LEGAL SPOTLIGHT

BlackHat Consultants
Information Security Solutions

PROFESSIONAL IT SUPPORT FOR GROWING BUSINESSES

SPECIAL POINTS OF INTEREST:

- **New law affects all Massachusetts businesses starting Jan 1st, 2009.**
- **Adopting good security standards is proven to save companies money.**
- **Being able to document compliance can be a "get out of jail free card" in a lawsuit**

INSIDE THIS ISSUE:

New Law Mandates Security Standards

After a few false starts, the Commonwealth of Massachusetts now has a strong, new law to protect its residents. However, what this really means can be somewhat puzzling for business owners.

The new law (201 CMR 17.00: Standards for The Protection of Personal Information of Residents of the Commonwealth) requires businesses to ensure the protection of Personally Identifiable Information (PII) on all Massachusetts residents.

This affects the entire range of businesses from sole proprietors to large corporations. Additionally, since non-profits also deal with PII, these entities must follow the same compliance requirements as businesses.

This new law requires all Massachusetts businesses and organizations to develop and implement a comprehensive information security program. The law is similar to that of other states. The goal is to have businesses secure their operations so that it makes it harder for identity theft and hacking incidents to occur.

Regardless of the industry you are in, you must become compliant with this new law.

On a positive note for businesses, by enacting the steps to become compliant with Information Security laws, an organization can reap long-term savings from the beneficial effects of a good security program. These savings include less virus outbreaks, decreased downtime from data loss or corruption, a better educated workforce, and decreased reactive computer and network support costs.

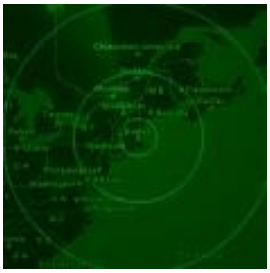
What is your plan to make your business compliant?

The Perfect Storm: What Is On Your Radar?

When the economy is down, there is a trend to see more lawsuits. Some are to right wrongs, but a frightening number are frivolous lawsuits that are filed with the intent to make money from an incident.

Non-compliance with a law or industry requirement sets the stage for a negligence lawsuit. In the realm of Information Security compliance, you are "guilty until proven innocent" by the very nature of having to prove you did everything correctly.

This new law and a weakening economy create a "perfect storm" for frivolous lawsuits against businesses. The best protection is clearly taking preventative steps to both become compliant and to maintain compliance.



Don't get caught in the storm—plan ahead and be safe!

But I Have Business Insurance

Does your business have a "negligence loophole" in your insurance policy?

'Most business owners are unaware that non-compliance means negligence and negligence is not covered by insurance"

Business insurance is a necessity that no one will refute. Another common understanding is that insurers will look for loopholes to keep from paying out on a policy.

Most business owners are unaware of how Information Security lapses can negate their coverage entirely. This gap in coverage has the proven ability to put a company out of business for good.

How can this be? It is actually quite simple. Laws and industry regulations are known standards. When a business is required to be compliant, it must take steps to ensure due care and due diligence in meeting those requirements. This is the legal standard for determining responsible behavior by a business or individual.

Failing to follow or document due care and due diligence is evidence of negligent behavior. In a world of lawsuits, the ability to show documentation that your business doing what is required can be the difference between a having insurance cover the costs of a data breach and getting on with business or going bankrupt from being denied insurance coverage and having to pay the costs out of pocket.

What costs are typical in a non-compliance incident? Costs include everything from legal fees, breach notification costs such as press releases, fines, and lost business revenue from both the business interruption as well as the loss of customer base.

When a company can prove compliance, through well documented policies and procedures, insurance works as it is supposed to by protecting the company from damaging lawsuits and expenses.

The weakness for most businesses is that they assume too much when it comes to their insurance coverage. Since the best defense is a strong offense, it is advisable to sit down with your insurance agent and ask the hard questions about your coverage with this new law.

You will find that your coverage will depend on your ability to prove compliance with the law.

What Is Really Required?

How protected is your company?

Within the *Standards for The Protection of Personal Information of Residents of the Commonwealth*, there are multiple requirements.

Every comprehensive information security program shall include, but shall not be limited to:

(a) Designating an employee to be in charge of the information security program
(b) Identifying and assessing internal and external risks.
(c) Developing security policies for employees who telecommute.
(d) Imposing disciplinary measures for violations.
(e) Preventing terminated employees from accessing data.
(f) Taking reasonable steps to verify that service providers are equally compliant.
(g) Collecting the minimum amount of personal information necessary to accomplish the job.
(h) Inventorying all paper and electronic data to identify personal information.
(i) Regularly monitoring and auditing employee access to personal information
(j) Reviewing the scope of the security measures at least annually
(k) Documenting responsive actions with any incident involving a security breach

A graphical example of this can be seen on the following page.

