

MAY ISOAG MEETING



AGENDA

- GREG WILLIAMS, EY
- BEN TIMMS, HP
- ERIC ROBINSON, KLDISCOVER
- UPCOMING EVENTS
- ADJOURN

TPRM Insights Session

Virginia Information Technologies Agency (VITA)
May 2021



The better the question.
The better the answer.
The better the world works.



EY

Building a better
working world

Today's presenters



Sam Jamison, PMP

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

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.



Operations and business services

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



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.



Finance

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



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.



Supply chain

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



Risk

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



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.

Functional focus



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**.



Third parties

- Suppliers
- Contractors
- Joint Ventures
- Service Providers
- Brokers
- Agents
- Specialty Mfg.
- Mutual Assistance
- Business Associates
- Consultants
- Vendors
- First Tier, Downstream and Related Entities

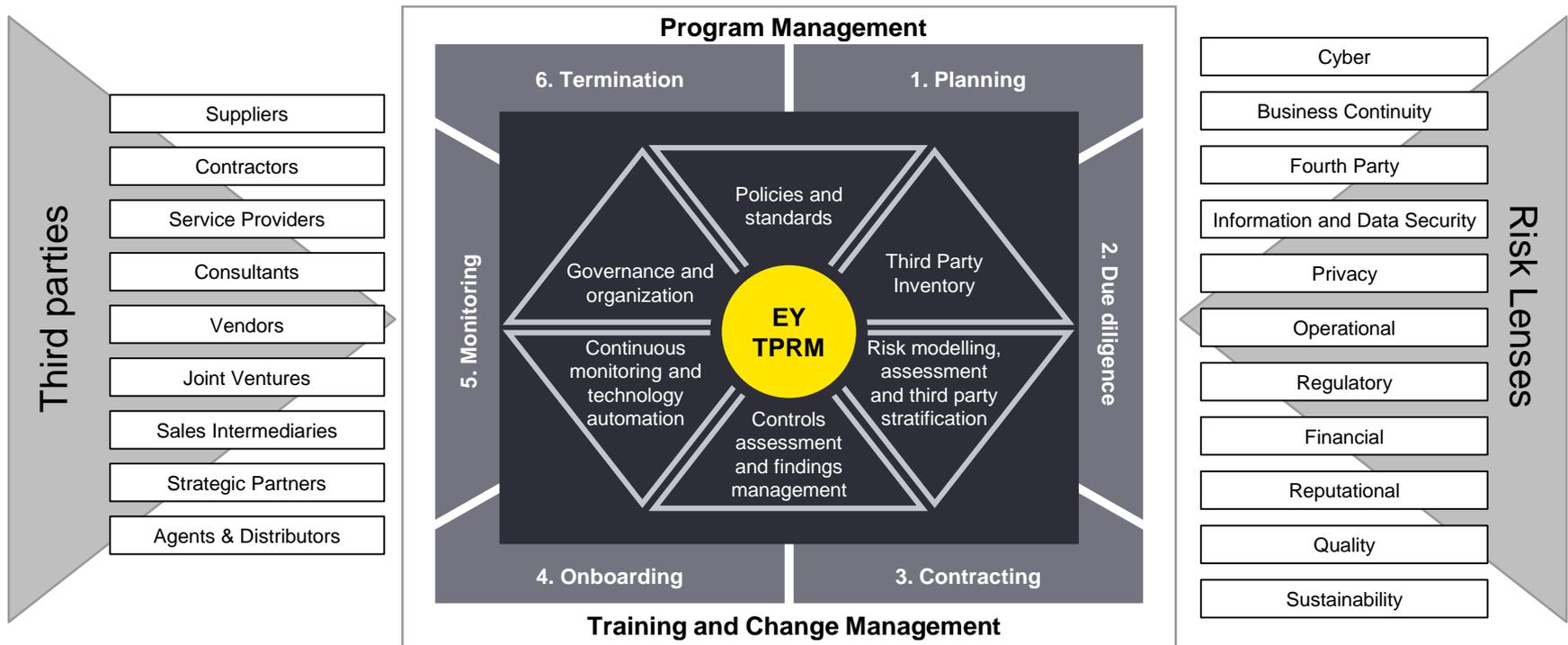
Contracts

- General Contract for Services
- Statement of Work
- Leases
- Business Associate Agreements
- Master Service Agreement

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).



Risks associated with third 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.

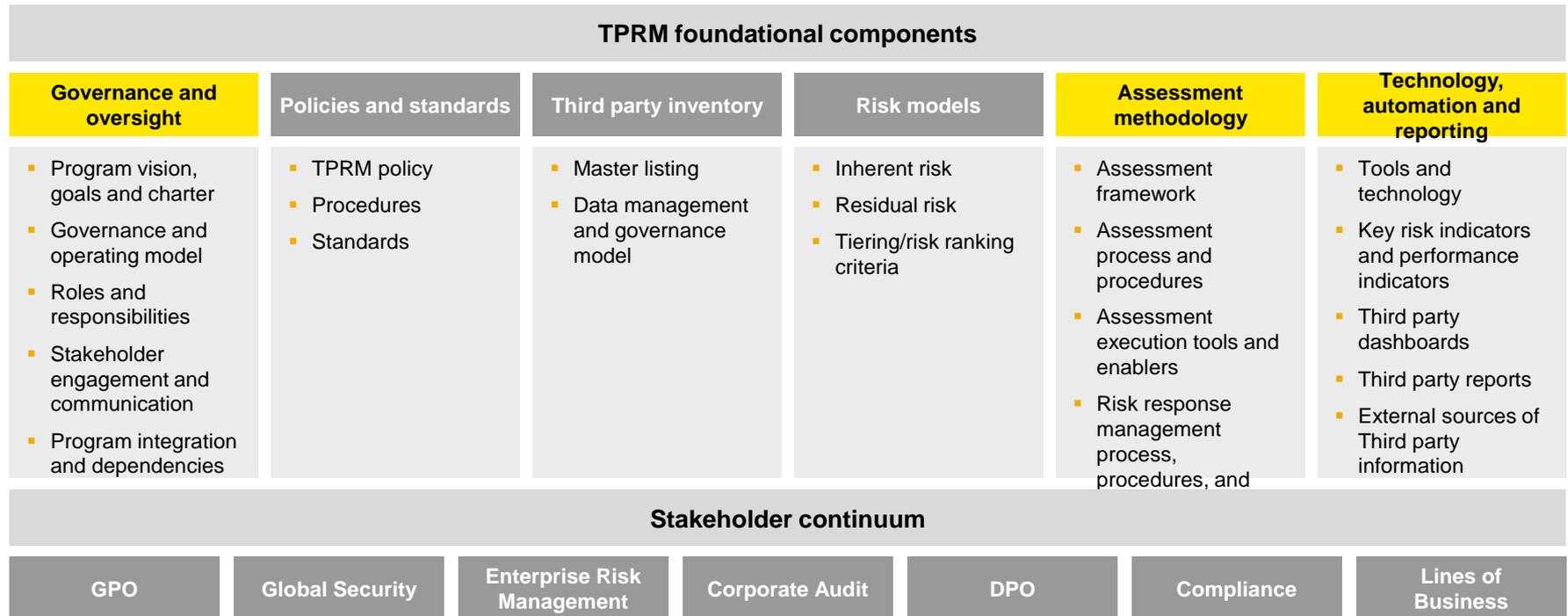
Diverse set of risks associated with third parties		
<p>Geopolitical risk</p> <p>Risk of doing business in a specific country and includes legal, regulatory, political and social economic considerations</p>	<p>Reputational risk</p> <p>Risk that the organization's brand and reputation is impacted should an event occur at the third party</p>	<p>Financial risk</p> <p>Risk that the third party cannot continue to operate as a financially viable entity</p>
<p>Regulatory and compliance risk</p> <p>Risk that a third party fails to comply with a required regulation, thus causing the organization to be out of compliance</p>	<p>Sustainability</p> <p>Risk that impacts a company's ability to execute its strategy and objectives</p>	<p>Cyber and privacy risk</p> <p>Risk that an organization's data is lost or security is compromised due to deficiencies in the cybersecurity and privacy controls of the third party</p>
<p>Operational risk</p> <p>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</p>	<p>Strategic risk</p> <p>Risk that the organization's and third party's strategic objective are misaligned</p>	<p>Business continuity and resiliency risk</p> <p>Risk of third party failure on the continuation of business as usual for the organization</p>



