MAY ISOAG MEETING
AGENDA

• GREG WILLIAMS, EY
• BEN TIMMS, HP
• ERIC ROBINSON, KLDISCOVER
• UPCOMING EVENTS
• ADJOURN
Sam Jamison is a senior manager in the Consulting practice of Ernst & Young LLP and co-leads the EY Federal Supply Chain Risk Management (SCRM)/Third Party Risk Management (TPRM) solution. Sam has more than 15 years of IT program management experience in IT risk management, enterprise risk management, program risk management, project management and delivery on system integration projects. Sam manages federal third-party risk management programs, assessing in-place controls to mitigate risks from both suppliers and services.

Greg Williams is a senior manager in the Consulting practice of Ernst & Young LLP and leads Consulting Services for the Commonwealth of Virginia. Greg has more than 15 years of IT risk management experience including cybersecurity, change management, identity and access management, NIST 800-53 control framework, COV SEC 501 / 525 control frameworks, program risk management and risk analytics.
Our purpose

Our Government and Public Sector (GPS) practice

Building a better working world

From strategy to execution, we help our clients implement new and tested ideas to achieve results in key focus areas such as:

► Boosting the performance of our education system to attract employers that offer qualify job opportunities
► Improving the health and welfare of our citizens, our military and our veterans
► Protecting our nation and increasing public safety
► Positioning states, counties and cities for the infrastructure demands in the short and long run
► Investing in the future by confirming fiscally sound principles and budget management

We bring leading public sector and commercial insights to help drive innovation and address challenges for government and education clients

Public sector focus

► We have worked with over 36 states across the US, bringing broad and deep experience in facing the challenges of public sector clients.
► We deploy teams with a mix of public sector and commercial experience to drive innovative, practical approaches for our government clients.

Commercial insights

► We bring leading commercial practices through our support of some of the largest companies across 16 industry sectors.
► Our alliances with leading innovation and technology organizations mean we can help our clients drive their current and future technology investments and enable better business outcomes.

Global reach

► Our Government and Public Sector team currently has more than 17,000 GPS clients across federal, state and local governments. We focus on key business issues that are impacting government today.
► Our distinct ability to access our network allows us to quickly bring the right experience on the issues that matter to our clients.

About our business

We are a highly integrated, global organization. This means we can respond faster than our competitors, quickly and seamlessly accessing knowledge and talent from across the world.

About our people

► People who demonstrate integrity, respect and teaming
► People with energy, enthusiasm and the courage to lead
► People who build relationships based on doing the right thing

Our culture

We attract great talent by providing purposeful, challenging work for our people. In 2017, the EY global organization was recognized for our forward-thinking approach to business and culture and named one of the World’s 25 Best Workplaces by Great Place to Work®.
Solution framework

**Business transformation and innovation**
Helping architect, design and deliver end-to-end transformations, utilizing immersive approaches within a proven methodology.

**Finance**
Assisting clients transform the finance function and financial outcomes of the business, including reporting, profitability, cost management, credit risk, liquidity risk and actuarial.

**Risk**
Transforming the risk and controls functions and outcomes of the business, including enterprise risk, enterprise resilience, compliance, internal audit and controls.

**Operations and business services**
Assisting clients to reengineer core business processes and business services outcomes, including global business services (shared services).

**Technology transform and trusted intelligence**
Helping clients reimagine the IT function and IT-related outcomes in a business. This includes technology architectures, infrastructure, operations, modernization to cloud and enterprise resource planning, digital engineering, data and artificial intelligence strategies.

**Cybersecurity, privacy and trusted technology**
Mitigating and transforming the IT risk, cybersecurity and data privacy functions and outcomes in the business. This includes cyber risk, compliance and resilience, data protection and privacy, identity and access management, and technology risk, technology resilience and technology controls.

**Supply chain**
Reimagining and improving supply chain functions and outcomes across the enterprise, including forecasting and planning, supplies, order fulfillment and the procurement function.

**Customer growth**
Transforming customer-facing commercial functions and outcomes in the business, including sales, marketing, channels, pricing, digital products/services and experiences.

**Organization, culture, people and workforce experience**
Transforming the client organization, people and HR function to enable improved business strategy and outcomes. This includes organization and workforce transformation, change experience and learning, culture and leadership, HR transformation, systems, rewards and people mobility.

**Health and human services**
We serve state entities charged with administering Medicaid, eligibility, enrollment, child support, public health and other human service areas.

**Finance, operations and technology**
Primary focus includes enterprise planning, budgeting, financial reporting, compliance, audit controls, human resources, facilities management and IT services.

**Education**
We serve all levels of education with consulting services, including financial analysis, distance learning strategies, organizational redesign and systems design and implementation.

**Infrastructure and transportation**
We help government with infrastructure challenges with services that include strategy and policy, procurement processes, financial, program controls and management and organizational capacity.

**Public safety and justice**
We help address efficient government and enhanced public services to benefit citizens, including administration, management, operations, systems, programs and other issues facing the public sector.
Third party risk management (TPRM) overview
Third party risk management (TPRM) defined

Third party risk management provides a function for management to identify, evaluate, monitor and manage the risks associated with third parties and contracts.

A third party is any entity that provides products or services to the organization.
TPRM framework

TPRM provides a function for management to identify, evaluate, monitor and manage the risks associated with third parties (e.g., vendors/suppliers, intercompany relationships and fourth parties).
There are several types of risks that organizations using third parties need to consider. The level of exposure to these upside, downside and outside risks is based on how organizations are using third parties.

<table>
<thead>
<tr>
<th>Diverse set of risks associated with third parties</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Geopolitical risk</strong></td>
</tr>
<tr>
<td>Risk of doing business in a specific country and includes legal, regulatory, political and social economic considerations</td>
</tr>
<tr>
<td><strong>Regulatory and compliance risk</strong></td>
</tr>
<tr>
<td>Risk that a third party fails to comply with a required regulation, thus causing the organization to be out of compliance</td>
</tr>
<tr>
<td><strong>Operational risk</strong></td>
</tr>
<tr>
<td>Risk that a third party fails to meet the organizational needs from a service or product delivery perspective due to deficiencies in the third party’s operations</td>
</tr>
</tbody>
</table>
TPRM foundational components
Third party risk management components

To manage third party risks, it is critical to establish foundational components within TPRM

