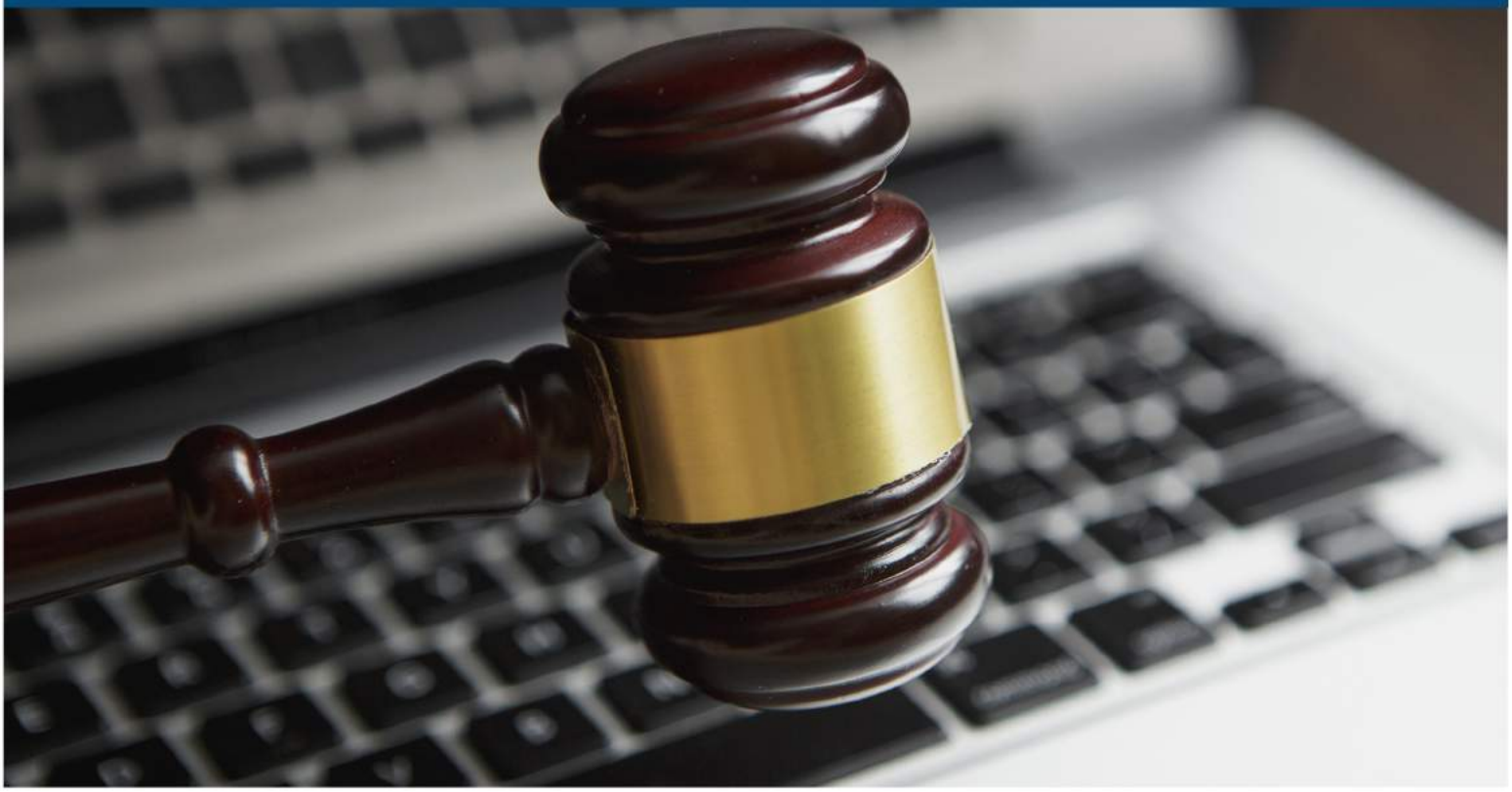
bis BUSINESS INFORMATION SOLUTIONS

Getting IT done.

Reduce the risk of an inadequate cybersecurity malpractice suit…



THE ULTIMATE CYBERSECURITY GUIDE

for Law Firms on Preventing Unauthorized Access of Client Information by Hackers

Business Information Solutions, Inc. | www.askbis.com | Phone: 251.410.7601

BUSINESS INFORMATION SOLUTIONS
We Get IT Done!

CYBER SECURITY

40% of law firms were breached in 2016 and didn't even know it

LOGICFORCE REPORT

THE IMPORTANCE OF CYBER SECURITY IN THE LEGAL INDUSTRY

Law firms have an abundance of data and hackers know it! Not only do they have access to clients' personal information like social security numbers, but firms also have court documents, mergers and acquisitions data, financial records and other information that would deal a devastating blow to a client if it were exposed. A data breach or cyber attack could pose an even greater risk to the firm itself by damaging its reputation or even resulting in a malpractice lawsuit being filed against them.