TPRM foundational components

Third party risk management components

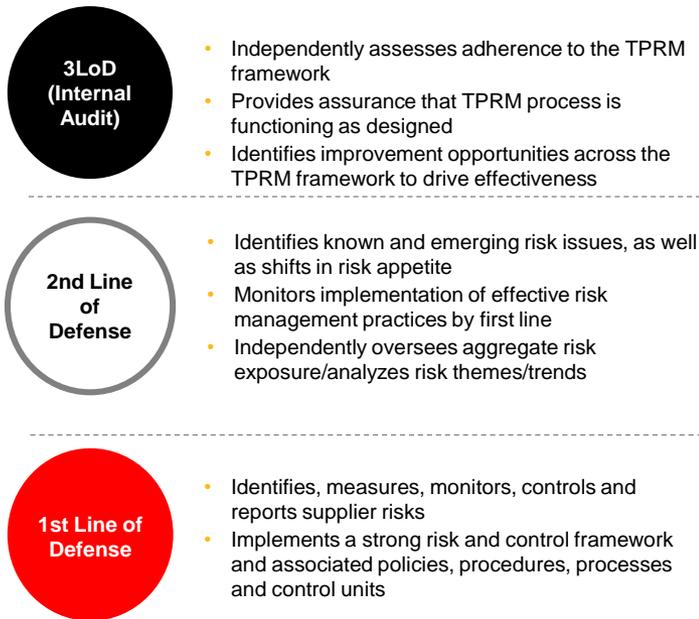
To manage third party risks, it is critical to establish foundational components within TPRM



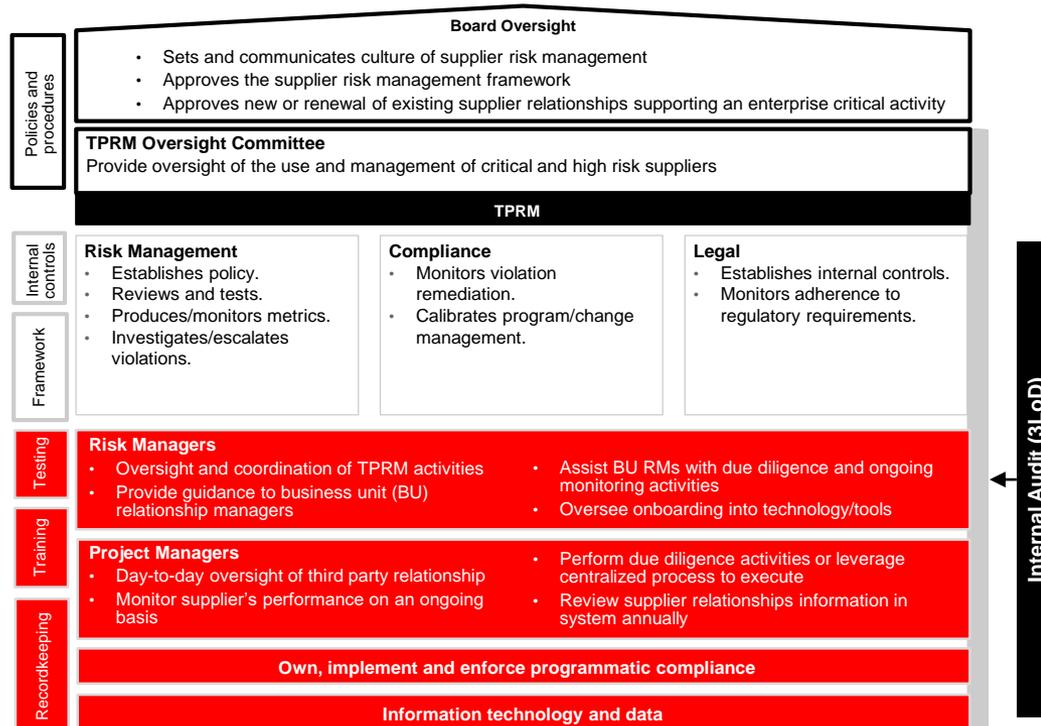
Governance and oversight overview

Category	Internal Audit	Risk Management	Compliance	Legal	Other
Board Oversight					
TPRM Oversight Committee					
Internal Controls					
Framework					
Testing					
Training					
Recordkeeping					

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.



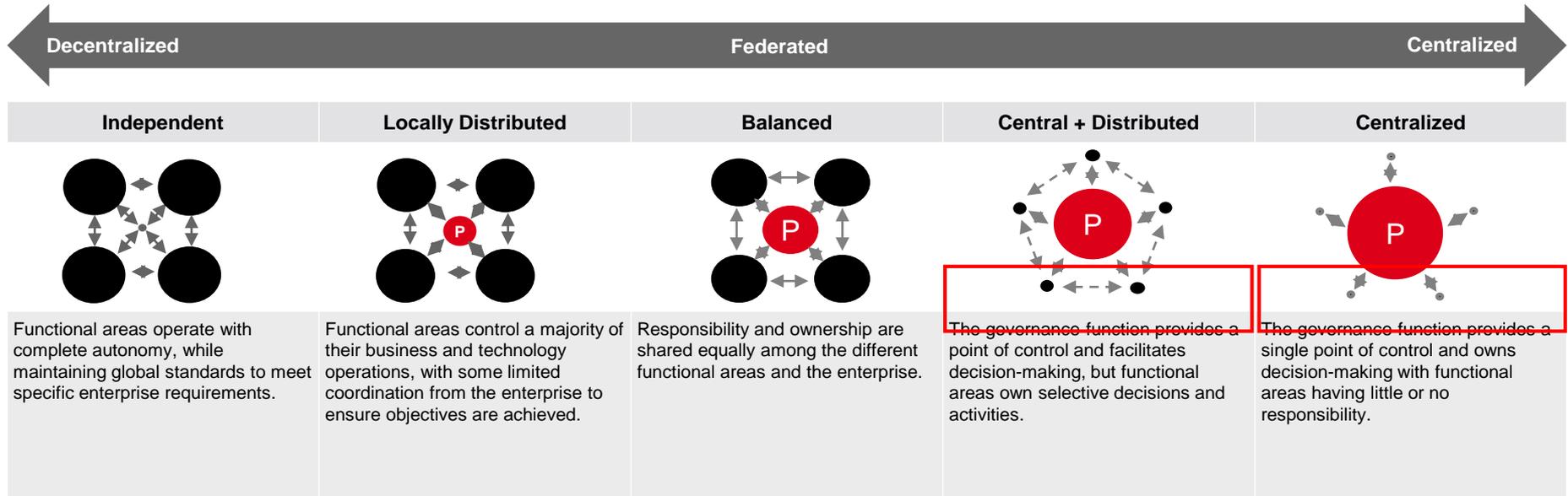
Continuous improvement and reporting drives compliance and optimization across the organization.



Governance and oversight overview

Category	Strategic	Operational	Compliance	Reporting	Monitoring	Improvement
Leadership	Board of Directors	Senior Management	Compliance Committee	Reporting Committee	Monitoring Committee	Improvement Committee
Policy	Enterprise Risk Management	Business Continuity	Information Security	Operational Resilience	Third Party Risk	Vendor Management
Process	Risk Assessment	Risk Mitigation	Risk Monitoring	Risk Reporting	Risk Improvement	Risk Review
Tools	Risk Register	Risk Dashboard	Risk Heatmap	Risk Scorecard	Risk Maturity Model	Risk Self-Assessment

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.



