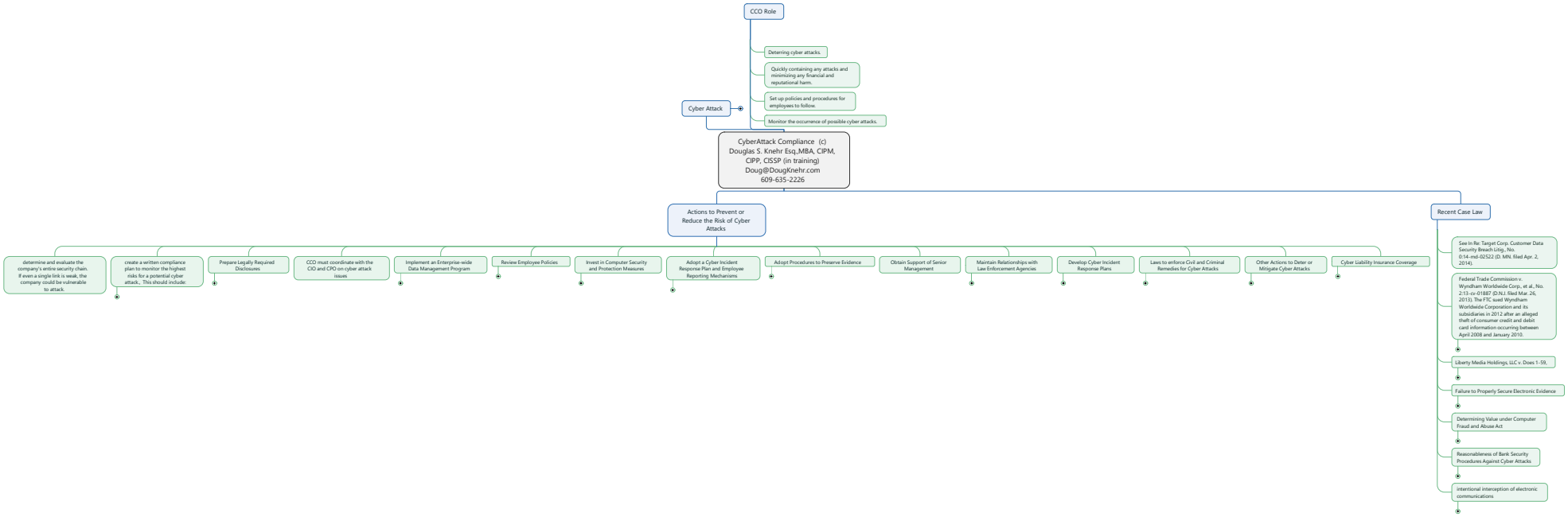
CCO Role
Deterring cyber attacks.
Quickly containing any attacks and minimizing any financial and reputational harm.
Set up policies and procedures for employees to follow.
Monitor the occurrence of possible cyber attacks.
Cyber Attack
CyberAttack Compliance (c)
Douglas S. Knehr Esq.,MBA, CIPM, CIPP, CISSP (in training)
Doug@DougKnehr.com
609-635-2226
Actions to Prevent or Reduce the Risk of Cyber Attacks
determine and evaluate the company's entire security chain. If even a single link is weak, the company could be vulnerable to attack.
create a written compliance plan to monitor the highest risks for a potential cyber attack.. This should include:
Prepare Legally Required Disclosures
CCO must coordinate with the CIO and CPO on cyber attack issues
Implement an Enterprise-wide Data Management Program
Review Employee Policies
Invest in Computer Security and Protection Measures
Adopt a Cyber Incident Response Plan and Employee Reporting Mechanisms
Adopt Procedures to Preserve Evidence
Obtain Support of Senior Management
Maintain Relationships with Law Enforcement Agencies
Develop Cyber Incident Response Plans
Laws to enforce Civil and Criminal Remedies for Cyber Attacks
Other Actions to Deter or Mitigate Cyber Attacks
Cyber Liability Insurance Coverage
Recent Case Law
See In Re: Target Corp. Customer Data Security Breach Litig., No. 0:14-md-02522 (D. MN. filed Apr. 2, 2014).
Federal Trade Commission v. Wyndham Worldwide Corp., et al., No. 2:13-cv-01887 (D.N.J. filed Mar. 26, 2013). The FTC sued Wyndham Worldwide Corporation and its subsidiaries in 2012 after an alleged theft of consumer credit and debit card information occurring between April 2008 and January 2010.
Liberty Media Holdings, LLC v. Does 1-59,
Failure to Properly Secure Electronic Evidence
Determining Value under Computer Fraud and Abuse Act
Reasonableness of Bank Security Procedures Against Cyber Attacks
intentional interception of electronic communications