GIBBONS

DATA PRIVACY & CYBERSECURITY TRAINING MANUAL

An overview of training programs offered by attorneys on the Gibbons Data Privacy & Security Task Force

www.gibbonslaw.com

Data Privacy & Cybersecurity Training

Cybersecurity is a 21st century phenomenon that affects each of us at work and at home. With technological advances occurring on an almost daily basis, an ever-increasing volume of confidential and proprietary business and personal data is stored, accessed, and shared electronically – not only within an organization, but with clients, customers, vendors, and other third parties that are integral to operations. Unfortunately, these technological advances also bring a range of new threats to the security of that stored data. These ever-emerging threats have a direct impact on the way an organization uses computers, the internet, phones, and tablets, as well as the policies and practices governing the use of technology and access to data.

Preparation is the best defense.

Data privacy and cybersecurity training educates all employees about best practices and the organization's responsibilities to prevent a security breach. In addition, appropriate training enables supervisory employees to understand the obligations and potential liabilities under the applicable state and federal laws in the event of a data breach. In short, training can help an organization prevent a data breach and, if a breach occurs, minimize the impact to ongoing operations and the potential for liability to regulators and third parties.

WHAT KIND OF COMPANIES SHOULD CONDUCT DATA PRIVACY AND CYBERSECURITY TRAINING FOR THEIR EMPLOYEES?

Because all organizations are vulnerable to security breaches, all organizations – large or small, for-profit or charitable – should train their employees. Different types of training are available for supervisory employees versus non-supervisory employees. At a minimum, all of the organization's employees should receive basic security and compliance training at least once every two years.

WHAT ARE THE BENEFITS OF HAVING AN ATTORNEY CONDUCT THESE TRAINING PROGRAMS?

Our attorneys conducting the training sessions are not only educated on the applicable state and federal laws and regulations, but also have actual experience counseling clients and litigating cases based on these laws. This real-life experience allows us to provide training that is relevant and practical.

WHAT IS INVOLVED IN A TRAINING PROGRAM?

Gibbons training programs include live, attorney-led classes in which interactive discussion and questions are encouraged. All programs are tailored to your organization's specific policies, practices, and needs and use real case examples, as well as hypotheticals. We also discuss and distribute pertinent and sample company policies and require acknowledgments of attendance.

WHAT TOPICS DO YOU TRAIN ON?

Gibbons attorneys train on all data privacy and cybersecurity topics, in any combination your organization finds most helpful. We can craft programs specific to your organization's policies and requirements and also offer several programs of general application in the following areas:

- Basics of Cybersecurity Compliance and Breach Prevention
- Cybersecurity: Legal and Policy Requirements
- Information Security Foundations and Cyber-Risk Assessment, Analysis, and Mitigation
- Information Security Risk Management Policies and Tools
- Operational Compliance for Protected Health Information (PHI)

These programs are described in more detail on the following pages of this brochure.

HOW DO YOU CHARGE FOR THESE TRAINING PROGRAMS?

Training programs are offered on an hourly or flat fee basis. The fees take into consideration the number and variety of programs your organization requires.

* * * * * *

CONTACT US

For additional information on your training program needs, contact Dawn Afanador, Chief Marketing Officer, at (973) 596-4555 or dafanador@gibbonslaw.com.

This communication provides general information and is not intended to provide legal advice. Should you require legal advice, you should seek the assistance of counsel.

© 2016. Gibbons P.C. All rights reserved. ATTORNEY ADVERTISING. Prior results do not guarantee a similar outcome.

BASICS OF CYBERSECURITY COMPLIANCE AND BREACH PREVENTION

This training program is tailored to the specific needs of each company and various levels of employees, as detailed below.

Non-Supervisory employees participate in a training program of approximately 1 hour focusing on:

- Overview of legal liabilities for the company from cybersecurity risks
- Social engineering attack strategies that every employee should recognize
- Reporting procedures and responsibilities if you become aware of a cybersecurity risk

Mid-Management employees participate in a training program of approximately 1.5 hours focusing on the above topics, plus:

- Duties of supervising staff members
- Guidelines for creating a culture of cybersecurity compliance
- The role of cybersecurity in the organization

Upper-Management employees participate in a training program of approximately 2 hours focusing on the above topics, plus:

- Tools for measuring cybersecurity risks
- Organizational structuring for cybersecurity compliance
- Methods for dealing with law enforcement and the media when a cybersecurity incident occurs

The average total cost of a data breach to an organization is $4 million.