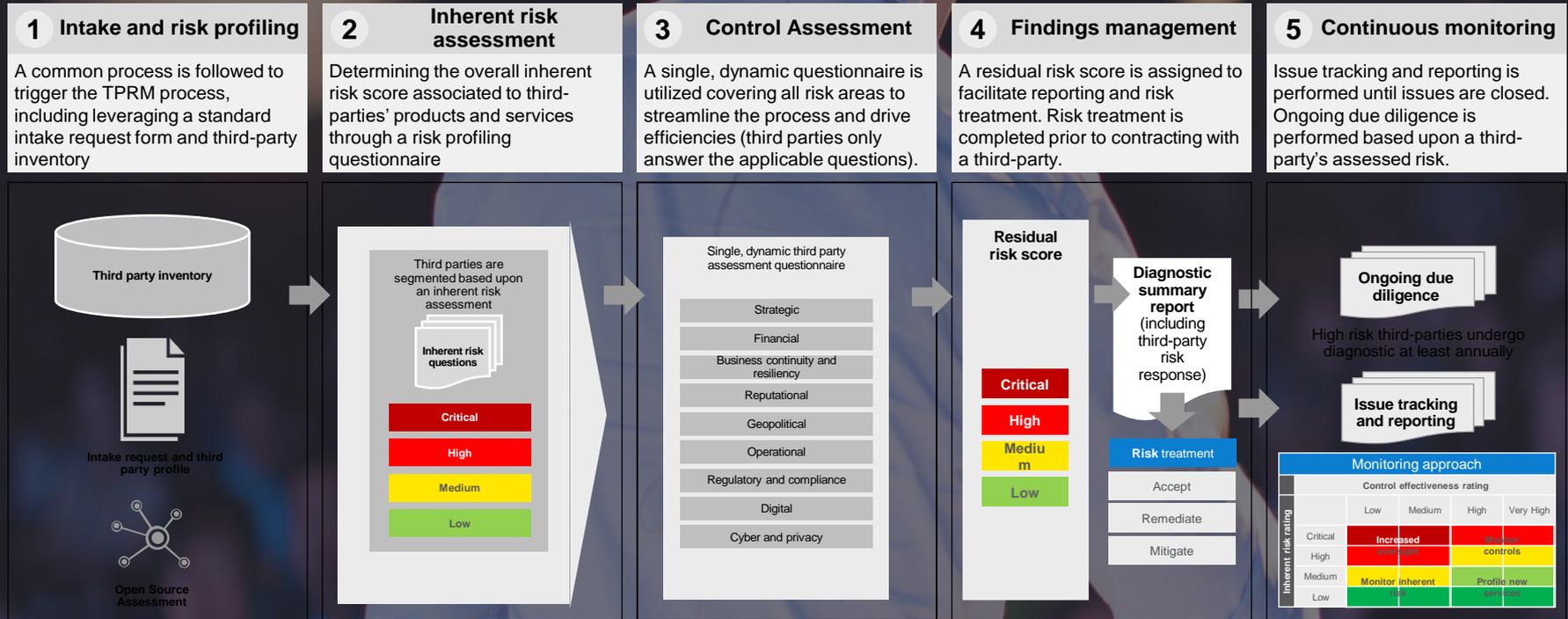
Key considerations

- 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

Third Party Assessment				
Category	Sub-category	Weight	Score	Overall Rating
Strategic	Business continuity and resiliency	10	10	Critical
	Financial	10	10	
	Reputational	10	10	
	Geopolitical	10	10	
Operational	Operational	10	10	High
	Regulatory and compliance	10	10	
	Digital	10	10	
	Cyber and privacy	10	10	
Business continuity and resiliency	Business continuity and resiliency	10	10	Medium
	Financial	10	10	
	Reputational	10	10	
	Geopolitical	10	10	
Cyber and privacy	Business continuity and resiliency	10	10	Low
	Financial	10	10	
	Reputational	10	10	
	Geopolitical	10	10	

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



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

Monitoring approach				
Control effectiveness rating				
	Low	Medium	High	Very High
Inherent risk rating	Critical	Increased	Review controls	
	High			
	Medium	Monitor inherent	Profile new	
Low				

Standard TPRM Process Triggers

Triggers	Example	Future-State Considerations
New Supplier	VITA engages a new supplier to provide goods or services.	Risk assessment process triggered as a part of the supplier registration/qualification process.
Existing Supplier, New Service	VITA purchases additional goods or services from an existing supplier.	Risk assessment is triggered prior to finalizing an agreement/contract with the supplier, which may be triggered at the point of contracting.
Change Order/Amendment	VITA agrees to a change order for an existing service provided by a supplier.	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).
Proof-of-Concept	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.	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.
Reassessment	A supplier requires a new assessment based on defined criteria (i.e., higher risk supplier that has not been assessed in 1 year).	Risk assessment triggered based on the last assessment date subject to the supplier being active and continuing to provide services to the organization.
Ad Hoc	Potential risks or concerns regarding an existing supplier are raised by an employee.	A Business Owner may request an assessment via a formal ticketing process.

Standard TPRM Process Triggers

Category	Item	Item	Item	Item	Item
Information Security					
Business Continuity					
Regulatory	Regulatory	Regulatory	Regulatory	Regulatory	Regulatory
Other	Other	Other	Other	Other	Other

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*?



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

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



Due diligence assessments (sample)

Privacy due diligence



Cyber/InfoSec due diligence



Business continuity due diligence

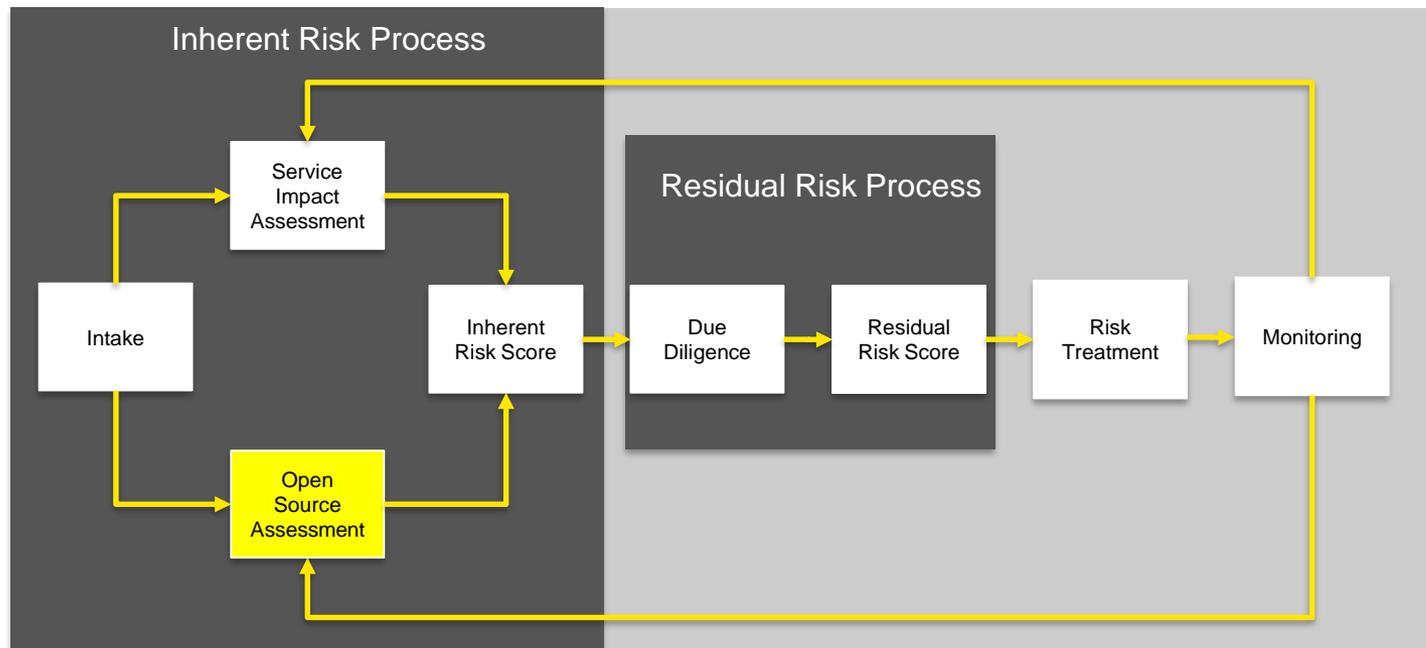


Regulatory due diligence

Open source assessments

Open Source Intelligence (OSINT) Data Sources				
Source	Category	Strengths	Weaknesses	Use Cases
Public Records	Government	Highly accurate	Often outdated	Background checks
News Media	Journalism	Timely reporting	Subjective bias	Public opinion
Social Media	Personal	Real-time updates	Unverified info	Reputation management
Academic Papers	Research	Highly credible	Niche focus	Technical insights
Industry Reports	Business	Market insights	Proprietary data	Competitive analysis

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



Open source evaluation

Rapidly evaluate a vendor based upon open source validated information to enable risk based decisions earlier in the process

Category	Sub-category	Score	Weight	Overall Score
Cyber Security	Vulnerabilities	High	10	10
	Data protection	Medium	10	10
	Data Privacy	Low	10	10
	Application security	Medium	10	10
Corporate Ownership	Ownership structure	High	10	10
	Board Members	Medium	10	10
	Political Exposed persons	Low	10	10
Geo-Political	Country Stability	High	10	10
	Country Risk	Medium	10	10
	Terrorism	Low	10	10
	Logistics	Medium	10	10
	Corruption	High	10	10
Compliance	Anti Corruption / Bribery	High	10	10
	Sanctions	Medium	10	10
	Tax Evasion	Low	10	10
	Government Fraud	Medium	10	10
	Environmental Protection	High	10	10
	Foreign Trade	Medium	10	10
Finance	Debt	High	10	10
	Margin	Medium	10	10
	Growth	Low	10	10
	Liquidity	Medium	10	10



Cyber Security

- ▶ Vulnerabilities
- ▶ Data protection
- ▶ Data Privacy
- ▶ Application security
- ▶ Historic breach activity
- ▶ Industry Certifications (e.g. ISO)



