EPSTEIN
BECKER
GREEN

Privacy & Security Crash Course: How Do I Execute a Risk Mitigation Plan?

June 23, 2015

Upcoming Webinars

Privacy & Security Crash Course Series

- Privacy & Security Crash Course: Recap – Your Questions Get Answered
  June 30, 2015 at 2:00pm – 2:15pm EDT
  People: Patricia M. Wagner

To register, please visit: http://www.ebglaw.com/events/

This presentation has been provided for informational purposes only and is not intended and should not be construed to constitute legal advice. Please consult your attorneys in connection with any fact-specific situation under federal, state, and/or local laws that may impose additional obligations on you and your company.

Cisco WebEx can be used to record webinars/briefings. By participating in this webinar/briefing, you agree that your communications may be monitored or recorded at any time during the webinar/briefing.

Attorney Advertising

Presented by

Brandon C. Ge

Associate

bge@ebglaw.com

202-861-1841

EPSTEIN BECKER GREEN

Introduction

- After conducting a risk assessment, an organization must respond to identified risks and reduce risk to an acceptable level
  - Maintain the confidentiality of data
  - Assure the integrity and availability of data
- Four basic approaches to risk control
  - Accept
  - Avoid
  - Transfer or share
  - Mitigate
- Need entire organization on board

Risk Acceptance

- Acknowledging a risk and making a conscious decision to accept the consequences
  - Risk is within the organization's risk tolerance
  - Not cost-effective to address
- Before accepting a risk, an organization should conduct a documented analysis that includes:
  - Likelihood of risk
  - Potential loss from risk
  - Cost of controls
  - Decision to accept the risk
- Regularly review risk acceptance decisions

Risk Avoidance

- Taking action to try to eliminate the risk
  - Source of risk
  - Exposure to the risk
- May be appropriate when the risk exceeds the organization's risk tolerance
- Often expensive
  - Consider opportunity cost

Risk Transfer

- Shifting responsibility for a risk to another party
  - Normally through cyber insurance
  - Indemnification
  - Outsource
- May be an attractive option when it's difficult to reduce the risk to an acceptable level
- Generally doesn't reduce likelihood of risk
- Secondary effects
  - Negative publicity
  - Dependency/loss of control

Risk Mitigation

- Taking action to reduce the probability and/or potential loss associated with a risk
- Involves implementing controls
  - Preventive vs. detective
- Cost-benefit analysis
  - Cost of control vs. projected benefits
  - If benefits > cost of control: consider implementing control
  - If cost of control > benefits: explore other controls or accept/avoid/transfer the risk

Considerations

- Develop an overall risk response strategy
  - Establish organizational risk tolerance
  - Outline goals and objectives
  - Provides the basis for determining whether to accept, avoid, transfer, or mitigate risk
- Prioritize
- Consider interim measures
- Detailed documentation
  - Mitigation strategies
  - Analyses and decisions

Risk Monitoring

- Risk management is an ongoing process
- Continue to monitor risk responses with respect to:
  - Compliance
    - Organizational mandates
    - Federal/state mandates
  - Effectiveness
    - Have the measures been effective in reducing risk to an acceptable level?
  - Changes
    - Systems
    - Environments

Questions?

Brandon C. Ge

Associate

bge@ebglaw.com

202-861-1841

EPSTEIN BECKER GREEN

Upcoming Webinars

Privacy & Security Crash Course Series

- Privacy & Security Crash Course: Recap – Your Questions Get Answered
  June 30, 2015 at 2:00pm – 2:15pm EDT
  People: Patricia M. Wagner

To register, please visit: http://www.ebglaw.com/events/