SQUIRE PATTON BOGGS

ACC Association of Corporate Counsel
NATIONAL CAPITAL REGION

Global Issues Forum:

Finding the Balance When Putting Your Data to Work – Best Practices for Information Governance

November 13, 2018

Presenters

SQUIRE PATTON BOGGS

- **Robin Campbell**
  Co-Head, Data Privacy & Cybersecurity Practice
  Squire Patton Boggs
  robin.campbell@squirepb.com

- **Steve Cooper**
  Former Chief Information Officer (Retired) – Commerce, FAA, American National Red Cross, DHS
  Strategic Information Concepts

- **Brian Corbin**
  Executive Director, Assistant General Counsel
  JPMorgan Chase & Co

- **Matt Yarbrough**
  Partner
  Squire Patton Boggs
  matthew.yarbrough@squirepb.com

- **David Cox**
  Assistant General Counsel, Privacy, Data Governance & E-Discovery
  Volkswagen Group of America

Information Governance Discussion

SQUIRE PATTON BOGGS

Steps we will cover:

- Developing comprehensive strategies for information governance
- Determining the appropriate stakeholders
- Assessing the value of data to each area of business
- Bringing together cross-disciplinary teams
- Assuring the relevance of the data that you collect and maintain
- Managing the eDiscovery process

Developing Comprehensive Strategies for Information Governance

Get Management Buy-In

SQUIRE PATTON BOGGS

Corporate Information Governance Program (CIGP)