<table>
<thead>
<tr>
<th>TPRM foundational components</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Governance and oversight</td>
<td>Policies and standards</td>
</tr>
<tr>
<td>Program vision, goals and charter</td>
<td>TPRM policy</td>
</tr>
<tr>
<td>Governance and operating model</td>
<td>Procedures</td>
</tr>
<tr>
<td>Roles and responsibilities</td>
<td>Standards</td>
</tr>
<tr>
<td>Stakeholder engagement and communication</td>
<td>Master listing</td>
</tr>
<tr>
<td>Program integration and dependencies</td>
<td>Data management and governance model</td>
</tr>
<tr>
<td>Third party inventory</td>
<td>Risk models</td>
</tr>
<tr>
<td>Inherent risk</td>
<td>Inherent risk</td>
</tr>
<tr>
<td>Residual risk</td>
<td>Residual risk</td>
</tr>
<tr>
<td>Tiering/risk ranking criteria</td>
<td>Tiering/risk ranking criteria</td>
</tr>
<tr>
<td>Assessment methodology</td>
<td>Assessment framework</td>
</tr>
<tr>
<td>Assessment process and procedures</td>
<td>Assessment process and procedures</td>
</tr>
<tr>
<td>Assessment execution tools and enablers</td>
<td>Assessment execution tools and enablers</td>
</tr>
<tr>
<td>Risk response management process, procedures, and enablers</td>
<td>Risk response management process, procedures, and enablers</td>
</tr>
<tr>
<td>Technology, automation and reporting</td>
<td>Tools and technology</td>
</tr>
<tr>
<td>Key risk indicators and performance indicators</td>
<td>Key risk indicators and performance indicators</td>
</tr>
<tr>
<td>Third party dashboards</td>
<td>Third party dashboards</td>
</tr>
<tr>
<td>Third party reports</td>
<td>Third party reports</td>
</tr>
<tr>
<td>External sources of Third party information</td>
<td>External sources of Third party information</td>
</tr>
</tbody>
</table>

Stakeholder continuum

| GPO | Global Security | Enterprise Risk Management | Corporate Audit | DPO | Compliance | Lines of Business |
Governance and oversight overview

The following is an example of a TPRM governance model that considers the “three lines of defense model” in which the business is the first line, risk management functions are the second line, and Internal Audit is the third line. Roles and responsibilities need to be clearly defined across the organization.

**1st Line of Defense**
- Identifies known and emerging risk issues, as well as shifts in risk appetite
- Monitors implementation of effective risk management practices by first line
- Independently oversees aggregate risk exposure/analyzes risk themes/trends

**2nd Line of Defense**
- Identifies known and emerging risk issues, as well as shifts in risk appetite
- Monitors implementation of effective risk management practices by first line
- Independently oversees aggregate risk exposure/analyzes risk themes/trends

**3LoD (Internal Audit)**
- Independently assesses adherence to the TPRM framework
- Provides assurance that TPRM process is functioning as designed
- Identifies improvement opportunities across the TPRM framework to drive effectiveness

Continuous improvement and reporting drives compliance and optimization across the organization.
**Governance and oversight overview**

Leading TPRM programs/functions most often leverage more centralized governance models in order to better standardize third party risk activities, coordinate activities across key stakeholder groups (e.g., Risk functions) and facilitate decision-making across the organization.

<table>
<thead>
<tr>
<th>Decentralized</th>
<th>Federated</th>
<th>Centralized</th>
</tr>
</thead>
<tbody>
<tr>
<td>Independent</td>
<td>Locally Distributed</td>
<td>Balanced</td>
</tr>
<tr>
<td>Federated</td>
<td>Central + Distributed</td>
<td>Centralized</td>
</tr>
</tbody>
</table>

**Functional areas**
- **Independent**: Functional areas operate with complete autonomy, while maintaining global standards to meet specific enterprise requirements.
- **Locally Distributed**: Functional areas control a majority of their business and technology operations, with some limited coordination from the enterprise to ensure objectives are achieved.
- **Balanced**: Responsibility and ownership are shared equally among the different functional areas and the enterprise.
- **Central + Distributed**: The governance function provides a point of control and facilitates decision-making, but functional areas own selective decisions and activities.
- **Centralized**: The governance function provides a single point of control and owns decision-making with functional areas having little or no responsibility.

**Key considerations**
- Leading TPRM programs most often leverage a more centralized governance model in order to better standardize third party risk activities, coordinate activities across key stakeholder groups.
- A centralized structure decreases redundancies and can be managed holistically. In a decentralized structure, the onus is on the individual business units for managing the risk. This can lead to an inconsistent use of standards and duplication of resources and work.
- TPRM governance defines the vision of the organization’s TPRM program and provides direction for its execution.
- “Siloed” approaches to TPRM usually lead to governance gaps, overlapping monitoring programs/functions and increased execution costs.
- An under-resourced program will slow the assessment process, resulting in inadequate third party risk evaluation and treatment, delayed third party onboarding and contracting processes.
Assessment methodology process overview

TPRM methodology below depicts standard and scalable processes to evaluate and monitor third-party risk levels.

1 Intake and risk profiling
A common process is followed to trigger the TPRM process, including leveraging a standard intake request form and third-party inventory.

2 Inherent risk assessment
Determining the overall inherent risk score associated to third-parties’ products and services through a risk profiling questionnaire.

3 Control Assessment
A single, dynamic questionnaire is utilized covering all risk areas to streamline the process and drive efficiencies (third parties only answer the applicable questions).

4 Findings management
A residual risk score is assigned to facilitate reporting and risk treatment. Risk treatment is completed prior to contracting with a third-party.

5 Continuous monitoring
Issue tracking and reporting is performed until issues are closed. Ongoing due diligence is performed based upon a third-party’s assessed risk.

Automated End-to-end TPRM process (e.g., questionnaires, workflow, issue management, reporting, dashboards)
## Standard TPRM Process Triggers

<table>
<thead>
<tr>
<th>Triggers</th>
<th>Example</th>
<th>Future-State Considerations</th>
</tr>
</thead>
<tbody>
<tr>
<td>New Supplier</td>
<td>VITA engages a new supplier to provide goods or services.</td>
<td>Risk assessment process triggered as a part of the supplier registration/qualification process.</td>
</tr>
<tr>
<td>Existing Supplier, New Service</td>
<td>VITA purchases additional goods or services from an existing supplier.</td>
<td>Risk assessment is triggered prior to finalizing an agreement/contract with the supplier, which may be triggered at the point of contracting.</td>
</tr>
<tr>
<td>Change Order/Amendment</td>
<td>VITA agrees to a change order for an existing service provided by a supplier.</td>
<td>Risk assessment is triggered as a part of the contracting process, if needed, depending on the nature of the change order (if the scope changed a risk assessment may be warranted).</td>
</tr>
<tr>
<td>Proof-of-Concept</td>
<td>VITA does not have a contract with the supplier, but the supplier is providing a proof of concept to the Company potentially utilizing VITA branding and data.</td>
<td>Risk assessment may be triggered as part of supplier qualification or registration, or where a non-disclosure agreement (NDA) is required to interface with the supplier regarding the proof of concept.</td>
</tr>
<tr>
<td>Reassessment</td>
<td>A supplier requires a new assessment based on defined criteria (i.e., higher risk supplier that has not been assessed in 1 year).</td>
<td>Risk assessment triggered based on the last assessment date subject to the supplier being active and continuing to provide services to the organization.</td>
</tr>
<tr>
<td>Ad Hoc</td>
<td>Potential risks or concerns regarding an existing supplier are raised by an employee.</td>
<td>A Business Owner may request an assessment via a formal ticketing process.</td>
</tr>
</tbody>
</table>
Standard TPRM Process Triggers

**TRPM Intake form (sample)**

**Description:**
- Minimal gating questions to determine due diligence required

**Sample questions:**
- Overall: name of supplier
- Overall: Region/location of company
- Overall: category of services
- Overall: VITA business requestor
- Cyber/privacy: will the third party have access to VITA data?
- Cyber/privacy: will the third party have access to VITA systems/networks?
- Cyber/privacy: will the services or products offered by the third party be deemed *business critical*?

