

# Legal Implications Regarding Data Security

*Having your data in the clouds is smart business, but having your head in the clouds about data security could have serious legal implications.*

By: *William S. Cherry III, Attorney at Manning Fulton*

The Internet, networked applications, and cloud computing have created a more equitable competitive environment for *Small and Mid-Sized Businesses* to expand their organizations and improve customer experiences while controlling costs. But with the rapid growth of cyber commerce and unprecedented levels of capturing, storing, and sharing of electronic data, comes an equally rapid increase in security threats. From Internet attacks (malicious content, authentication, and privilege issues) to physical system attacks and theft, cyber threats and privacy breaches are on



the rise. Private industry has answered the call with an increasingly sophisticated \$30 billion cyber security and privacy industry that is

helping government agencies, companies, and individuals contend with the growing array of threats and concerns.

The legal system has been slower to respond with the majority of regulations imposed thus far specifically directed to highly regulated industries such as financial services, healthcare,

and utilities. To date, remedies within the legal system relating to cyber-theft and privacy breaches have been addressed by pre-existing laws

**MANNING FULTON**<sup>®</sup>

WE FOCUS ON WHAT MATTERS  Attorneys

3605 Glenwood Avenue  
Suite 500  
Raleigh, North Carolina 27612  
(919) 787-8880  
[www.manningfulton.com](http://www.manningfulton.com)

## Related Links

Manning Fulton & Skinner, P.A.  
[www.manningfulton.com](http://www.manningfulton.com)

Windstream Hosted Solutions  
[www.windstreambusiness.com](http://www.windstreambusiness.com)

XL Insurance  
[xlgroup.com/insurance](http://xlgroup.com/insurance)

CrowdStrike  
[www.crowdstrike.com](http://www.crowdstrike.com)

North Carolina Bankers  
Association  
[www.ncbankers.org](http://www.ncbankers.org)

North Carolina Healthcare  
Information and Communications  
Alliance (NCHICA)  
[www.nchica.org](http://www.nchica.org)

Small Business Association  
[www.sba.gov](http://www.sba.gov)



and regulations such as the Consumer Fraud and Abuse Act (CFAA, 18 U.S.C. §1030), the Stored Communications Act (SCA, 18 U.S.C. §2702), and the Fair Credit Reporting Act (FRCA, 15 U.S.C. §1861(b)). However, a survey of case law indicates that success in claims under these acts is limited. Other potential remedies include civil causes of action such as claims for negligence, breach of contract and breach of fiduciary duty, depending on the factual circumstances of each individual attack or breach.

We predict a significant increase in the tangential suits and claims against companies participating in these highly regulated industries as suppliers and subcontractors. There will be expectations within companies in these industries that suppliers and subcontractors will be taking necessary steps to protect their own business, their client's business, and their customer base. We have heard from lawmakers on both the Federal and State levels, that this coming year may well see major developments in the legal regime governing data security and privacy. This

means more laws and regulations will be put into place for businesses that operate and rely on data. The increased threats, and subsequent laws and regulations to address them, has put additional pressure on businesses to be secure, reliable and law-abiding with respect to the data that they own, store or are privy to at any point.

Businesses should be aware of the North Carolina Identity Theft Protection Act (NCITPA, N.C. Gen. Stat. §75-60 to §75-66). Enacted in 2005, a primary purpose of the NCITPA was to provide greater protection of personal and confidential information of consumers. Importantly, for small and mid-size businesses, the NCITPA sets forth certain notification requirements to customers in the event that a business becomes aware of a security breach. Failure to follow the notification requirements set forth in the NCITPA may result in liability and monetary penalties for businesses in situations in

*We predict a significant increase in the tangential suits and claims against companies participating in these highly regulated industries as suppliers and subcontractors.*



which they would not otherwise be responsible for the security breach.

Equally important for small to mid-sized businesses is the need to evaluate their particular situation, client base, and industries in which they operate and take a common sense approach to protecting

themselves. To do this, small to mid-sized businesses will need more education to understand the implications that new legislation and industry regulations pertaining to data security breaches can have on their organizations and how they are connected directly and/or indirectly.

---

## WHERE DO SMALL AND MID-SIZED BUSINESSES TURN TO UNDERSTAND THEIR RESPONSIBILITIES WITHIN THE DATA SECURITY AND PRIVACY ISSUE?

### GOVERNMENT AGENCIES

such as the *Small Business Administration* and the *Federal Trade Commission* on the federal level and *North Carolina Department of Justice* for state related information can be excellent resources for business owners in understanding the implications of federal and state laws.

### TRADE ORGANIZATIONS

like the *North Carolina Healthcare Information and Communications Alliance (NCHICA)* and the *North Carolina Bankers Association* track these issues and help educate their industry

members as well as business associates and suppliers operating in these highly regulated industries.

Two industry specific articles that help educate on the sophisticated nature of data security in *Healthcare* and *Finance* are:

- [Avoiding Financial Penalties and Loss of Reputation: Creating, Managing, and Enforcing a Healthcare Data Security Policy \(NCHICA\)](#)



- [Potential Liability for Financial Institutions Stemming from Cyber Attacks](#) (*CrowdStrike*)

**DATA AND ENTERPRISE SERVICE PROVIDERS** for networking, data storage, internet, voice, and other technology needs can be one of the best partners to help prepare you for the next generation of operating in the cyber world. A good data and communications service provider can help you prevent disaster and gain efficiencies and productivity that will add to the bottom line.

- [IT as a Service : Convergence is happening on the Network](#) (*Windstream Hosted Solutions*)

**INSURANCE CARRIERS** have designed products to help companies cope with the increasing frequency and severity of data security and privacy issues.

These products are designed to help companies cope with liability and litigation costs. Whether there will be a

"boom" in cyber security insurance remains to be seen, but 2013 saw an increase in privacy and data security claims. As laws progress, we will most certainly see the influence of newly adaptive insurance products and policies on lawsuits and business disputes.



- [Minimizing Risks from Increased Vulnerability in the Technology Age](#) (*XL Insurance*)

Lastly, **LEGAL ADVISORS** who work within the regulatory and legal structures governing business law in the area of technology, cyber security, and e-commerce are valuable advisors to companies defining their responsibilities under these laws. They can perform internal audits to evaluate these issues and help prepare preventative action strategies that fit within your operating plan. When necessary, attorneys defend claims of liability in matters related to breach of privacy and stolen data.



To discuss any of these issues from a legal standpoint and to ensure you are protected in your business dealings from a data security and privacy standpoint, contact [Will Cherry](#) at (919) 787-8880 or [cherry@manningfulton.com](mailto:cherry@manningfulton.com).

## Special Thanks to Contributing Authors

 <p>MANNING FULTON® WE FOCUS ON WHAT MATTERS Attorneys</p>	<p><a href="#">David A. Harlow</a> (Attorney)</p>
 <p>NCHICA</p>	<p>Holt Anderson (Executive Director)</p>
 <p>CROWDSTRIKE</p>	<p>Matt Dahl (Manager, Global Threat Analysis/Legal Counsel)</p>
 <p>windstream® Hosted Solutions</p>	<p>Windstream (Corporate Communications)</p>
 <p>XL Group Insurance Reinsurance</p>	<p>John Coletti (Chief Underwriting Officer, Cyber &amp; Technology, XL Insurance)</p>