Corporate Ownership

- ▶ Ownership structure
- ▶ Board Members
- ▶ Political Exposed persons



Geo-Political

- ▶ Country Stability
- ▶ Country Risk
- ▶ Terrorism
- ▶ Logistics
- ▶ Corruption
- ▶ Business Culture
- ▶ Infectious Disease Vulnerability



Compliance

- ▶ Anti Corruption / Bribery
- ▶ Sanctions
- ▶ Tax Evasion
- ▶ Government Fraud
- ▶ Environmental Protection
- ▶ Foreign Trade



Finance

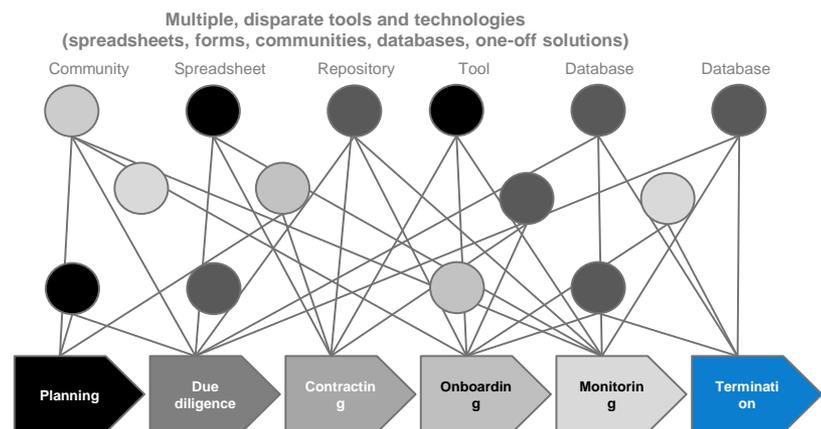
- ▶ Debt
- ▶ Margin
- ▶ Growth
- ▶ Liquidity
- ▶ M&A
- ▶ Divestiture

Technology, automation and reporting

Third Party Risk Management					
Category	Sub-category	System	Integration	Reporting	Notes
Risk Management	Supplier Risk	SRM	ERP	Dashboard	High
	Contract Risk	CRM	Contracts	Dashboard	High
	Operational Risk	ORM	HR	Dashboard	High
	Compliance Risk	CRM	Feeds	Dashboard	High
	Financial Risk	FRM	ERP	Dashboard	High
	Reputational Risk	RRM	Feeds	Dashboard	High
	Legal Risk	LRM	Contracts	Dashboard	High
	Environmental Risk	ERM	Feeds	Dashboard	High
	Human Resources Risk	HRM	HR	Dashboard	High
	Information Security Risk	ISM	Feeds	Dashboard	High

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.

Current state (Illustrative)

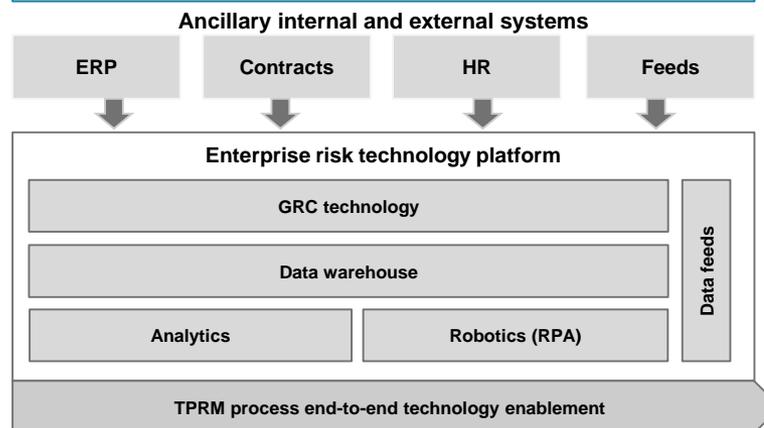


Costs

- 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.

Future state (Illustrative)

Rationalize



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

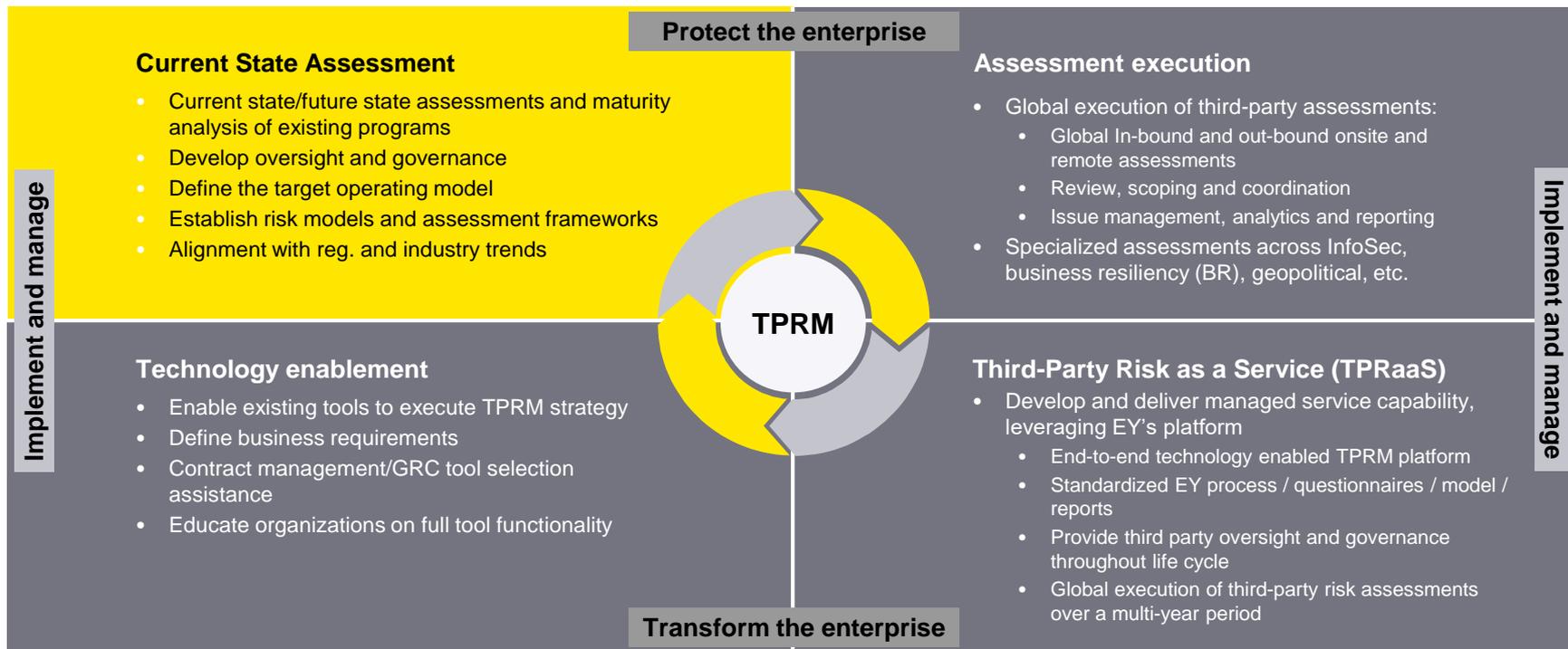
Technology Capabilities					
Technology	Capabilities	Benefits	Current usage	Challenges	Future Outlook
Governance, risk and compliance (GRC) technology	Automates and standardizes risk activities (e.g., issue management, reporting, assessments). Serves as a single "source of truth" for risk, control and 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)	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	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	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.		

Technology	Description	Capabilities	Benefits	Current usage
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.	<ul style="list-style-type: none"> 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). 	<ul style="list-style-type: none"> Provides a holistic view of risk across the organization, including regulatory compliance. Provides dynamic and real-time risk and control intelligence and reporting. 	<ul style="list-style-type: none"> 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.	<ul style="list-style-type: none"> Automates routine activities (e.g., testing, evidence reviews). Automates review of third parties responses to a questionnaire or submission of evidence. 	<ul style="list-style-type: none"> Reduces costs, errors and process cycle time. Increases economies of scale. 	<ul style="list-style-type: none"> 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.	<ul style="list-style-type: none"> 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. 	<ul style="list-style-type: none"> Identifies patterns and improves execution speed. Allows employees to make better decisions. 	<ul style="list-style-type: none"> 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.	<ul style="list-style-type: none"> Facilitates unsupervised learning on broad data access. 	<ul style="list-style-type: none"> Processes large volumes of data. Generates real-time reports. Provides insights into emerging risks. 	<ul style="list-style-type: none"> Risk pattern analysis and trending.