---

**Cyber/Privacy IRA (sample)**

**Sample questions:**
- Will the third party access, process, or store VITA data as part of the services provided?
- What type of data will the third party access, process, or store?
- How much data will the third party access, process, or store?
- How does the third party access VITA systems or networks?
- in the event of a third party service outage or disruption? Will the third party customize, configure, or develop software for VITA?
- Will subcontractors of the third party (or nth parties) have access to VITA data?
- What is the impact to VITA business processes

(Only prompted when cyber/privacy intake questions are answered ‘Yes’)

---

**Due diligence assessments (sample)**

- Privacy due diligence
- Cyber/InfoSec due diligence
- Business continuity due diligence
- Regulatory due diligence

---

*Virginia Information Technologies Agency – EY TPRM Insights Session*
Open source assessments

Leverage publicly available data to prioritize where to apply your resources:

Inherent Risk Process:
- Intake
- Service Impact Assessment
- Inherent Risk Score
- Open Source Assessment

Residual Risk Process:
- Due Diligence
- Residual Risk Score
- Risk Treatment
- Monitoring
Open source evaluation
Rapidly evaluate a vendor based upon open source validated information to enable risk based decisions earlier in the process.
Technology, automation and reporting

Organizations are leveraging GRC technology solutions, analytics and robotics to establish a scalable and efficient platform to automate risk and compliance activities end-to-end, including third party risk management.

**Costs**
- Increased inefficiencies and cost of ownership (e.g., infrastructure).
- Manual activities and intervention is required (e.g., data input).
- Multiple touch points with third parties and business.
- Incomplete view of risks and issues across the organization.

**Benefits**
- Increased efficiencies and reduce cost of ownership.
- Streamlined, integrated, and automated processes end-to-end.
- Comprehensive and real-time view of risks and issues.
- Reduce touch points with third parties and business.
## Technology, automation and reporting

<table>
<thead>
<tr>
<th>Technology</th>
<th>Description</th>
<th>Capabilities</th>
<th>Benefits</th>
<th>Current usage</th>
</tr>
</thead>
</table>
| Governance, risk and compliance (GRC) technology | A solution that provides a holistic view of risk and compliance across the enterprise by supporting multiple capabilities, including policy administration, controls management, compliance management, issue management, third party risk management, risk reporting and dashboarding. | ▪ Automates and standardizes risk activities (e.g., issue management, reporting, assessments).  
▪ Serves as a single "source of truth" for risk, control and compliance information across the organization.  
▪ Enables the aggregation and reporting of risk across multiple risk dimensions (e.g., third party risk, policy compliance). | ▪ Provides a holistic view of risk across the organization, including regulatory compliance.  
▪ Provides dynamic and real-time risk and control intelligence and reporting. | ▪ Policy maintenance.  
▪ Inventory of processes, risks, controls and compliance requirements.  
▪ Risk assessments.  
▪ Control testing.  
▪ Risk reporting.  
▪ Issue management. |
| Robotics process automation (RPA) | Automation of frequent, manual, and repetitive tasks by configured software in order to reduce costs, increase efficiencies and reduce human errors. | ▪ Automates routine activities (e.g., testing, evidence reviews).  
▪ Automates review of third parties responses to a questionnaire or submission of evidence. | ▪ Reduces costs, errors and process cycle time.  
▪ Increases economies of scale. | ▪ Data collection and aggregation.  
▪ Control testing. |
| Analytics and digital | Usage of analytics to extract and analyze data in order to identify patterns and trends. Usage of technology to digitize risk and control activities, including improving the customer experience. | ▪ Enables analysis of large volumes of data and emerging risks.  
▪ Facilitates decision-making and reporting.  
▪ Expands access to risk insights across the organization through online portals. | ▪ Identifies patterns and improves execution speed.  
▪ Allows employees to make better decisions. | ▪ Risk assessments.  
▪ Control testing.  
▪ Monitoring/surveillance.  
▪ Pattern analysis and dashboard reporting. |
| Artificial intelligence (AI) and machine learning | Machine learning that mimics human cognitive and problem solving capabilities. | ▪ Facilitates unsupervised learning on broad data access. | ▪ Processes large volumes of data.  
▪ Generates real-time reports.  
▪ Provides insights into emerging risks. | ▪ Risk pattern analysis and trending. |
EY TPRM Service Offerings
EY’s TPRM service offerings

**Current State Assessment**
- Current state/future state assessments and maturity analysis of existing programs
- Develop oversight and governance
- Define the target operating model
- Establish risk models and assessment frameworks
- Alignment with reg. and industry trends

**Assessment execution**
- Global execution of third-party assessments:
  - Global in-bound and out-bound onsite and remote assessments
  - Review, scoping and coordination
  - Issue management, analytics and reporting
  - Specialized assessments across InfoSec, business resiliency (BR), geopolitical, etc.

**Technology enablement**
- Enable existing tools to execute TPRM strategy
- Define business requirements
- Contract management/GRC tool selection assistance
- Educate organizations on full tool functionality

**Third-Party Risk as a Service (TPRaaS)**
- Develop and deliver managed service capability, leveraging EY’s platform
  - End-to-end technology enabled TPRM platform
  - Standardized EY process/questionnaires/model/reports
  - Provide third party oversight and governance throughout life cycle
  - Global execution of third-party risk assessments over a multi-year period
Case study: TPRM program design and implementation for a US Government agency

Business need

- Design, deploy and operate an TPRM program aligned to NIST 800-161 and leading commercial and governmental sector practices
- Establish a scalable TPRM service that can be utilized by internal government agency entities and external federal agencies
- Deploy a scalable technology to support TPRM designed processes Develop TPRM enablers to include policy, standards, training material, assessment questionnaires, dashboards, SLAs and metrics
- Support organizational change and communications management activities during rollout, adoption and execution of the TPRM program
- Execute assessments to meet compliance requirements, e.g., FedRAMP