Although legal is not the most targeted industry, many law firms still fall victim to cyber attacks with about one in five being hacked; and, the majority of those breaches were smaller firms with 10 to 49 attorneys. Since confidentiality is of utmost importance when it comes to the attorney-client relationship, it's crucial that law firms create a strong offense against hackers to protect their clients...

CYBERSECURITY MALPRACTICE

CLAIMS AGAINST LAW FIRMS

RUDOLF V. SHAYNE, DACHS, STANISCI, CORKER & SAUER

Malpractice claim brought against a law firm for cybersecurity negligence

Cybersecurity and the Lawyer's Standard of Care, ABA

SHORE V. JOHNSON & BELL

The first class action lawsuit against a law firm for inadequate cyber security although there was no breach

Cybersecurity and the Lawyer's Standard of Care, ABA

MILLARD V. DORAN

A malpractice suit where the law firm's email was allegedly hacked and resulted in hackers wiring $1.9 million from the client's account

Cybersecurity and the Lawyer's Standard of Care, ABA

bis Getting IT done.

HOW TO SECURE CLIENT DATA FROM HACKERS

Law firms are now coming under fire for not adequately protecting clients' data. In fact, there have been multiple malpractice lawsuits filed against firms for data breaches and even for the possibility of a data breach. Due to the importance of confidentiality in their every day work, the legal industry has had to take a more guarded approach against hackers.

In order to properly secure client information, every law firm should implement a proactive, data breach prevention strategy. Our in-house, Certified Information Systems Security Professional (CISSP) has carefully designed an easy 6-step approach to minimize or even eliminate the risk of a breach.

6 KEY STEPS TO PROTECT CLIENT INFORMATION

IDENTIFY CONFIDENTIAL INFORMATION
Know what data you have and what needs to be protected.

PERFORM A YEARLY NETWORK AUDIT
Evaluate your network for vulnerabilities that could put you at risk.

DEVELOP A BACKUP AND DISASTER RECOVERY PLAN
Establish a disaster recovery plan to prevent data loss.

IMPLEMENT EMPLOYEE SECURITY TRAINING
Require frequent security training on the latest cyber threats.

EXECUTE A DEFENSE-IN-DEPTH STRATEGY
Prevent data breaches with layered cyber security protection.

CREATE A DATA BREACH INCIDENT RESPONSE PLAN
Devise an incident response plan and communicate with your staff so that you can successfully handle a data breach.

DEFENSE-IN-DEPTH STRATEGY

This defense-in-depth strategy is a multi-layer approach to securing your network and client data. Each step is crucial to providing adequate cyber security fro your firm's clients.

Patch Management with Malware Detection

Patch 150+ software through an automated critical update service.

SIEM and SOC Monitoring

Meet your PCI, HIPAA and SOC compliances while getting real time alerts when your systems behave outside the baseline security policy.

FINISH

Data Backup and Business Continuity

Backup your encrypted data both locally and in the cloud.

Cloud-Based DNS Firewall

Stop threats in the cloud before they enter your network by preventing malicious Internet connections.

DPI/SSL Firewall

Protect the entire network at the gateway since 60% of network traffic now encrypted.

Next Gen End Point Security

Use cloud-based protection against zero-day exploits and targeted behavioral attacks.

Security Awareness Training with Dark Web Scanning

Create a strong offense by training your staff and running a dark web scan since 95% of successful attacks are caused by the end-user.

Password Management

Use password best practices along with password complexity rules, account lock out and automated screen lock policies.

START

Advanced Threat Protection (ATP) Email

Filter and encrypt emails to safeguard against the 70-80% of attacks that originate in your inbox.

bis Getting IT done.

bis Getting IT done.

DON'T GET HACKED!

Every 40 seconds, a business is hit with ransomware!

My name is Phillip Long and I'm the CEO of Business Information Solutions. As a cyber security specialist, I continue to see law firms who are blindsided by cyber attacks that damage their reputation and cost them a fortune.

It's my duty to warn as many organizations as possible against the real threats they face so that they can protect everything they have worked so hard to build. Even if you've already got a guy, it's extremely important to get a second opinion because you don't want to wait until it's too late!

{FREE} 4-POINT CYBERSECURITY AUDIT

Point 1: Dark Web Scan

Point 2: Network Evaluation

Point 3: Simulated Phishing Email

Point 4: Security Training

This offer includes:

- ✔ Free network vulnerability report
- ✔ One-page technology roadmap
- ✔ Dark web scan results
- ✔ Defense-in-depth security strategy
- ✔ Report with employee testing scores
- ✔ Copy of my book

Call 251-410-7601, email security@askbis.com or visit www.askbis.com/4-point-audit to redeem this offer!

*Only 1 offer per company. Must have at least 10 computers.