A hand holding a magnifying glass over a long, brightly lit office hallway. The hallway has large windows on both sides, potted plants, and a wooden floor. The scene is viewed through the lens of the magnifying glass, which is held by a hand. The text "EY TPRM Service Offerings" is overlaid in yellow on a dark blue horizontal band across the middle of the image.

EY TPRM Service Offerings

EY's TPRM service offerings



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

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

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

EY | Building a better working world

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

ISOAG



Ben Timms

Print security and Solutions Specialist



TODAY'S THREAT LANDSCAPE

600% INCREASE OF **CYBERTHREAT** INDICATORS RELATED TO CORONAVIRUS PANDEMIC*



Johns Hopkins COVID-19 map



Deteque botnet threat map



*<https://www.cyfirma.com/news/coronavirus-in-cyberspace/>



WHAT HAS CHANGED FOR IT SECURITY?



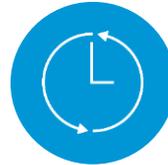
Large number of Corporate Endpoints are outside the IT “Sphere of Control”

- Beyond corporate “perimeter”
- Harder to update OS/Firmware/Apps
- Data leakage to personal devices
- Not designed with security features



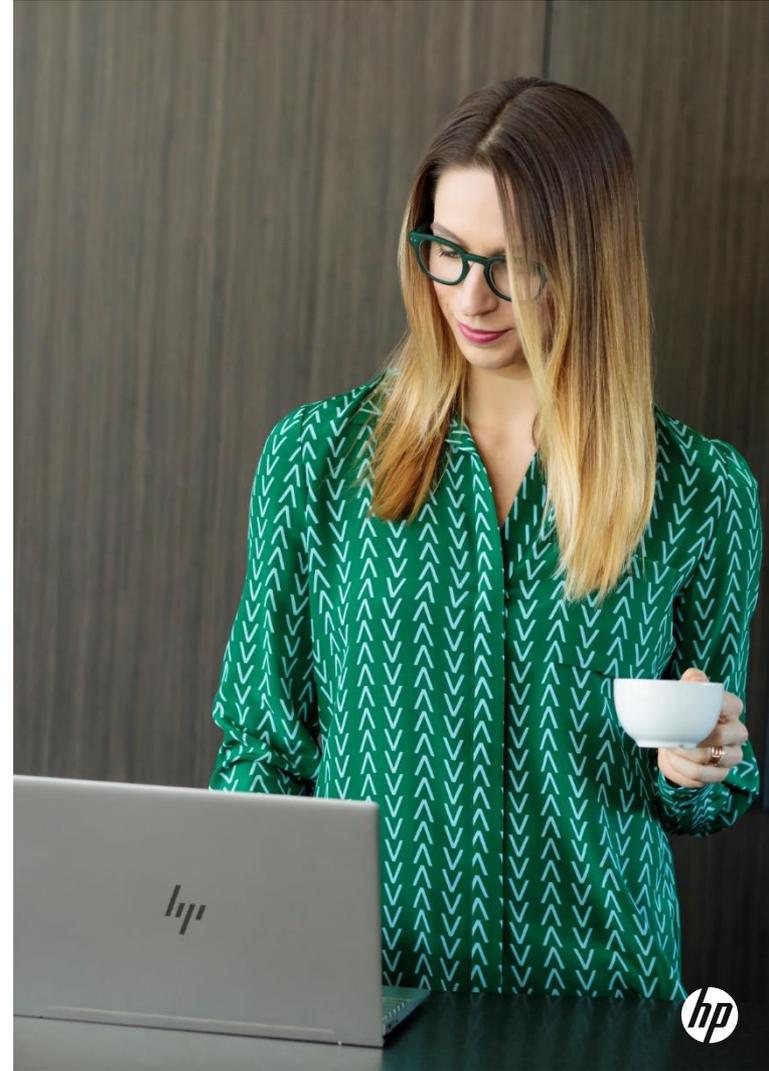
Remote work infrastructure not designed for scale

- 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



Rapidly changing tactics of cyberthreat



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.

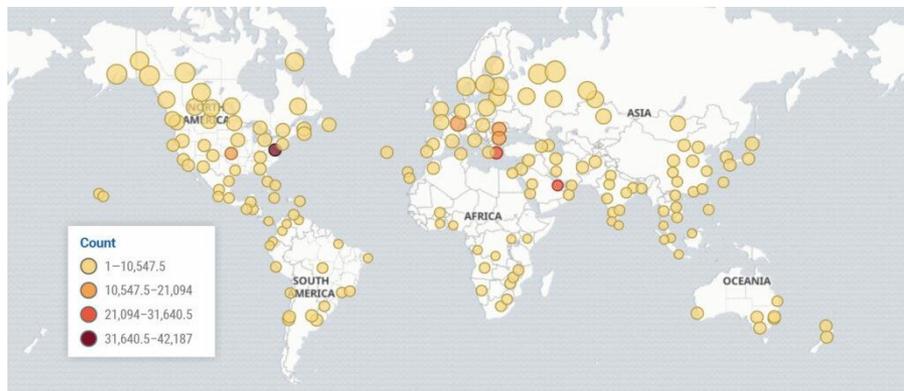
Cyber criminals are pivoting towards long-term command and control presence on networks and moving “farther down the stack” to get low-level access to systems.

Trickbot Malware's newest trick... TrickBoot



“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.”

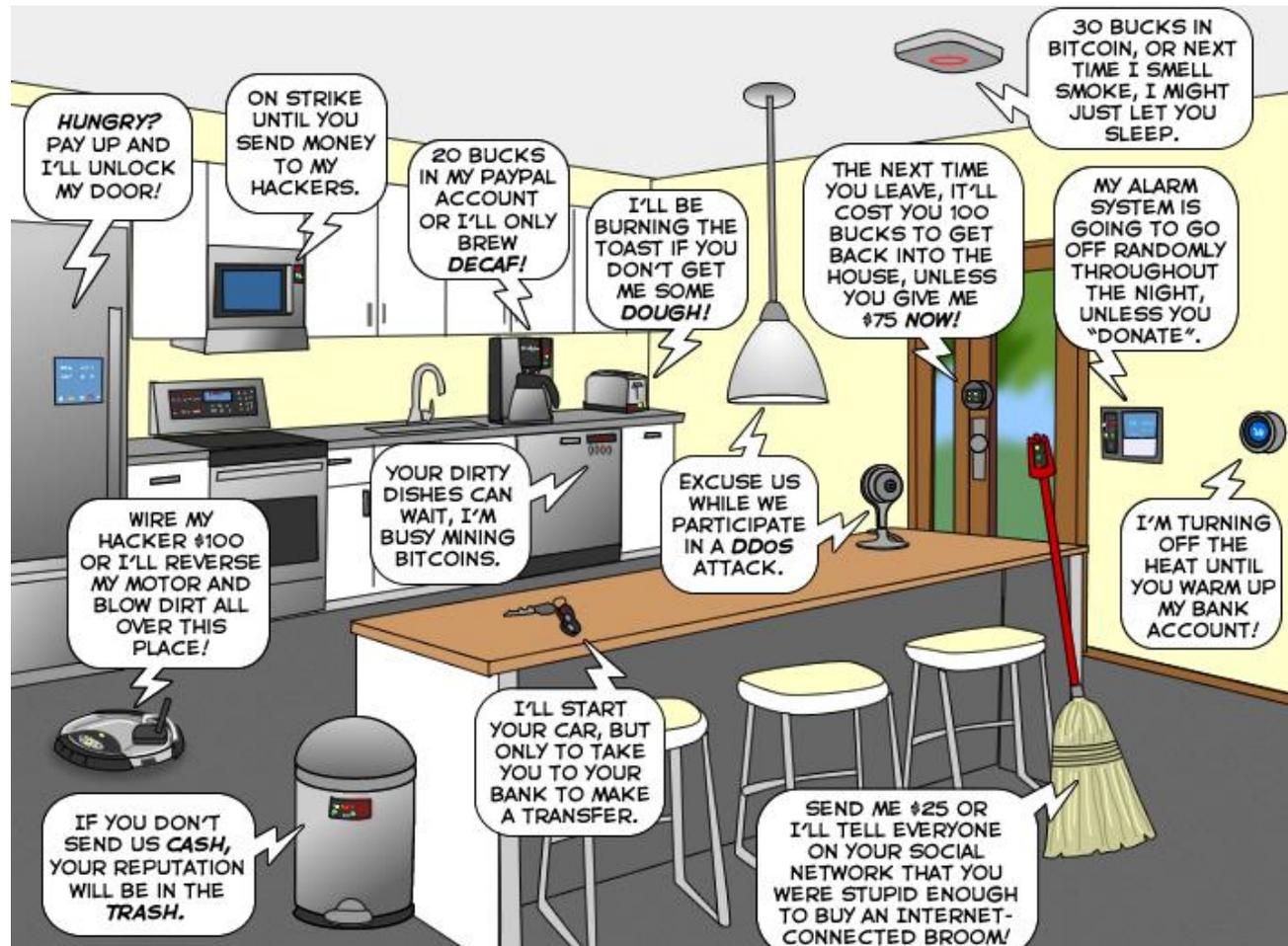
Remotely brick a device at the firmware level
Bypass security controls such as BitLocker, ELAM, Windows 10 Virtual Secure Mode, Credential Guard, endpoint protection controls like A/V, EDR, etc.
Set up a follow-on attack
Reversing ACM or microcode updates that patched CPU vulnerabilities like Spectre,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



t

[https://eclipsium.com/2020/12/03/trickbot-now-offers-trickboot-persist-brick-profit//](https://eclipsium.com/2020/12/03/trickbot-now-offers-trickboot-persist-brick-profit/)

THE INTERNET OF RANSOMWARE THINGS



Source: joyoftech.com

THE INTERNET OF VULNERABILIT IES



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

More collaboration
says research.