Value delivered

- Established TPRM program through the use of Agile sprints to enable continuous delivery of processes and technology
- Established strong stakeholder integration to support ongoing process and technology show-backs to facilitate stakeholder ownership of the program and an ongoing feedback loop
- Established initial operating capability to provide rapid assessment capabilities through open source evaluation of cybersecurity, business continuity, privacy, foreign interest, compliance, geopolitical and financial risk; completed 300+ assessments to date (as of June 2020)
- Designed risk-based TPRM program whereas the greater the risk to the organization the greater the due diligence while aligning to NIST 800-161, EO 13873, Department of Commerce guidance and NERC-CIP. Program includes the following key features:
  - Rapid evaluation of inherent risk utilizing open source and impact analysis
  - Due diligence questionnaires to evaluate cybersecurity risks based upon NIST 800-53
  - Due diligence evaluation of supply chain risk (Provenance) through determination of product supply chain
  - Risk determination and remediation support to recommend, coordinate and validate findings required to be remediated
  - Monitoring of vendors on a periodic basis based upon risk
  - Customizable deployment model whereas customers have segmented environments with abilities to define risk weighting, tolerance, and customize questionnaires and metrics while leveraging vendor evaluations “raw data” across platform

Engagement summary

- Designed TPRM end-to-end process to include the following:
  - Intake
  - Impact assessment
  - Control-based assessments
  - Issue management and risk treatment
  - Monitoring
- Established TPRM program for VRM technology to enable designed TPRM end-to-end process
EY exists to build a better working world, helping to create long-term value for clients, people and society and build trust in the capital markets.

Enabled by data and technology, diverse EY teams in over 150 countries provide trust through assurance and help clients grow, transform and operate.

Working across assurance, consulting, law, strategy, tax and transactions, EY teams ask better questions to find new answers for the complex issues facing our world today.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation are available via ey.com/privacy. EY member firms do not practice law where prohibited by local laws. For more information about our organization, please visit ey.com.

Ernst & Young LLP is a client-serving member firm of Ernst & Young Global Limited operating in the US.

© 2021 Ernst & Young LLP. All Rights Reserved.

2101-3679576 ED None

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax, legal or other professional advice. Please refer to your advisors for specific advice.

ey.com
TODAY’S THREAT LANDSCAPE

600% INCREASE OF CYBERTHREAT INDICATORS RELATED TO CORONAVIRUS PANDEMIC*

JoHns Hopkins COVID-19 map

Deteque botnet threat map

WHAT HAS CHANGED FOR IT SECURITY?

Large number of Corporate Endpoints are outside the IT “Sphere of Control”
- Beyond corporate “perimeter”
- Harder to update OS/Firmware/Apps
- Data leakage to personal devices
- Not designed with security features

Remote work infrastructure not designed for scale
- VPN capacity load increase
- Endpoint [security] visibility
- User behavior (e.g., public Wi-Fi)

Productivity solutions not optimized for large scale work-from-home
- Remote management
- Remote recovery and restoration
- IT staffing
In 2020, Pandemic-related uncertainty, remote work conditions, and employee experience (EX) collided to create the ideal conditions for insider incidents.

One-third of security breaches will be caused by insider threats in the coming year. Security and risk professionals must adapt to this new reality.

Cyber-espionage and “chaos attacks” rising sharply.

Cyber criminals are pivoting towards long-term command and control presence on networks and moving “farther down the stack” to get low-level access to systems.
“Most organizations and missions are not tooled to be able to detect, let alone mitigate, this class of firmware threat. It is precisely, for this reason, that threat actors push further down the stack.”

Remotely brick a device at the firmware level
Bypass security controls such as BitLocker, ELAM, Windows 10 Virtual Secure Mode, Credential Guard, endpoint protection controls like A/V, EDR, etc.
Set up a follow-on attack
Reversing ACM or microcode updates that patched CPU vulnerabilities like Spectre, MDS, etc

https://eclypsium.com/2020/12/03/trickbot-now-offers-trickboot-persist-brick-profit//
THE INTERNET OF RANSOMWAR E THINGS
THE INTERNET OF VULNERABILITIES

IoT security warning: Cyber-attacks on medical devices put patients at risk

More collaboration required, says research.

- Security and Survival in a Hyper-connected World
  - CLICK HERE FOR DESTRUCTION
WAYS TO EXPLOIT YOUR IOT DEVS
Botnet target
Data exfiltration
Ingress point
7-POINT PROGRAM: FOR
IT DECISION MAKERS, SECURITY OPS, IT
ADMINS, AND END USERS

- Protect Your Endpoints
- Advocate and Enable Digital Hygiene
- Secure Sensitive Data
- Ensure Safe Network Access
- Take Special Care of Credentials
- Manage Conferencing Security and Privacy
- Productivity
SO WHAT CAN YOU DO???

DID WE SAY PATCH?

- IoT device
- Guest network
- Corporate Devices
- Home devices
- Patch, patch, patch . . .
- VPN
- Back it up
- Admin passwords everywhere
- Disable what you don’t need
- Multifactor Authentication
OH, AND…

USE A PASSWORD MANAGER

There are many out there...

Business ➔ Home use
CONFERENCE CALL SECURITY

- No URL on social media
- Unique meeting ID
- Password protection
- Verify attendees
- Lock the call
- Encrypt if possible
ADVISABLE TO USE ORIGINAL OEM CARTRIDGES

Engineered for security to protect your print device and your data.

Secure Supply Chains are mission-critical for ongoing cybersecurity.

1. Supply chain security
2. Cartridge chip security
3. Cartridge packaging security
4. Printer hardware security
MAKE YOUR HOME A CYBER-SAFE STRONGHOLD

Choose strong and different passwords for your email and social media accounts.

Secure electronic devices with passwords, PIN or biometric information.

Back up your data and run regular software updates.

Review the privacy settings of your social media accounts.

WIFI: always change the default router password.

Review your apps’ permissions and delete those you don’t see.

Install antivirus software on all devices connected to the internet.
ONLINE SHOPPING SAFETY TIPS

- Buy from reliable online vendors and check individual ratings
- Use credit cards when shopping online for stronger customer protection
- Think twice: if an offer sounds too good to be true, it probably is
- Check your bank account often for suspicious activity
REMEMBER:

Follow trusted sources for up-to-date factual information. If you become a victim of cybercrime, always report it to your national police.

Check the security and privacy settings of smart toys.

Talk to your child about cyber-safety.

Listen to their online experiences.

Explain to them the importance of being just as safe online as offline.

Change the default factory password and keep software up-to-date.

Use parental controls to safeguard your child's online activity.
STAY ALERT AND DON’T…

DON’T reply to suspicious messages or calls
DON’T share your bank card details or personal financial information
DON’T share news that doesn’t come from official sources
DON’T make donations to charities without double-checking their authenticity
DON’T open links and attachments in unsolicited emails and text messages
DON’T buy things online that seem to be sold out everywhere else
DON’T send money upfront to someone you don’t know
REMEMBER: YOU ARE A CRUCIAL PART OF THE SYSTEM

Source: www.jklossner.com
KLDiscovery…Solutions to Meet Your Needs
Assessing the Scope and Impact of a Data Breach

How advanced eDiscovery helps address the problems, risks and inefficiencies arising from a breach

Eric Robinson - Senior Consultant, Advisory Services and Client Solutions
Proposed Agenda

- Introduction
- Typical Workflow
- Technology and Reporting Highlights
- Case Studies
- Key action items to take with you
- Q&A Welcome
1 Introduction

When You Need Help
Addressing Data Privacy Challenges and Opportunities

Data privacy issues require more management and innovation. What are your clients’ priorities?