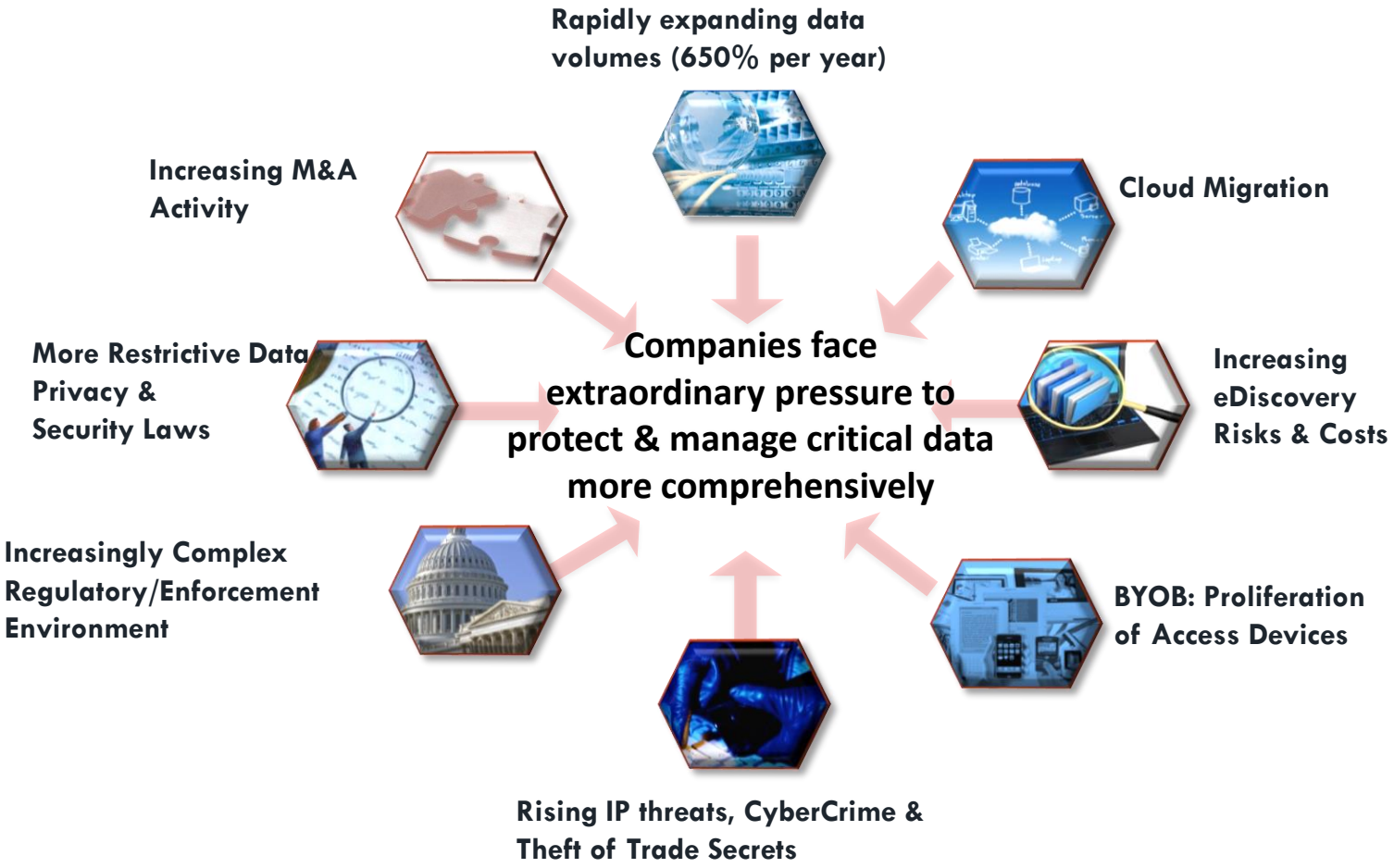
CIGP Framework

Understand & Assess	Identify Stakeholders & Project Sponsors	Understand Business Objectives	Understand User Needs	Inventory Information & Systems	Identify IG Committee Participants
Plan & Document	Conduct Business Need Analysis	Document Needs & Budget	Initiate Requests for Information	Document CIGP Implementation Plan	Communicate CIGP to Business
Implement	Form IG Committee & CIGP Kick-Off	Create Policies Mapped to Business Needs	Implement Technology	Provide CIGP Traning & Communications	Roll Out Changes to Existing Policies
Manage	Audit Policy Compliance	Update Regulatory Requirements	Update Technology Requirements	Communicate Updates to Business	Conduct Annual Review of CIGP

What are the Information Risks?

SQUIRE PATTON BOGGS

Companies are dealing with Information Risk on a massive scale



Our Experience: Data Impacts Everything

SQUIRE PATTON BOGGS

Proactive - Information Governance

IP Protection

Data Privacy & Security

eDiscovery & Legal Response

Records Mgmt & Compliance

Data Remediation/ Destruction

Reactive – Investigation & Litigation Response

Know What You Have and Where it Resides

SQUIRE PATTON BOGGS

Where is Electronically Stored Information (ESI)?

- PC Hard Drives
- Servers (Fileshares)
- Cloud
- Company Issued Phones, Tablets, etc.
- External Drives – USB, External Hard Drives, etc.
- Backup Tapes

What Information Do I Need to Protect?

SQUIRE PATTON BOGGS

Understand the regulatory requirements:

- Personal information/personal data (PI, PII, EU Personal Data)
- Protected health information (PHI)
- Payment card industry (PCI) Data
- HIPAA-protected data
- Intellectual Property (IP)
- DoD data
- FISMA-protected data
- Records data
- Personnel files
- Corporate financial data
- Tax forms
- FMLA-related forms
- IT security data

Most Common Formats of Electronically Stored Information

SQUIRE PATTON BOGGS

- Email
- Unstructured Data – Word, Excel, PowerPoint Files, etc.
- Database
- Text Message
- Voice Mail

Determining the Appropriate Stakeholders

Stakeholders

SQUIRE PATTON BOGGS

Internal

Business Users

- **HR** – Compensation/Equity, Benefits, Recruitment
- **Marketing** – Customer Contacts/PII/3rd Parties
- **Customer Relations/Experience** – CRM/Loyalty Programs

