Move the Needle
Active Agent Approach to Cybersecurity and Data Protection Compliance

Oleg Vasilyev, Director-Compliance, AT&T
Brian Novack, Lead Compliance Analyst, AT&T

September 15, 2019
"Just do the right thing"

Where we start...

§ 8B2.1. Effective Compliance and Ethics Program
a) To have an effective compliance and ethics program . . ., an organization shall—
   1) exercise due diligence to prevent and detect criminal conduct; and
   2) otherwise promote an organizational culture that encourages ethical conduct and a commitment to compliance with the law.
Legal Obligations, Industry & Internal Standards/Requirements

- General Data Protection Regulation (GDPR)
- FCC rules pertaining to Customer Proprietary Network Information (CPNI)
- Health Insurance Portability and Accountability Act (HIPAA)
- NY Department of Financial Services Cybersecurity Regulations
- Fair Credit & Reporting Act (FCRA) / FTC Red Flags Rule
- Payment Card Industry (PCI) Standards
- California Consumer Privacy Act (CCPA)
- Internal Policies & Operating Practices (e.g., Security, Privacy)

Skilling Up Our Team
Know Your Data & How it is Utilized

Privacy Principles
- Transparency
- Choice & Control
- Security
- Integrity

Risk Identification and Prioritization

- Identify your business specific risks
- Prioritize your business specific risks
- Look ahead to emerging risks
- Framework to identify and address risks
Framework: Core Functions

Identify

NIST Cybersecurity Framework

Protect

Detect

Respond

Identify

Protect

Detect

Respond

Actively Analyze & Monitor Risks

Metrics & Data Feeds

Key Risk Indicators

• # of Fraudulent Events
• % of Timely Revocation
• # of Critical Vulnerabilities

Tools

• Dashboards / Charts / Graphs
• Knowledge Worker & Executive Views
• Alerts / Automation

Regularly Revisit and Reevaluate Risks
Plan Now

Plan and Prepare for the Worst
• Incident Response Plan
• Media, stakeholder (e.g., executive) communications
• Post-event root cause analysis and remediation
• Consider pre-designated SWAT team
• Conduct tabletop exercises
• Develop training
• Federal Reporting Requirements

We can’t do it alone...

Partner with key Business Units
• Use of and role of compliance coordinators (are they a help or a roadblock?)
• Must have a buy-in from the top
• Responsible cyber security behavior applies to all employees at all levels
• Buy-in is a start but cross-functional collaboration is key
  • Audit, Legal, HR, IT, CSO, Privacy
  • Earn trust and be transparent
• Maintain independence
Become an Active Agent in your Data Protection Compliance Program

- Compliance is relevant to data protection and cyber risk
- Skill up your team or fill skill gaps
- Know your data & how it is utilized
- Perform regular risk assessments, monitor, and reassess
- Collaborate cross-functionally
- Educate employees on good cyber practices
- Operate with Integrity and Transparency