GOODWIN | PROCTER

Cybersecurity: It's Not Just for CIOs Anymore

Gus Coldebella, Goodwin Procter LLP
Mark Seifert, The Brunswick Group
Emily Stapf, PricewaterhouseCoopers

Goodwin Procter Directors' Forum

May 21, 2013

Cybersecurity

...It's Not Just for CIOs Anymore

Four Cybersecurity Topics Directors Should Focus On Now

1. The Cyber Threat:
   Who is Attacking? What Are They Looking For?

2. The Legal and Regulatory Environment:
   Regulation is Coming, One Way or Another

3. Preparing for the Inevitable:
   Board Organization, Company Oversight, A Record of Diligence

4. Responding to an Attack:
   Surviving a "Bet the Company" Situation

GOODWIN | PROCTER

The Cyber Threat: *Who is Attacking? What Are They Looking For?*

The Cyber Threat

- The Attackers
  - *Nation-States*
  - *Organized Crime*
  - *"Hacktivists"*

- What They're Looking For
  - *Intelligence*
  - *Access to or control over critical infrastructure*
  - *Intellectual property or other business-sensitive information*
  - *"To make a point" / Vandalize*

GOODWIN | PROCTER

The Legal and Regulatory Environment: *Regulation is Coming, One Way or Another*

The Legal and Regulatory Environment

- Substantive regimes
  - E.O. 13636, "Improving Critical Infrastructure Security," calls for "Voluntary Cybersecurity Standards" for "Critical Infrastructure"
  - "Trickle-down regulation" and market forces
  - Standard of care
- Disclosure-based regimes
  - CF Disclosure Guidance: Topic No. 2 (Oct. 2011)
  - State breach notification laws

CF Disclosure Guidance: Topic No. 2 (Oct. 2011)

- Where? Two main places: Risk factors and MD&A.
- Risk factors: If "among the most significant factors that make investment in a registrant speculative or risky"
- MD&A: If costs and other consequences of known or potential cyber events represents a material event, trend or uncertainty.
- SEC expects registrants to:
  - Evaluate cyber risks
  - Take into account all relevant information, including
    - Prior cyber incidents, their severity and frequency
    - Probability of cyber risks occurring
    - Qualitative and quantitative magnitude of risks, including potential costs and other consequences
- No generic disclosure
- May need to disclose known or threatened attacks to put risks in content

GOODWIN | PROCTER

Preparing for the Inevitable: *Board Organization, Company Oversight, A Record of Diligence*

Board Organization and Company Oversight

- Set "tone at the top"
- Understand and assess the threat and risks
- Ensure board-level attention
- Pre-crisis planning (and exercising)
- …All of this enhances security, and creates an *continuing record of diligence*

GOODWIN | PROCTER

Responding to an Attack: *Surviving a "Bet the Company" Situation*

Responding to an Attack

- Breach should be treated as an *investigation*
- Engage Outside Experts
  - Law Firm
  - Forensic Cyber Investigator
  - Crisis PR Firm
- Ask and Answer The Important Questions FAST
- Disclosure
  - Do we have to? Do we want to?
- Assess Law Enforcement Involvement

GOODWIN | PROCTER

Questions?

Cybersecurity

...It's Not Just for CIOs Anymore

Gus Coldebella
Partner, Goodwin Procter LLP
gcoldebella@goodwinprocter.com
(202) 346-4034

Mark Seifert
Partner, The Brunswick Group
mseifert@brunswickgroup.com
(202) 393-7337

Emily Stapf
Director, PwC Forensic Technology
emily.stapf@us.pwc.com
(703) 868 0269