... can't cause harm to patients.



CLICK HERE FOR DESTRUCTION

Security and Survival in
a Hyper-connected World

OK





SHODAN



mirai
malware

```
c:>PRET-master\pret.py 192.168.1.200.pl
```



(ASCII art by Jan Foerster)

```
PRET| Printer Exploitation Toolkit v0.40
by Jens Mueller <jens.a.mueller@rub.de>
pentesting tool that made
dumpster diving obsolete
```

```
Nmap scan report for hub
Host is up (0.046s latency).
Not shown: 995 closed ports
PORT STATE SERVICE
8008/ tcp open http
8009/ tcp open ajp13
8443/ tcp open https-alt
9000/tcp open cslistener
10001/ tcp open scp-config
```



WAYS TO EXPLOIT YOUR IOT DEV

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



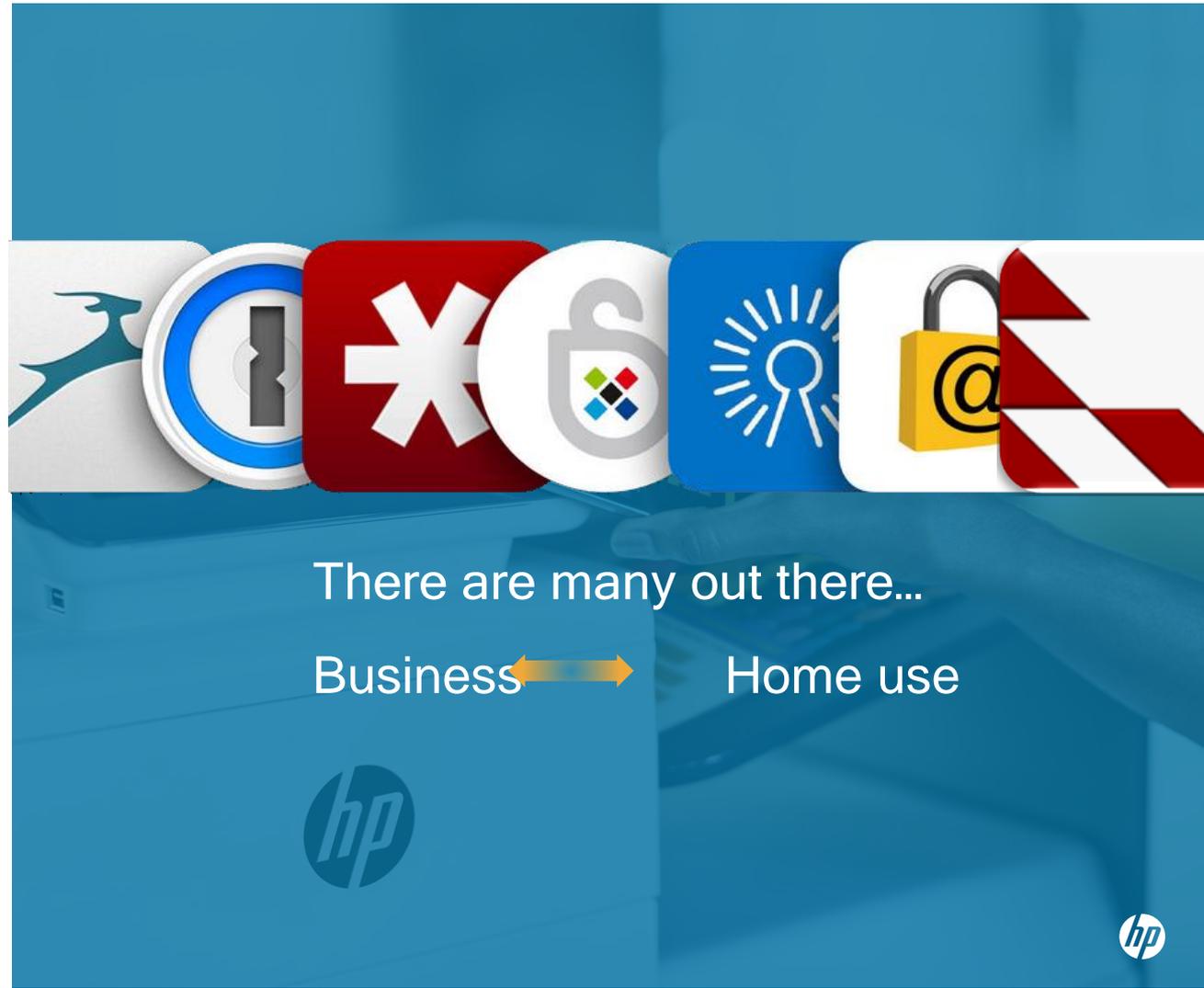
Disable what you don't need



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

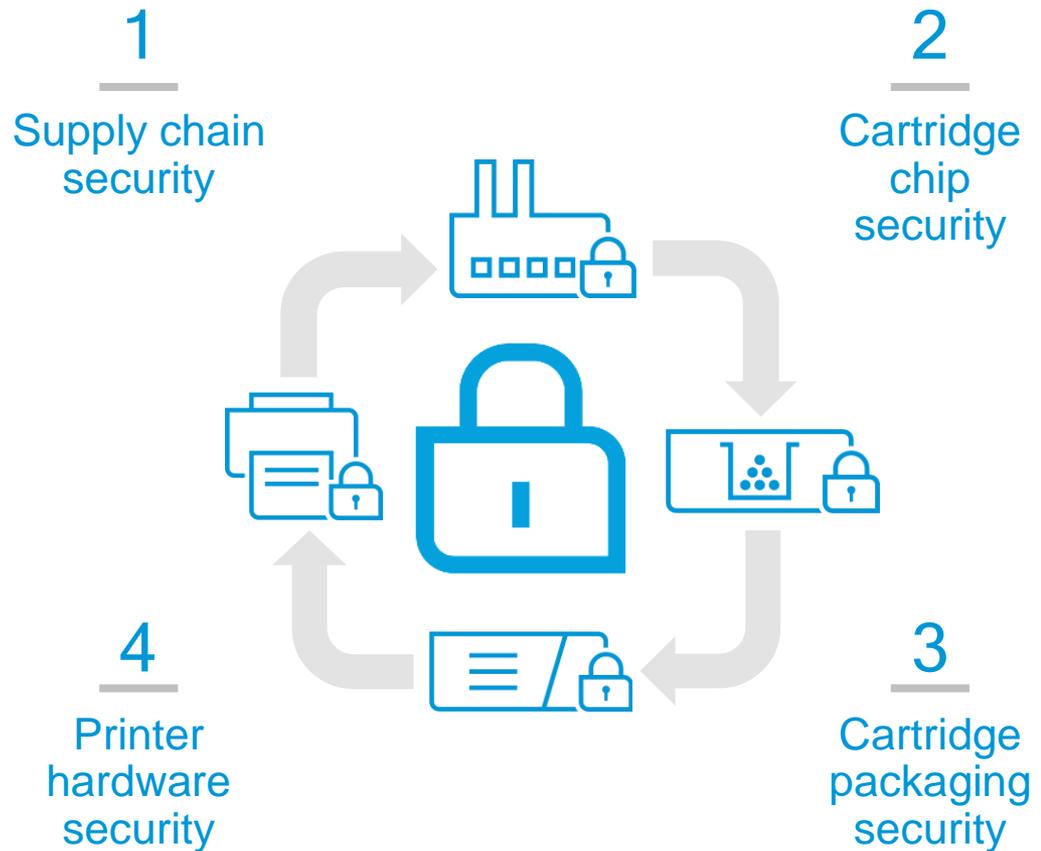


Encrypt if
possible

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.



