Getting Started

- Map data in your systems – what’s where
- Classify data assets you need to protect by level of sensitivity
  (e.g. trade secrets, credentials, information subject to contractual obligations, information that would trigger data breach notice obligation)
- Track confidentiality obligations and label all information that must be protected
- Establish cross-organizational data governance team
- Processes must be tailored to work within organization’s operational and technical structures
Cyber Risk – Board level issue

- Board level impact
- Big incidents pose Legal and Reputational Risk to Directors & C-suite
- Big difference between media focused and real legal risks
- BUT Congress, State AGs, regulators and the market respond to media risks –> reputational risk must be taken seriously
- It is important to have strong policies and practices managed below Board level with easy to understand reporting to Board
Board Governance Approach

- Board Role: Oversee the company’s cyber security program, not manage it directly
  1) Review reports from senior management regarding cyber security risks, cyber attacks, and cyber risk management plans
  2) Monitor whether the company is adequately managing cyber risk, including whether sufficient resources are devoted to cyber security
  3) Records should document oversight steps, briefings
Board IT Expertise

Emerging Board Recruiting Need: expertise to oversee company cyber security programs

3 Options in use at Public Companies:

- Board member with technical expertise who receives briefings or
- Briefings from third party experts, government agencies, etc., or
- Using independent advisors (external auditors, outside counsel) who have a multi-client, industry wide perspective
Enterprise-wide Governance

- Enterprise-wide risk, not just an IT risk
- Appoint a cyber risk management team with all substantial stakeholder departments represented (including Legal, Finance, HR, IT, and Risk Management)
  - Led by a senior manager with cross-departmental authority
  - Team reports to the full Board or Committee of the Board
- Develop incident response and preparation protocols
  - Breach response protocol, tabletop exercises, review contractual obligations with vendors/customers
- Clearly establish cross-departmental ownership and roles and responsibilities
Keeping Up with Changing Threat Landscape

- Highly dynamic risk, so team should:
  - Meet regularly and develop reports to the Board
  - Track and report metrics that quantify the impact of cyber threat risk management efforts
  - Include evaluation of cyber threat risk environment and management as part of regular reviews, *e.g.*:
    - Current state of threats & defenses at peer entities
    - Qualified reviewers of logs for suspicious activity
    - Conducting penetration testing
    - Examining and updating white lists & black lists for threat actors
    - Maintaining incident response preparedness
    - Legal requirements review
Overseeing Risk Management Strategy

- Oversee development and adoption of risk management plan
- Assess the cyber risks facing the company
  - What “crown jewels” need to be protected at all cost
    - E.g., IP, business strategy, breach notice data, credentials
    - Need to have multiple layers of security behind the firewall
    - Oversee continuous evaluation of sufficiency
- Which cyber risks to avoid, accept, mitigate or transfer through insurance
  - Evaluate plans associated with each decision and if resources are sufficient to achieve desired protection
- Ensure budget is sufficient and appropriately allocated
Risk Assessments, Analysis and Management Strategies

- Determining your current state of security
  - Internal assessments and audits (incl. network architecture)
  - Vulnerability and penetration testing (internal and external)
  - Bounty programs
  - Third party partners/vendors

- Remediation and mitigation
  - Closure of vulnerabilities, patch placement, and validation
  - OS/software/hardware upgrades
  - Improved segmentation, encryption and other strategies
  - Training and the human element
  - Remote systems and employees, and mobile devices
  - Improve intrusion prevention system/intrusion detection system (IPS/IDS) monitoring efficacy
Weigh Litigation and Regulatory Risk

- Class Action Litigation
  - Consumer (Previously losers, but Adobe and Remijas cases accepting standing make this more of a threat)
  - Special classes (card issuing banks, business partners)
- Card issuer litigation
- Shareholder derivative litigation against Board
- State AG and FTC investigations, enforcement proceedings
- Breach of contract actions from/with partners
- Payment card brand fines and disputes (MasterCard pressing)
- Insurance coverage disputes
- Attacks on critical infrastructure could present worse claims
Oversee Incident Response
Preparation and Practice

- Preparing a breach incident response plan
  - Team identification and mobilization (24 x 7 availability)
  - Role of counsel and the privilege in an investigation
  - Forensic and PR teams
  - Preventing data loss and immediate security changes
  - Securing evidence and logs, and documentation
  - Law enforcement involvement
  - Defining legal obligations vis-à-vis individuals, AGs, card brands

- Practice
  - Tabletop exercises with PR, counsel, forensics, C-suite
  - Training
  - Periodic updating (e.g., of team and contact info)
  - Require the same of key vendors/others interconnecting with your network
Expenses and Insurance

- Breach notice costs can be huge (Target, TJX)
- Ponemon Institute 2014 survey average - $200 per record affected
  - But significantly less if have an incident response program in place
  - Costs can include: forensic investigation, legal, PR, notice handling, call centers, class action litigation, payment card and regulator investigations and fines, SEC disclosures, business interruption, stock price fluctuations, loss of good will

- Cyber Insurance Market is Maturing
  - Can obtain coverage for most of the above costs
  - But not goodwill/reputational, or catastrophic losses
  - Review exclusions and limits carefully as well as any conditions
While cybersecurity risk management activities may vary, effective programs have some common elements:

1. Senior Management Commitment
2. Code of Conduct and Compliance Policies and Procedures
3. Oversight, Autonomy, and Resources
4. Risk Assessment
5. Training and Continuing Advice
6. Disciplinary Measures and Incentives
7. Third-party Due Diligence and Payments
8. Confidential Reporting and Internal Investigation
9. Continuous Improvement: Periodic Testing and Review
Assess a cybersecurity program - Maturity Model

- Programmatic: from IT process to sustainable enterprise program
  - Documented – program, authoritative framework, maturity level, outcomes
  - “Operationalized” – map risk to controls
  - Sustainable - organization, change management, feedback

- Contextual: from tactical process focused to enterprise risk based
  - Market & Industry – benchmarking
  - Regulatory – identification
  - Third party – inventory, evaluate, risk rank, require, enforce

- Risk based: from checklist to dynamic and flexible response
  - Asset and environment
  - Criteria established
  - Consistently applied

- Metrics, Measurement and Reporting - Effectiveness
  - Design vs Effectiveness
  - Actionable
  - Outcomes vs availability
WHAT TO TELL YOUR CONSTITUENTS

- Change passwords frequently
  - Even if not using an affected site, good idea to change any password that is likely to have been affected in a breach

- Use different passwords
  - Many services help users track create and remember unique passwords (AOL one point, 1Password, LastPass)

- Use 2-Factor authentication where possible