Legal, Risk and Regulatory – including procurement

Information Technology – New Technologies, Data Security, Physical Security, Surveillance, Cloud, Mobile Devices, Social Media, IoT

External

- **Finance/Investor Relations**
- **Partners** – JVs, Licensing & Other Partners

Make Information Governance Part of Your Company Culture

SQUIRE PATTON BOGGS

- Communicate
- Socialize the initiative
- Train everyone

Assessing the Value of Data to Each Area of Business

IG is Not Just About Litigation Response

SQUIRE PATTON BOGGS

- Data is a valuable company asset
- Good IG enables a company to have the right data assets at its finger tips
- Old, irrelevant data costs money and creates risk
- It is important to understand your regulatory obligations, but also the data needs of each of your business teams

Bringing Together a Cross-Disciplinary Team

IT Does Not Touch Everything

SQUIRE PATTON BOGGS

- IT is a critical stakeholder in an information governance exercise
- However, many businesses handle data assets outside of the normal business resources (shadow IT and other media)
- Teams across all disciplines must work together to map existing data and develop an ongoing means to track and manage data within the company
- Important to reach a cross-disciplinary consensus on terms and objectives

Assuring the Relevance of the Data that You Collect and Maintain

New World of Privacy/Security

SQUIRE PATTON BOGGS

- Days of “let’s collect and keep everything and figure out whether we need it later” are over
- Laws around the globe are
  - limiting the ability to collect data without a legitimate purpose in the first instance
  - requiring detailed notice to consumers/employees about the data collected and how it is used
  - mandating disclosure about sharing data with third parties, whether for internal business purposes or for the sale of data
- Data minimization, purpose limitation and limited retention are all concepts that must be included with your IG plan
- Marketing restrictions around the globe make it essential to maintain “clean” marketing lists, which means you must be able to identify the source and the notice/choice provided at collection (proving to be a difficult task post-GDPR)

Monetization

SQUIRE PATTON BOGGS

- With new data monetization limitations cropping up around the globe, it is important to be able to demonstrate valid collection and proper authorization to monetize data
- Companies must be able to segregate data so that they can use/monetize appropriate data and exclude other data from these efforts
- Technology and business needs must be aligned

Managing the eDiscovery Process

What is eDiscovery?

SQUIRE PATTON BOGGS

- Discovery is the exchange of documents & electronically stored information (ESI) in the context of litigation or governmental investigation
- The Federal Rules of Civil Procedure (FRCP) were amended in 2006, 2010, and 2015 to address issues specific to ESI

Electronic Discovery Reference Model (EDRM)

SQUIRE PATTON BOGGS

Objective

- To implement **legally defensible** data preservation
- Standardize policies and process to **ensure legal defensibility**
- Reduce risk of inadvertent data deletion
- Create efficiencies in issuing and tracking holds:
  - More efficient case management (interaction with Case Track) and creation of centralized repository
  - More efficient tracking of multiple relevant sources of evidence and ESI
  - Create notification, termination and audit procedures
- Lower costs and business impact of complying with law
  - Reduce “over-preservation” of data & cost of review by outside counsel
  - Ability to implement regular purges of data

Electronic Discovery Reference Model (EDRM)

SQUIRE PATTON BOGGS

Ultimate Objective

- From a risk mitigation perspective, **defensibility** is the ultimate objective of any eDiscovery process
- Discovery Objectives
  - Comprehensiveness
  - Efficacy
  - Auditability
  - Consistency
  - Transparency

General Practice Tips

SQUIRE PATTON BOGGS

- The “worst phrase” ever spoken in the world of data management & eDiscovery: **“Just to be safe, let’s keep it forever”**
- Strategic insourcing and outsourcing (e-discovery processing, managed review)
- Understanding regulatory risk beyond active litigation (Data Privacy, Information Governance, HIPAA)
- Tips to encourage your clients to engage you early and often**: (how to be an enabler vs. a roadblock)**