- Intra and inter-company data exchange
- GDPR Compliance
- Data Breach Response & Litigation
- Regulatory Expectations
- Inherent Value of Data ("Infonomics")

“You can’t protect everything equally…find a way to control only what matters”
- Earl Perkins, Research VP, Gartner
Why you need to analyze the impact of data breaches

Actionable insights, solutions and data-driven trends

- Well-meaning workers in organizations are putting more data at risk while some are just trying to get their job done.
- There’s more reportable employee and customer data at risk than many often think.
- Practical application of proven technologies and methods help measure, contain and uncover risk and opportunities for improvement.
- The scope of litigation resulting from data breaches is getting broader.
Every Major Industry is Impacted

Post-breach impact assessments and related discovery arises across a broad spectrum

- **Financial Services**
  - Banking
  - Accounting
  - Real Estate
  - Mortgage Services

- **Health Care**
  - Hospital systems
  - Managed Care
  - Health Insurance
  - Benefits Administration
  - Doctors

- **Insurance**

- **Legal Services**

- **Life Sciences**
  - Pharmaceutical
  - Medical Device

- **Higher Education**

- **Retail**
How Discovery Technology Aids Breach Response

- Primary objectives
  - Analyze breached data
  - Report on amount and type of PII, PHI or sensitive data that’s been compromised
  - Identify and report on impacted individuals
  - Be ready for any associated litigation or regulatory investigations

- Relevant Services
  - Data Collection
  - Processing
  - Hosting
  - Analytics
  - Managed Review
  - Consulting
  - Custom Reporting

- Key components for success
  - Proven lexicons of precise, customizable search terms
  - Pattern matching to identify and report on expected sequences like account numbers or social security numbers

- Complementary to other key components of the response team
  - Outside counsel
  - Cybersecurity threat assessment, attack analysis and system hardening
  - Insurance
  - Public Relations
Overview of Typical Workflow

Impact Assessment Methodologies
Overview of Data Breach Impact Assessment

Data Identification Preservation & Collection
- Compromised Data Sources (for impact analysis)
- Parallel consideration: Others Potentially Subject to Legal Hold (in anticipation of litigation)

Data Processing & Hosting
- Standardized templates to capture impacted individuals
- Optimized platform for all downstream search, analytics and reporting

Baseline Impact Assessment
- Initial analysis to estimate scope of documents containing potentially impacted individuals
- Establish initial estimates regarding number of impacted individuals

Detailed Impact Assessment
- Full Analysis of identified documents
- Full data capture
- Impacted individuals
- Flags for compromised data types
- Name level de-duplication
Overview of Data Breach Impact Assessment

Data Identification Preservation & Collection

- Collection Options
  - Remote Collection Kits
  - On site forensic data collection

Data Processing & Hosting

- Data Ingestion
- Processing Engine
- De-duplication & OCR
- Preliminary Data Filtering (where applicable)
- Hosted database setup

Baseline Impact Assessment

- Estimate Scope
  - Regular Expression Searches
  - Curated search terms (developed through our experience)
  - File Type Analysis (e.g. large volume of spreadsheets)
  - Statistical Sampling & Document Review

Detailed Impact Assessment

- Refine Scope & Workflow
  - Regular Expression Searches
  - File Type & File Name Grouping
  - Analytics: Concept Clustering, Concept Search, Predictive Coding
  - Standard & customized PII and PHI search terms (sampling)
  - Sampling excluded universe
3 Technology and Reporting Highlights

Noteworthy Elements to Innovating Data Breach Impact Assessments
Regular Expressions Help Uncover Critical Data

Pre-defined patterns can be used to find common patterns

- **Credit Card Numbers**
- **Social Security Numbers**
  - National Identification Numbers, National Insurance Numbers, Registration Numbers, Social Insurance Numbers, or any other international equivalents are added to specific databases as needed.
  - Drivers license numbers, passport numbers, medical identifiers, or other alpha-numeric patterns are easily identified and installed in specific databases as needed
- **IP Addresses**
- **Phone Numbers**
- **E-mail addresses**
- **Gender**
Sample Reports: Patterns Identified

Record level analysis and reporting

- Number of patterns identified per document facilitates easy estimates
- Automated quality control highlights outliers
- Automatic, real-time reporting with document and hit frequency per pattern aids high level risk assessment
- Record-level pattern extraction enables easy content level analysis
Sample Reports: PII and PHI Search Terms

Immediately following application of well curated search terms, the following types of tallies should be reviewed to assess scope.

<table>
<thead>
<tr>
<th>STR - All Docs</th>
<th>csv</th>
<th>doc</th>
<th>docm</th>
<th>docx</th>
<th>msg</th>
<th>pdf</th>
<th>txt</th>
<th>xls</th>
<th>xlsx</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filter</td>
<td>-</td>
<td>-</td>
<td>Filter</td>
<td>-</td>
<td>Filter</td>
<td>-</td>
<td>Filter</td>
<td>-</td>
<td>Filter</td>
</tr>
<tr>
<td>&quot;SSN&quot; OR &quot;S.S.N.&quot; OR (&quot;Social Security&quot; OR &quot;SS&quot; OR &quot;S.S&quot;) w/3 (&quot;no.&quot; OR number*)</td>
<td>0</td>
<td>50</td>
<td>9</td>
<td>13</td>
<td>37</td>
<td>835</td>
<td>2</td>
<td>4</td>
<td>0</td>
</tr>
<tr>
<td>(driver* w/3 (ic* OR &quot;no.&quot; OR number*)) OR(gov* w/3 (id OR &quot;no.&quot; OR number*))</td>
<td>4</td>
<td>46</td>
<td>5</td>
<td>20</td>
<td>94</td>
<td>608</td>
<td>0</td>
<td>1</td>
<td>5</td>
</tr>
<tr>
<td>policy w/2 period</td>
<td>0</td>
<td>43</td>
<td>6</td>
<td>1</td>
<td>2</td>
<td>682</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>policy w/2 number</td>
<td>0</td>
<td>13</td>
<td>6</td>
<td>4</td>
<td>2</td>
<td>701</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>&quot;policy period&quot;</td>
<td>0</td>
<td>42</td>
<td>6</td>
<td>1</td>
<td>2</td>
<td>680</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Social Security number</td>
<td>0</td>
<td>30</td>
<td>1</td>
<td>5</td>
<td>21</td>
<td>611</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>&quot;Named Insured&quot;</td>
<td>0</td>
<td>18</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>572</td>
<td>0</td>
<td>0</td>
<td>4</td>
</tr>
<tr>
<td>&quot;DOB&quot; OR &quot;D.O.B.&quot; OR (date w/3 birth)</td>
<td>0</td>
<td>21</td>
<td>0</td>
<td>14</td>
<td>50</td>
<td>309</td>
<td>0</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>liability w/2 insurance</td>
<td>0</td>
<td>30</td>
<td>6</td>
<td>3</td>
<td>0</td>
<td>421</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Date w/3 Coverage</td>
<td>0</td>
<td>20</td>
<td>0</td>
<td>0</td>
<td>3</td>
<td>386</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>&quot;Liability Insurance&quot;</td>
<td>0</td>
<td>20</td>
<td>0</td>
<td>3</td>
<td>0</td>
<td>386</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Date of birth</td>
<td>0</td>
<td>7</td>
<td>8</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>((transit OR bank* OR check* OR sav*) w/3 acc*) w/10 (&quot;no.&quot; OR number*))</td>
<td>0</td>
<td>18</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>discharge</td>
<td>0</td>
<td>15</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Fax and order</td>
<td>4</td>
<td>8</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>insured* w/2 policy</td>
<td>0</td>
<td>8</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Thoughtfully crafted and proven sets of search terms enables targeting of highly relevant, potentially impacted data early.
Predictive Coding to Enhance Data Classification