- 2016 Ponemon Institute Cost of Data Breach Study

CYBERSECURITY: LEGAL AND POLICY REQUIREMENTS

This half-day training program is appropriate for senior managers, C-suite executives, and board members who are charged with protecting their company from various risks – including the organization's cybersecurity risks. It covers specific legal requirements, as well as questions relating to public relations, corporate ethics, and social responsibility arising from data breaches and other cybersecurity issues, including:

- Regulatory responsibilities concerning information security (focusing on industry-specific issues as appropriate – *e.g.*, healthcare, government, financial services, energy)
- Reporting responsibilities in the event of a breach
- Working with the FBI, Secret Service, and other law enforcement entities
- Public-private incident information sharing
- Civil liability
- Establishing and preserving privileged communications
- E-discovery issues
- Cybersecurity insurance considerations

> The lack of awareness by executives on the state of their cybersecurity protocols and training initiatives is alarming, and puts them at a serious disadvantage against cyber attackers.
>
> *- 2016 BAE Systems Cybersecurity Survey Report*

INFORMATION SECURITY FOUNDATIONS AND CYBER-RISK ASSESSMENT, ANALYSIS, AND MITIGATION

This half-day training program is appropriate for anyone in the organization who handles sensitive company information, employee data, or customer data, as well as anyone involved in developing cybersecurity policies and procedures or managing cybersecurity risks. It covers foundational principles of information security and risk assessment, including:

- Types of information security threats
- Overview of legal liability for information security violations
- Cybersecurity compliance
- The Principle of Least Privilege
- The Authentication, Authorization, and Accountability (AAA), Policy, Procedure, and Training (PPT) and Confidentiality, Integrity, and Availability (CIA) Triads
- The Prevent/Detect/Respond (PDR) Principle
- Cybersecurity gap analysis
- Calculating a cybersecurity annual loss expectancy
- Cybersecurity quantitative risk assessment
- Introduction to the NIST cybersecurity framework
- Cyber-Risk mitigation through insurance coverage

Prevention is ideal.

Detection is a must.

Detection without response is useless.

- SANS Institute

INFORMATION SECURITY RISK MANAGEMENT POLICIES AND TOOLS

This half-day training program is appropriate for IT managers and other employees with line responsibilities over company IT assets. It covers basic security policies and technologies, with an emphasis on how those policies and technologies may relate to the organization's legal and compliance responsibilities, including:

- Data and information policies
- Application configuration
- Encryption
- Backups
- The Cloud: SaaS, PaaS, and IaaS
- Application and equipment hardening
- Spam, malware, and firewalls
- Data classification and Data Loss Prevention (DLP)
- Six phases of incident handling

42% of respondents expect their company's information security team would be able to detect and respond to only simple issues relating to a security breach.

- ISACA and RSA Conference; State of Cybersecurity: Implications for 2016

OPERATIONAL COMPLIANCE FOR PROTECTED HEALTH INFORMATION ("PHI")

Several training programs concerning the protection of the privacy and security of PHI are available. A half-day training program covering the HIPAA Privacy, Security and Breach Notification Rules is appropriate for anyone in the organization who is involved in developing and implementing the organization's HIPAA-compliance policies. It also will be useful for senior executives and board members concerned about the privacy and security risks to the PHI maintained by an organization. The program covers specific legal requirements and questions relating to public relations, corporate ethics, and social responsibility arising from data breaches and other cybersecurity issues involving PHI.

Shorter and more tailored programs addressing specific areas of HIPAA compliance are also available, including:

- Privacy rule compliance (90 minutes)
- Security rule compliance
  (including preparation for Phase II HIPAA Audits - 150 minutes)
- Data breach prevention/minimization and response to a data breach (90-120 minutes)
- General training for employees with restricted access to PHI (60 minutes)
- Customized programs (generally 60 minutes) focused on the organization's specific PHI compliance needs

90% of industries - including industries that are not in the healthcare sector - have experienced a PHI breach.

- Verizon 2015 Protected Health Information Data Breach Report