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



Think twice: if an offer sounds too good to be true, it probably is



Use credit cards when shopping online for stronger customer protection



Check your bank account often for suspicious activity

CYBER SAFETY WITH CHILDREN



STAY ALERT
AND DON'T...



REMEMBER:
YOU ARE
A CRUCIAL
PART OF
THE SYSTEM



Source: www.jklossner.com



THANK
YOU



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

May 5, 2021

Proposed Agenda

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

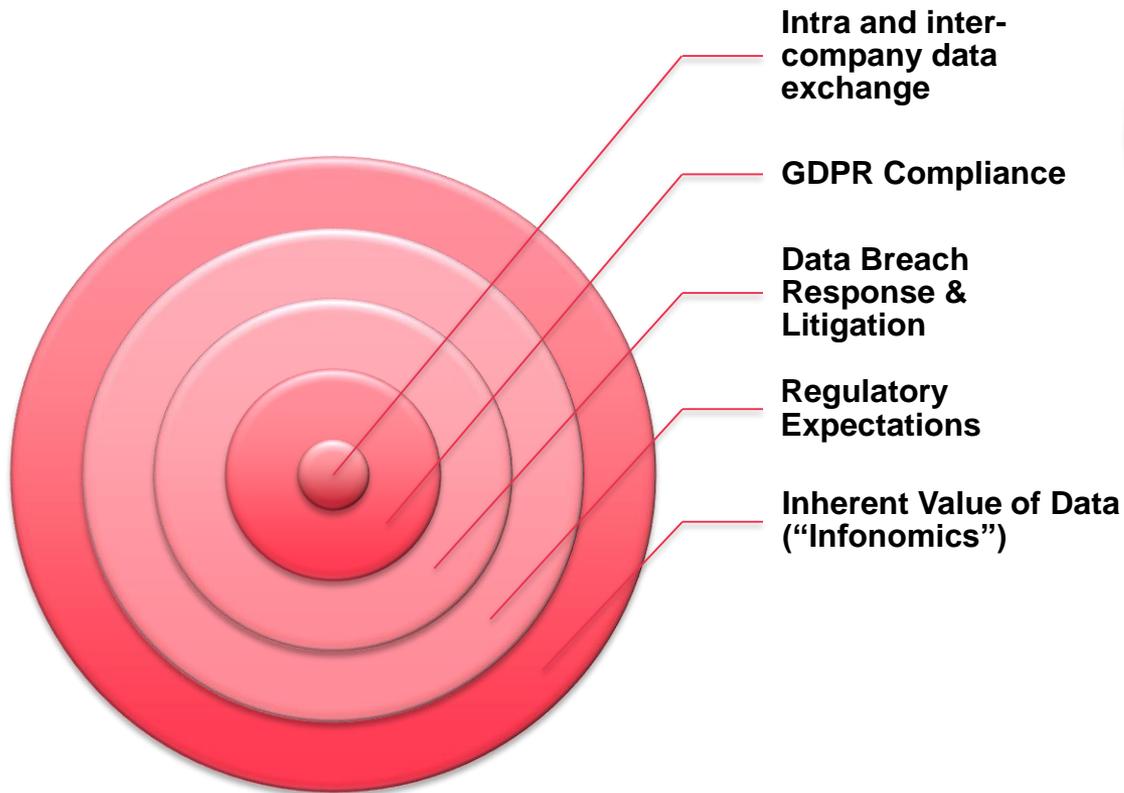
1 Introduction

When You Need Help

Addressing Data Privacy Challenges and Opportunities

Data privacy issues require more management and innovation.

What are your clients' priorities?



"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

2 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

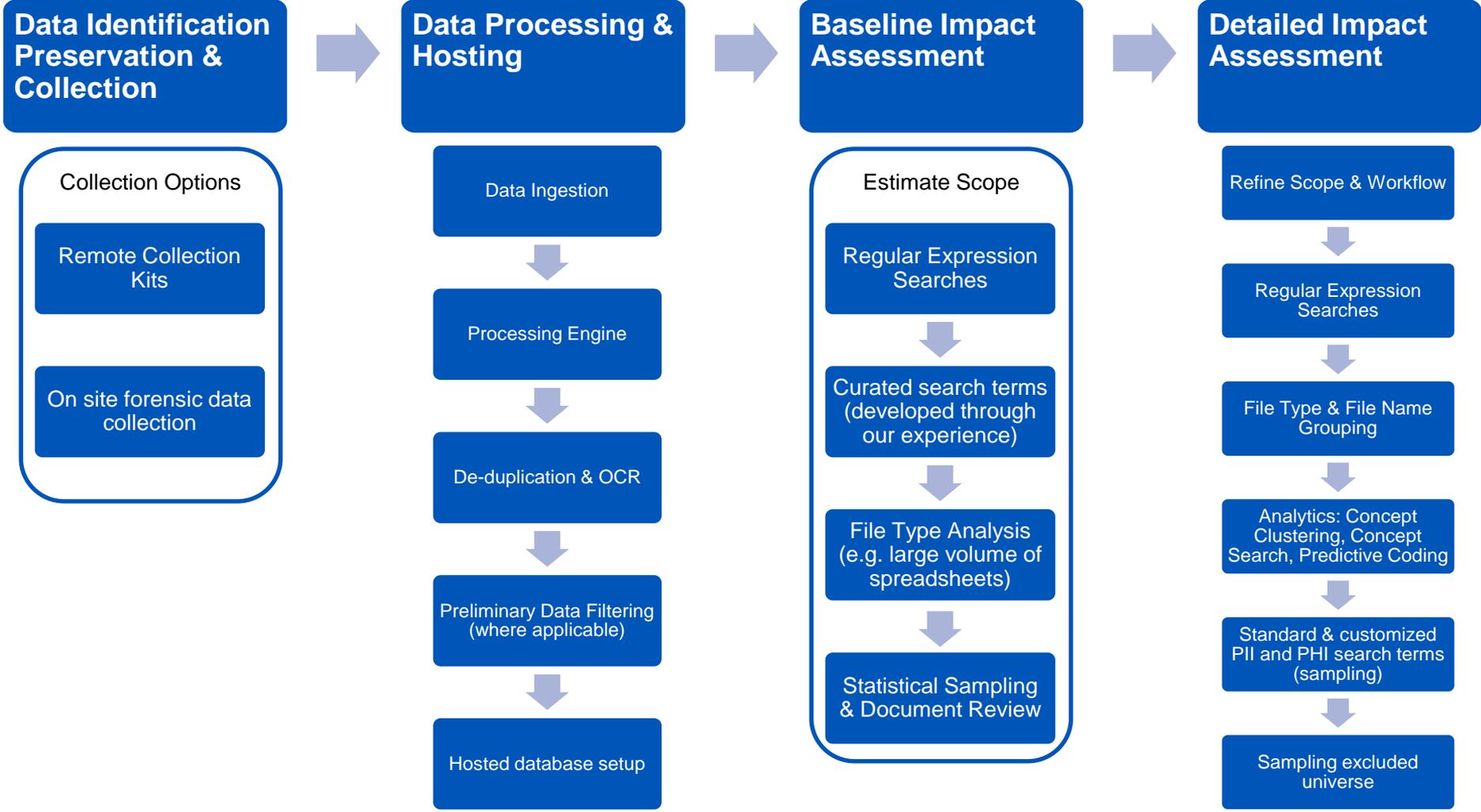
- Initial analysis to estimate scope of documents containing potentially impacted individuals
- Establish initial estimates regarding number of impacted individuals



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



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**



RegEx for detecting Visa credit card numbers

```
\b(4\d{3}[-\w]\d{4}[-\w]\d{4}[-\w]\d{4})\b
```

Sample Reports: Patterns Identified

Record level analysis and reporting

	A	B	C
1	Pattern Name	Documents Hit	Total Hits
2	Credit Cards	6	10066
3	Email Addresses	182	603
4	Gender	2	3
5	IP Addresses	1	1
6	Phone Numbers	117	338
7	Social Security Numbers	8	123

Automatic, real-time reporting with document and hit frequency per pattern aids high level risk assessment

TMB Test Data Extrac...	Redaction Jobs
8355;766-20-3191	
003-09-2398;007-46-5581;009-38-4601;111-22-3333;150-66-8842;205-34-0054;219-78-4469;223-37-8011;236-46-9509;237-01-3979;403-66-5530;422-27-5056;425-	153