Continuous Active Learning bolsters content identification

- Finding and prioritizing content using predictive coding and technology assisted review tools streamlines data identification, classification, consistency, and reporting.

- Continuous Active Learning functionality can iteratively prioritize related content

- Results can be measured and extrapolated during initial impact assessments or fully applied during detailed document review
Quantifying Initial Results

Early estimates can be prepared based on initial workflow to quantify volume of impacted documents and records of impacted individuals.

<table>
<thead>
<tr>
<th>Department</th>
<th>% of total</th>
<th>Documents</th>
<th>Documents with Impacted Data</th>
<th>Customer Records per Document</th>
<th>Gross Estimate of Number of Potentially Impacted Individuals</th>
<th>Estimated Number of Unique Potentially Impacted Individuals (Assuming 50% Duplicates)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Department 1</td>
<td>83.48%</td>
<td>289,745</td>
<td>241,821</td>
<td>12</td>
<td>2,901,854</td>
<td>1,450,927</td>
</tr>
<tr>
<td>Department 2</td>
<td>7.81%</td>
<td>1,506,528</td>
<td>117,660</td>
<td>5</td>
<td>588,299</td>
<td>294,150</td>
</tr>
<tr>
<td>Department 3</td>
<td>5.13%</td>
<td>112,549</td>
<td>5,841</td>
<td>4</td>
<td>23,305</td>
<td>11,683</td>
</tr>
<tr>
<td>Department 4</td>
<td>1.43%</td>
<td>256,527</td>
<td>3,668</td>
<td>5</td>
<td>18,342</td>
<td>9,171</td>
</tr>
<tr>
<td>Department 5</td>
<td>1.20%</td>
<td>108,970</td>
<td>1,308</td>
<td>11</td>
<td>14,884</td>
<td>7,192</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Custodian Mailbox</th>
<th>% of total</th>
<th>Documents</th>
<th>Documents with Impacted Data</th>
<th>Customer Records per Document</th>
<th>Estimated Number of Potentially Impacted Individuals</th>
<th>Estimated Number of Unique Potentially Impacted Individuals (Assuming 50% Duplicates)</th>
</tr>
</thead>
<tbody>
<tr>
<td>David</td>
<td>24.90%</td>
<td>96,582</td>
<td>24,049</td>
<td>29</td>
<td>697,416</td>
<td>348,708</td>
</tr>
<tr>
<td>Maria</td>
<td>16.58%</td>
<td>502,176</td>
<td>83,261</td>
<td>30</td>
<td>2,497,823</td>
<td>1,248,912</td>
</tr>
<tr>
<td>Donna</td>
<td>14.15%</td>
<td>37,516</td>
<td>5,309</td>
<td>4</td>
<td>21,234</td>
<td>10,617</td>
</tr>
<tr>
<td>Lisa</td>
<td>6.24%</td>
<td>85,509</td>
<td>5,336</td>
<td>4</td>
<td>21,343</td>
<td>10,672</td>
</tr>
<tr>
<td>Joan</td>
<td>4.92%</td>
<td>36,323</td>
<td>1,787</td>
<td>7</td>
<td>12,510</td>
<td>6,255</td>
</tr>
</tbody>
</table>
Standard Data Capture Form

Unique Information about Individuals is Input Once

Individual names or businesses are entered into a centralized reusable database object as identified.
Standard Data Capture Forms

Potentially Impacted PII, PHI, PFI or PSI is Accounted For

- Default list of potentially impacted features account for domestic and global concerns from state level regulations to the GDPR.
- All capture options should be customized to address specific client needs and the nature of the data.
- Entering actual data points is typically minimized.

<table>
<thead>
<tr>
<th>Personally Identifiable Information</th>
<th>Financial Information</th>
<th>Other Account Information</th>
<th>Security Information</th>
<th>Health Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Driver’s License Number</td>
<td>Bank Account Number</td>
<td>Email Address w/ Password</td>
<td>Hom(e) Data</td>
<td>Medical Information</td>
</tr>
<tr>
<td>Social Security Number</td>
<td>International Bank Account Number</td>
<td>Unique Electronic Identifier w/ Password</td>
<td>Electronic/Digital Signature</td>
<td>Health Insurance Information</td>
</tr>
<tr>
<td>Individual Taxpayer Identification Number</td>
<td>Credit or Debit Card Number</td>
<td>Username w/ Password</td>
<td>Identity Protection PIN (IRIS)</td>
<td>LK National Health Service Number</td>
</tr>
<tr>
<td>EU Social Security Number or Equivalent ID</td>
<td>Other Financial Account Information</td>
<td></td>
<td>Mother’s Maiden Name</td>
<td>LK National Insurance Number (NINO)</td>
</tr>
<tr>
<td>EU National Identification Number</td>
<td>Access Code</td>
<td></td>
<td>Date of Birth</td>
<td>Health Status Information</td>
</tr>
<tr>
<td>Passport Number</td>
<td>Account Password</td>
<td></td>
<td>Manage</td>
<td>Other Health Information</td>
</tr>
<tr>
<td>Tribal Identification Card Number</td>
<td>Personal Identification Number</td>
<td></td>
<td>Manage</td>
<td>Manage</td>
</tr>
<tr>
<td>Other Identification Number</td>
<td>Security Code</td>
<td></td>
<td>Manage</td>
<td>Manage</td>
</tr>
<tr>
<td>Manage</td>
<td>Manage</td>
<td></td>
<td>Manage</td>
<td>Manage</td>
</tr>
</tbody>
</table>