MANDATORY COMPLIANCE REQUIREMENTS	MA State Law	PCI DSS	HIPAA	FACTA	GLBA	SOX
Information Security policies for employees & contractors	•	•	•	•	•	•
Take preventative action to protect against anticipated threats	•	•	•	•	•	•
Protect data from unauthorized access or disclosure	•	•	•	•	•	•
Appoint Information Security officer to oversee security program	•	•	•	•	•	•
Ensure the security & confidentiality of data	•	•	•	•	•	•
Secure destruction / disposal of physical & electronic data	•	•	•	•		
Implement a security awareness & training program	•	•	•	•		
Perform risk assessments	•	•	•	•		
Regularly test security systems & processes	•	•	•	•		
Adjust the security program according to risk management	•	•	•	•		
Monitor the effectiveness of all safeguards	•	•	•	•		
Ensure service providers are compliant with requirements	•	•	•	•		
Develop a contingency / data breach plan	•	•	•	•		
Ensure employees acknowledgement policies in writing	•	•	•			
Encrypt sensitive data during storage & transmission	•	•	•			
Restrict access to sensitive data by business need-to-know	•	•	•			
Conduct inventory and maintain accountability of sensitive data	•	•	•			
Track and monitor all access to network resources & data	•	•	•			•
Ensure default / vendor-supplied passwords are not used	•	•				
Encrypt all transmitted records and files containing sensitive data	•	•				
Maintain updated computer operating systems	•	•				
Maintain active & updated antivirus software	•	•				
Ensure network is protected by a hardware firewall	•	•				
Ensure wireless security minimum standards		•				
Develop and maintain secure systems & applications		•				
Assign users a unique ID & password for network access		•				
Perform quarterly vulnerability assessments		•				
Complete an annual compliance questionnaire		•				
Maintain current network diagram & hardware inventory		•				
Change user passwords no less than every 90 days		•				
Ensure complex passwords are used with at least 7 characters		•				
Maintain data for specific time periods			•			•
Measures to ensure data integrity is maintained						•
APPLICABLE PROFESSIONS	**COMPLIANCE CONCERNS**					
CPAs, bookkeepers and financial planners	•	•			•	
Realtors, title and real estate settlement companies	•	•			•	
Consumer credit agencies and debt collectors	•	•		•	•	
Mortgage brokers, lenders and automobile dealers	•	•		•		
Service providers (if they use credit reports)	•	•		•		
Lawyers	•	•	•	•	•	
Medical, dental, and mental health professionals	•	•	•			
Publicly traded companies	•	•			•	•
Businesses that maintain personal information on any resident	•					

MA	201 CMR 17.00 (Massachusetts State law)
PCI DSS	Payment Card Industry (Industry-specific)
HIPAA	Medical Privacy (Federal Law)
FACTA	Credit Privacy (Federal law)
GLBA	Financial Privacy (Federal law)
SOX	Public Companies (Federal law)

BlackHat Consultants
Information Security Solutions

BlackHat Consultants
19725 SW 49th Ave, Suite 201
Portland, OR 97062

(503) 427-8006 Office
(302) 635-8423 eFax

Customer Support:
support@BlackHatConsultants.com

Please visit us at:
www.BlackHatConsultants.com

Most computer and network consultants do not specialize in Information Security, so there is generally a void of attention shown to both regulatory & non-regulatory compliance. BlackHat Consultants was developed by a Certified Information Systems Security Professional (CISSP) and former military officer.

Our mission at BlackHat Consultants is to fill this void and provide growing businesses with a set of professionally written Information Security policies that their existing IT provider will be able to enact without issue.

Information Security is necessary for organizations to protect not only their clients, but their employees and partners. Information Security affects everyone in business.

Why BlackHat Consultants?

In our ongoing commitment to provide excellent customer service, we feel compelled to make sure Small and Medium Businesses (SMBs) have the support they need for their Information Technology and Information Security needs. This is where we want to make a difference and decrease the liabilities associated with being a smaller business.

Our beliefs at BlackHat Consultants.com include:

1. We are here to help businesses that lack this special knowledge & experience
2. Information Security is too important to be left to amateurs
3. Every company needs robust security policies, procedures, standards, and guidelines
4. Our solution should be affordable to all businesses and simple to obtain
5. Security policies must be based on industry-recognized best practices & standards
6. Security policies should be written in a business-context so users can understand them

Never trust your security needs to amateurs.