



# PROTECTING CONFIDENTIAL INFORMATION IN THE AGE OF CYBERATTACKS: DO YOU HAVE A PLAN?

Jason M. Storck  
Wilson Sonsini Goodrich & Rosati  
Direct: (512) 338-5435  
[jstorck@wsgr.com](mailto:jstorck@wsgr.com)

Wilson Sonsini Goodrich & Rosati  
PROFESSIONAL CORPORATION

1



## OVERVIEW

- Guarding against cyberattacks and mitigating their effects is of critical importance for organizations
- In the age of cyberattacks, organizations must understand and comply with cybersecurity legal requirements and enforcement mechanisms
- Developing an effective cybersecurity plan is the best protection against the risks of a cyberattack
- Employee awareness, policies, training, and problem reporting processes are integral to an effective cybersecurity plan

Wilson Sonsini Goodrich & Rosati  
PROFESSIONAL CORPORATION

2



## WHY IS CYBERSECURITY IMPORTANT?

*LifeLock to Pay \$113 Million to Settle  
FTC Charges*

– Wall Street Journal



*Target settles for \$39 million over  
data breach*

– CNN Money

*Yahoo's Top Lawyer Resigns and  
C.E.O. Marissa Mayer Loses Bonus in  
Wake of Hack*

– New York Times



*Home Depot to Pay Banks  
\$25 Million in Data Breach  
Settlement*

– Fortune



Wilson Sonzini Goodrich & Rowat  
PROFESSIONAL CORPORATION

3



## COSTS OF A DATA BREACH

- Average cost to U.S. companies in FY2016 was *\$7 million total per company, or \$221 per record*
- **Financial costs:** notifications, ID theft coverage, technology remediation, investigations, class actions
- **Business and reputation costs:**
  - Front page news
  - Major business disruptions and loss of data
  - Loss of customer trust
  - Harm to brand image
  - Heightened scrutiny for any future missteps

Wilson Sonzini Goodrich & Rowat  
PROFESSIONAL CORPORATION

4



## DATA SECURITY REGULATORS



- **Federal Trade Commission (FTC)**
  - Main enforcer of “reasonable data security”
  - Brought over 60 cases since 2002



- **Industry-specific Agencies (FDIC, SEC, FCC, HHS)**
  - Increasing interest in data security by agencies that oversee financial and healthcare industries
  - Sectoral regulations: GLBA, HIPAA, SOX



- **State Attorneys General**
  - States are enacting data security legislation and bringing enforcement actions



- **Payment Card Industry**
  - Payment card companies (e.g., Visa, MasterCard) enforce Payment Card Industry Data Security Standards (PCI-DSS)



## LEGAL REQUIREMENTS & ENFORCEMENT

- **FTC Enforcement**
  - Has cybersecurity enforcement authority under Section 5 of the FTC Act.
  - Brings cybersecurity unfairness actions and cybersecurity deception actions
- **State Laws**
  - Many states have consumer protection laws that mirror the FTC Act
  - Texas Biometric Law
  - Massachusetts law requiring implementation of information security program similar to type of program sought by FTC
- **Regulated Industries**
  - Financial Information – regulated by Gramm-Leach Bliley Act (GLBA) and Payment Card Industry Data Security Standards (PCI-DSS)
  - Health Information –Health Insurance Portability and Accountability Act (HIPAA); Health Information Technology for Economic and Clinical Health (HITECH) Act
  - Children’s Information – Children’s Online Privacy Protection Act (COPPA)

Find the full text of this and thousands of other resources from leading experts in dozens of legal practice areas in the [UT Law CLE eLibrary \(utcle.org/elibrary\)](http://utcle.org/elibrary)

## Title search: Protecting Confidential Information in the Age of Cyber Attacks: Do You Have a Plan?

Also available as part of the eCourse

[2017 Labor and Employment Law eConference](#)

First appeared as part of the conference materials for the  
24<sup>th</sup> Annual Labor and Employment Law Conference session

"Protecting Confidential Information in the Age of Cyber Attacks: Do You Have a Plan?"