General Practice Tips

SQUIRE PATTON BOGGS

- **The importance of expectation setting**
  - Kickoff calls
  - Introducing all matter participants (internal and external)
  - Setting milestones
  - Written recaps of phone conversations to ensure accountability
  - Standing status update calls to ensure milestones are being met and strategy is still appropriate
- **Understanding e-discovery and its role in the legal process**
  - What are internal capabilities
  - Developing a workflow
  - Early involvement in the process to align in-house counsel and outside counsel, internal discovery resources and vendor resources
- **Measuring results against expectations, post-mortem to remediate any gaps/deltas**

General Practice Tips

SQUIRE PATTON BOGGS

- **Outside Counsel: Beware Not to Re-create the Wheel**
  - They don't know our internal workflows
  - They don't know what IT is/isn't doing in terms of preservation: "we image everything"
  - They don't know who may separate from the company and whose devices may be wiped/repurposed and their data lost
  - They may not have a standard process for key witness interviews
  - They may not be familiar with eDiscovery or proper forensics, discovery, collection, and targeted searches
  - They may not have a clearly defined strategy for a particular matter:
    - e.g., Are fraud claims in play? If so, may want to image key exec devices
  - They may be operating in an inefficient manner causing expenses to grow:
    - Too many bodies, youthful lack of experience, and the wrong tools (tech can solve this)

Federal Rule 26(b)(1)

SQUIRE PATTON BOGGS

Factors to Consider

- Importance of what is at stake
- Amount in controversy
- Parties' access to relevant information
- Parties' resources
- Importance of discovery in resolving the matter
- Burden versus benefit

eDiscovery Overview

SQUIRE PATTON BOGGS

- **Trigger**: A party in litigation has a duty to preserve all evidence that it **reasonably knew or could reasonably foresee was material** to a potential legal action
- **Sanctions**: Failure to preserve and produce relevant information in discovery can result in sanctions, fines and adverse court orders.
- **Proportionality**: Costs and level of effort for eDiscovery required should be in proportion to the amount in dispute and nature of matter
- **Safe Harbor**: Companies are protected from inadvertent deletion of data if adequate processes and measures are in place to minimize
- **Defensibility**: Establishing effective, consistent, transparent policies, and processes are key to deflecting challenges to eDiscovery efforts

When Does Legal Hold Duty Arise?

SQUIRE PATTON BOGGS

- Duty arises when legal proceeding is "**reasonably foreseeable**." *In re Napster, Inc. Copyright Litig.*, 462 F. Supp. 2d 1060, 1068 (N.D. Cal. 2006)
  - $29 million reasons to be concerned: *Zubulake v. UBS Warburg LLC*, 220 F.R.D. 212, 216 (S.D.N.Y. 2003)
  - May come well before action is commenced: *e.g*. "when a party **should have known** that the evidence may be relevant to future litigation"
- **Sedona Guideline 1:**
  - Reasonable anticipation of litigation arises when an organization "is on notice of a credible probability that it will become involved in litigation, seriously contemplates initiating litigation, or when it takes specific actions to commence litigation." S*edona Conference Commentary on Legal Holds: The Trigger & The Process*, 11 Sedona Conf. J. 265, 271 (2010)

Legal Hold Tips

SQUIRE PATTON BOGGS

- Be proactive and prepared
- Consult counsel
- Interview key witnesses
- Ensure it's a team effort
- Communicate across departments
- Consider all potentially relevant systems
- Know your custodians' systems

Know When to Stop

- Over-preserving can be costly, but on the other hand, releasing a legal hold too soon can lead to sanctions
- Evaluate the status of the matter
- Verify that preservation obligations have ended
- Confirm that they are not likely to re-emerge
- Have defensible procedures in place for releasing ESI from a legal hold

QUESTIONS?