Proprietary and Confidential
## Representative Sample of Results

Potentially Reportable Individuals, PII and PHI Features are Compiled

<table>
<thead>
<tr>
<th>Name</th>
<th>Address</th>
<th>Minor</th>
<th>Deceased</th>
<th>Social Security Number</th>
<th>Driver's License</th>
<th>State ID</th>
<th>Date of Birth</th>
<th>Passport Number</th>
<th>Health Insurance Identification Number</th>
<th>Checking or Savings Account Number</th>
<th>Medical History</th>
<th>Disability Info</th>
<th>Prescription Information</th>
<th>Physician Provider Identifier</th>
<th>Medical Record Number</th>
<th>Health Insurance Information</th>
<th>Associated Documents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last 1, First 1</td>
<td>Address 1</td>
<td>Y</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>REL00001090; REL00001417</td>
</tr>
<tr>
<td>Last 2, First 2</td>
<td>Address 2</td>
<td></td>
<td>Y</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>REL00006605; REL00006656</td>
</tr>
<tr>
<td>Last 3, First 3</td>
<td>Address 3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>REL00007796; REL00007802</td>
</tr>
<tr>
<td>Last 4, First 4</td>
<td>Address 4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>REL00002143</td>
</tr>
<tr>
<td>Last 5, First 5</td>
<td>Address 5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>REL00008517; REL00008663; REL00008759</td>
</tr>
</tbody>
</table>

Results of data capture, including all unique names and types of personal information are easily reportable. Counsel can assess and respond to reporting obligations based on relevant requirements.
4 Case Studies

Projects, Metrics and Industries
Noteworthy Metrics

Personal data buried in unstructured data like email, file systems, and collaboration platforms is pervasive and can pose a tedious challenge.

<table>
<thead>
<tr>
<th></th>
<th>Compromised Documents</th>
<th>Documents with suspect PII or PHI</th>
<th>Impacted Individuals</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>616,293</td>
<td>187,733</td>
<td>~ 25,000</td>
</tr>
<tr>
<td>2</td>
<td>284,405</td>
<td>155,452</td>
<td>~ 4,500</td>
</tr>
<tr>
<td>3</td>
<td>82,459</td>
<td>41,815</td>
<td>41</td>
</tr>
<tr>
<td>4</td>
<td>60,595</td>
<td>25,211</td>
<td>1,298</td>
</tr>
<tr>
<td>5</td>
<td>16,320</td>
<td>4,057</td>
<td>322</td>
</tr>
</tbody>
</table>
How Many Reportable Individuals Might be Impacted?

We find client data tends to contain many reports with duplicative and overlapping customer information

- Many organizations tend to frequently generate reports that contain detailed information about specific individuals.
- Reports are frequently distributed via email and saved on file systems.
- Reports tend to have information about the same people reported frequently.
- In the example on the right, one organization’s data had a rate of 20:1 when comparing rows of client data to unique individuals
  - Although, in another instance, we found a ratio of approximately 40:1
  - Of course, results can vary greatly depending on unique business practices in any organization
- Generally, the rate of duplicity increases throughout the compilation of multiple reports over time
Case Study | Data Breach Impact Analysis

KLDiscovery Technology Assisted Methodologies Precisely Targeted Potentially Relevant Data

**Number of Documents**

- **Total Compromised**: 13,349,000
- **Unique Records Identified using KLDiscovery Technology**: 3,893,000
- **Potentially Reportable based on Actual Identifiers Found**: 3,173,000
- **Confirmed Reportable Information According to Applicable Criteria**: 755,974

**Efficient Cost Control:** KLDiscovery’s technology assisted methods eliminated 71% of data from review.

**Precision:** 82% of targeted data set actually contained relevant PII or PHI identifiers.

**Containment:** 24% of the documents with identifiers met the state specific criteria for notification.

**Project Timeline:** 3 Months
Case Study | Discovery Response to Data Breach

Lesson learned: The scope of discovery in litigation can be managed with technology

The Case
Two class action suits were filed against a major retailer after a data breach. KLDiscovey was hired to conduct an extensive analysis of the data that was collected for discovery responses related to the breach.

Challenges: A major U.S. retailer suffered a large data breach resulting in loss of customer information, which led to litigation filed against the retailer by a number of financial institutions.

Solution: KLDiscovey assisted with data preservation and collection, early case assessment, extensive search analytics, and predictive coding. We combined search term analytics, Concept Clustering, Advanced Review Services, and structured data solutions to identify relevant material and reduce the amount of data for manual attorney review.

Outcome: Over 1 million records were excluded from review, which would have otherwise been included through traditional search mechanisms. The results of our efforts enabled expedient and prioritized review of over 150,000 records, proactive data productions, and well-informed search term negotiations with opposing counsel.
Additional Project Overviews

Reportable PII or PHI found in unstructured data sources can be surprising in some industries

- **An employee benefits broker with client data regarding employees.** The breached data included PHI (HIPAA) as they were the client employee’s advocate to insurance companies as well as PII based on benefit enrollment. Reporting was done on a per client basis to streamline the communication with their clients.

- **An accounting firm where three partners and an administrative assistant’s email accounts were compromised.** The first phase required review of the documents for a specific period of time for client and firm confidential information, information that could be used to perpetuate additional phishing attacks, and Personally Identifiable and Personal Financial Information on clients and the clients employees. Reporting was done both on a document level for the confidential information and potential fraud concern and on a client and employee basis for those with PII or PFI potentially exposed.

- **A life insurance company that had two agent accounts breached that contained PII and PFI information on their clients.** Document meta-data was added to the Impacted Individuals in order to allow the parent company to work with their agents on notification requirements.

- **A real-estate company where multiple broker/agent accounts were breached** that contain real estate documents with PII information. In addition to identifying the affected data, KLDiscovey’s work enabled counsel to enhance compliance training.
Industry Trends & Case Law

Where are we headed from here?
Expanding Scope and Need for More Clarity in Data Breach Litigation

Overall, the standard of harm varies

- A continued threat of harm such as identity theft is enough to claim injury
  - Theresa Stevens et al. v. Zappos.com Inc.¹
  - CareFirst, Inc., et al., Petitioners v. Chantal Attias, et al.²
  - Fero et al v. Excellus Health Plan, Inc. et al³

- Punitive damages claims on the rise in some jurisdictions
  - Larry Wade et al. v. ABM Industries Inc.⁴
  - City of San Francisco, City of Chicago, Massachusetts attorney general, Cook County and the Washington state attorney general have all filed suits against companies who have been breached⁵

- While the merits of bringing suit seem to be surviving lengthy appeals, it doesn’t necessarily mean damages will be easily proven
  - Note cases against Barnes & Noble, Neiman Marcus and P.F. Chang’s⁶

- But punitive damages in other courts aren’t easily accepted
  - In Re: Yahoo! Inc. Customer Data Security Breach Litigation⁷

- HMH operates 17 Hospitals
- Their network was disrupted for 2 days by a ransomware attack on December 2, 2019
- Plaintiff’s filed suit in February 2020
- Claim that the ransomware attack disrupted their medical services for days and exposed their sensitive medical information to thieves
- A breach hadn’t been reported to DHHS
- The suit’s focus is on the potential for harm due to their belief their information was compromised

<table>
<thead>
<tr>
<th>Does the risk of harm alone support a lawsuit?</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>No</strong></td>
</tr>
<tr>
<td>Peters v. St. Joseph Services Corp., S.D. TX.</td>
</tr>
<tr>
<td>Dyson v. Sky Chefs Inc., N.D. TX.</td>
</tr>
<tr>
<td><strong>Yes</strong></td>
</tr>
<tr>
<td>Perrill v. Equifax, W.D. TX.</td>
</tr>
<tr>
<td>U.S. Court of Appeals for the Seventh Circuit</td>
</tr>
<tr>
<td>U.S. Court of Appeals for the Third Circuit</td>
</tr>
</tbody>
</table>
Healthcare Sector Impacts

Ransomware incidents and class action litigation

Class action lawsuit filed in February 2020 against two hospitals in Puerto Rico for alleged ransomware attacks

- Ransomware attack on Pavía Hospital Santurce and Pavía Hospital Hato Rey hospitals, affected 305,737 people in February 2019
- Plaintiffs claim their PII was affected, have had to pay for identity protection and face potential for future harm
- Hospitals claim patient information was not compromised
- Ransomware, however, is increasingly used in tandem with exfiltration of data

Allscripts, Inc. faced a class-action lawsuit filed by a healthcare provider in 2018 after a ransomware attack

- The January 2018 attack prohibited access to Allscripts electronic health record, scheduling and patient management platforms
- Plaintiff argued “While no sensitive or health information is disseminated, the risks to patient treatment, health, and safety are significantly increased because of the serious and even life-threatening consequences presented by even a short-lived interruption of health care services.”
- Surfside also alleged Allscripts’ “wanton, willful, and reckless disregard” also allowed for a breach under HIPAA patient privacy laws.
- The suit was thrown out in 2019 based on responsibility and an enforceable arbitration clause with the LLC
Cyber Industry Outlook

Challenges and opportunities

- **Prediction:** The industry and case law will coalesce around models that calculate the inherent value of data

- Securely managing data in a cohesive fashion continues to conflict with entrepreneurial, competitive markets, sectors or business units
  - More cohesive data management can bring efficiencies that lead to competitive advantages

- The problem and the solution are incongruent because the amount of data and the number of daily attacks are so overwhelming.
  - The $150 billion cyber security market is on pace to exceed $200 billion by 2021
  - Responding to breaches is laborious, leading to an average cost of $141 per lost or stolen record or $3.6 million per incident.

- Yet, there is a big talent gap that continues to grow, with approximately 350,000 open cyber security positions
  - It could 3.5 Million by 2021

- Technology is still on the chase
  - Employment talent gap signals unsolved innovation
  - Talent, technology and innovation will need to come together
Conclusions

What should we do next?
What’s Next?

How can you act on today’s information with your clients?

- Align data-driven solutions with executive leadership
  - Corporate Counsel
  - CISO
  - Law Firm Cyber Practices
- Have the response team and response plan in place ahead of time
- Consider reporting requirements in all domestic and international jurisdictions
- Sample representative data to measure and mitigate risk
  - Remember, there’s more out there than you think
  - DLP technology might not be enough
## Proactive Approaches

Marshal the expertise and information you need to get ahead wherever possible

<table>
<thead>
<tr>
<th>Conduct proactive impact analysis to measure potential risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Sample data to see how much semi managed data could be at risk</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Conduct training</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Train users and data stewards to securely transfer data</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Perform data remediation</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Minimize proliferation of private data</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Enhance data governance</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Align data use with policies and practices</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Evaluate your plan</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Look for opportunities for continual enhancement</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Test the plan with table top exercises</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Invest in time and expertise to run through how you will respond to an incident</td>
</tr>
</tbody>
</table>
Be Prepared for Discovery in Resultant Litigation

- Where are relevant information management, security, usage and incident response policies, practices, workflows, training and attestations maintained?
- What systems and devices are being used for communications and decisions during and after the incident?
- Who are the relevant custodian? They aren’t necessarily the same ones who have been attacked.
- Are actual incident reports, analyses, advice, etc., being centrally compiled from the outset?
- Which sets of impacted data are necessary, available and preserved for support and analysis of the claims and defenses of the matter(s)?
What Questions Do You Have?
We will be hosting a series of webinar events throughout 2021

Please check the events page on KLDiscovery.com or our social media channels for the latest info as new events are announced.


11. Resources and commentary about the economic value of data:
UPCOMING EVENTS
The 2021 virtual Commonwealth of Virginia Information Security Conference is open for registration! The theme of the conference is “2021 Cybersecurity Reboot: Tools for building cyber resilience.” In addition to break-out presentations, the conference program will feature two keynote addresses.

**We encourage you to register early – we expect to reach maximum capacity!**

**Date:** June 24  
**Location:** Virtual! Event will be hosted by the College of William & Mary.  
**Registration cost:** $25 for conference, which covers access to top-notch speakers and presentations, as well as a conference swag bag (mailed to participants).  
**Questions:** covsecurityconference@vita.virginia.gov
AGENCY SECURITY AWARENESS TRAINING FORM REMINDER

The Agency Security Awareness Training Solution Form was due on April 16. We still have agencies who have not submitted the form, and it is imperative that you submit the form to let us know what training solution you are currently using. **Reminder:** The training program must be in compliance with the requirements listed in SEC527 by January 1, 2022.

If you do not have access to Archer, you may submit your completed form to Commonwealthsecurity@vita.virginia.gov.

The form is located at the link below:

https://www.vita.virginia.gov/policy--governance/itrm-policies-standards/

If you questions about completing the form, contact: Tina.gaines@vita.virginia.gov
2021 National Security Poster Contest Winner!

Melia – Spotsylvania High School
2021 National Security Poster Contest Finalist!

Esthefanny – Patrick Henry High School
2021 National Security Poster Contest Finalist!

Javier – G.H. Reid Elementary School
IS ORIENTATION

DATE:  June 30, 2021

TIME:  1 p.m.

REGISTRATION LINK:  
https://covaconf.webex.com/covaconf/onstage/g.php?MTID=e36fecc7d3d8344a0b0944dfa8f891bcc

PRESENTER:  Marlon Cole (marlon.cole@vita.virginia.gov)
JUNE ISOAG MEETING DETAILS

Date: June 2
Time: 1- 4 p.m. WebEx

Agenda
Patrick Robinson & Bindu Sundaresan, ATT

Tony Encinia, Dell

Mark Martens & Jon Smith, VITA
THANK YOU FOR ATTENDING!