Record-level pattern extraction enables easy content level analysis

RelativityID	Redaction Jobs	Pages	Number of Auto Reda...	Needs Review	Needs Review Reason
ENRON00243607	134		2	7 No	
ENRON00245091	134		1	1 No	
ENRON00245096	134		1	1 No	
ENRON00246771	134			32 Yes	Text/OCR Inconsistent
ENRON00248365	134			1 No	
ENRON00248366	134			3 No	
ENRON00249161	134			1 No	
ENRON00249162	134			7 No	
ENRON00249641	134		1	4 No	
ENRON00256776	134		1	11 No	

Number of patterns identified per document facilitates easy estimates

Automated quality control highlights outliers

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

▼ Count of Extension by STR - All Docs

Items 1 - 25 (of 88) in sets of 25 per page

STR - All Docs	csv	doc	docm	docx	msg	pdf	txt	xls	xlsm	xlsx
"SSN" OR "S.S.N." OR ("Social Security" OR "SS" OR "S.S.") w/3 ("no." OR number*)	0	59	9	13	37	835	2	4	0	0
(driver* w/3 (lic* OR "no." OR number*)) OR(gov* w/3 (id OR "no." OR number*))	4	46	5	20	94	608	0	1	5	19
policy w/2 period	0	43	6	1	2	682	0	0	0	0
policy w/2 number	0	13	6	4	2	701	0	0	1	6
"policy period"	0	43	6	1	2	680	0	0	0	0
Social Security number	0	30	1	5	21	611	0	1	0	0
"Named Insured"	0	18	0	1	0	572	0	0	4	1
"DOB" OR "D.O.B." OR (date w/3 birth)	0	21	9	14	50	399	0	1	4	13
liability w/2 insurance	0	30	6	3	0	421	0	0	0	3
Date w/3 Coverage	0	20	0	0	3	386	0	0	0	1
"Liability insurance"	0	26	0	3	0	361	0	0	0	3
Date of birth	0	7	6							
((transit OR bank* OR check* OR sav*) w/3 acc*) w/10 ("no." OR number*)	0	18	0							
discharge	0	15	0							
Fax and order	4	8	6							
insured* w/2 policy	0	8	0							

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



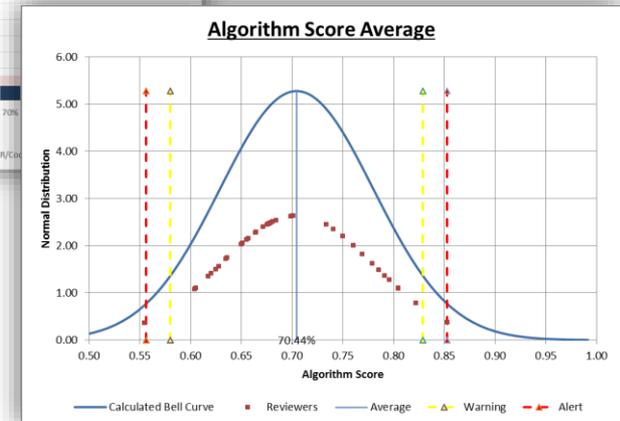
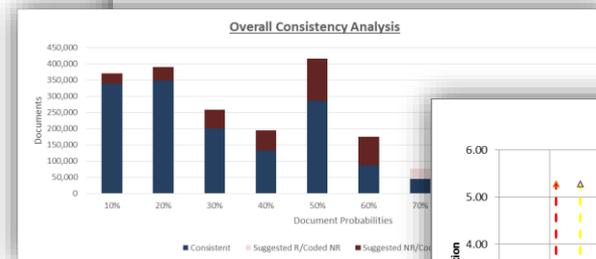
Predictive Coding – Leverage human expertise to automatically classify millions of documents in a matter of hours. Predictive Coding supports entirely custom workflows and methodologies, and is capable of continuous prioritization of important documents for review.



Workflow – Automate the routing and distribution of documents to streamline document review and maximize accuracy and defensibility. Workflow eliminates the need to maintain static batch sets and manually transition documents to different review teams. Workflow works hand-in-hand with Predictive Coding to provide the most efficient review possible.



Near-duplicates – Identify and group similar records, and highlight the subtle differences for a quicker review.



Quantifying Initial Results

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

Estimated Portion of Mailboxes Containing Data with Potentially Impacted Data						
Department	% of total	Documents	Documents with Impacted Data	Customer Records per Document	Gross Estimate of Number of Potentially Impacted Individuals	Estimated Number of Unique Potentially Impacted Individuals (Assuming 50% Duplicates)
Department 1	83.46%	289,745	241,821	12	2,901,854	1,450,927
Department 2	7.81%	1,506,528	117,660	5	588,299	294,150
Department 3	5.19%	112,549	5,841	4	23,365	11,683
Department 4	1.43%	256,527	3,668	5	18,342	9,171
Department 5	1.20%	108,970	1,308	11	14,384	7,192
Custodian Mailbox	% of total	Documents	Documents with Impacted Data	Customer Records per Document	Estimated Number of Potentially Impacted Individuals	Estimated Number of Unique Potentially Impacted Individuals (Assuming 50% Duplicates)
David	24.90%	96,582	24,049	29	697,416	348,708
Maria	16.58%	502,176	83,261	30	2,497,823	1,248,912
Donna	14.15%	37,516	5,309	4	21,234	10,617
Lisa	6.24%	85,509	5,336	4	21,343	10,672
Joan	4.92%	36,323	1,787	7	12,510	6,255

Standard Data Capture Form

Unique Information about Individuals is Input Once

Individual names or businesses are entered in to a centralized reusable database object as identified

Named Individual

Profile Type: Business Individual Manage

Business Name:

Named Individual (Last, First):

Middle Name:

Suffix: Manage

Legal Surname Prior to Marriage:

Address Information ▼

Street:

Street II:

City:

State: Manage

Zip Code:

Foreign Country:

2nd Address?:

Other Information

Minor?:

Date of Birth: ...

Deceased?:

SSN:

Standard Data Capture Forms

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

Personally Identifiable Information ▾

PII Identification Type:	<input type="checkbox"/> Driver's License Number	Financial Information:	<input type="checkbox"/> Bank Account Number
	<input type="checkbox"/> State ID Card Number		<input type="checkbox"/> International Bank Account Number
	<input type="checkbox"/> Social Security Number		<input type="checkbox"/> Credit or Debit Card Number
	<input type="checkbox"/> Individual Taxpayer Identification Number		<input type="checkbox"/> Other Financial Account Information
	<input type="checkbox"/> EU Social Security Number or Equivalent ID		<input type="checkbox"/> Access Code
	<input type="checkbox"/> EU National Identification Number		<input type="checkbox"/> Account Password
	<input type="checkbox"/> Passport Number		<input type="checkbox"/> Personal Identification Number
	<input type="checkbox"/> Tribal Identification Card Number		<input type="checkbox"/> Security Code
	<input type="checkbox"/> Other Identification Number		Manage
	Manage	Other Account Information:	<input type="checkbox"/> Email Address w/ Password
EU Personal Sensitive Information:	<input type="checkbox"/> Salary		<input type="checkbox"/> Unique Electronic Identifier w/ Password
	<input type="checkbox"/> Commissions		<input type="checkbox"/> Username w/ Password
	<input type="checkbox"/> Personal Phone		Manage
	<input type="checkbox"/> Personal Address		
	<input type="checkbox"/> Personal Email Address		
	<input type="checkbox"/> Racial/Ethnic Origin		
	<input type="checkbox"/> Political Opinions		
	<input type="checkbox"/> Religious Beliefs		
	<input type="checkbox"/> Trade Union Membership Status		
	<input type="checkbox"/> Physical or Mental Condition		
	<input type="checkbox"/> Sexual Life Information		
	<input type="checkbox"/> Offence Information		
	<input type="checkbox"/> Court Proceeding Information		
	<input type="checkbox"/> Other Employee Data		
	Manage		
Security Information:	<input type="checkbox"/> Biometric Data	Health Information:	<input type="checkbox"/> Medical Information
	<input type="checkbox"/> Electronic/Digital Signature		<input type="checkbox"/> Health Insurance Information
	<input type="checkbox"/> Identity Protection PIN (IRS)		<input type="checkbox"/> UK National Health Service Number
	<input type="checkbox"/> Mother's Maiden Name		<input type="checkbox"/> UK National Insurance Number (NINO)
	<input type="checkbox"/> Date of Birth		<input type="checkbox"/> Health Status Information
	Manage		<input type="checkbox"/> Other Health Information
			Manage

✓ 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.

Representative Sample of Results

Potentially Reportable Individuals, PII and PHI Features are Compiled

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

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

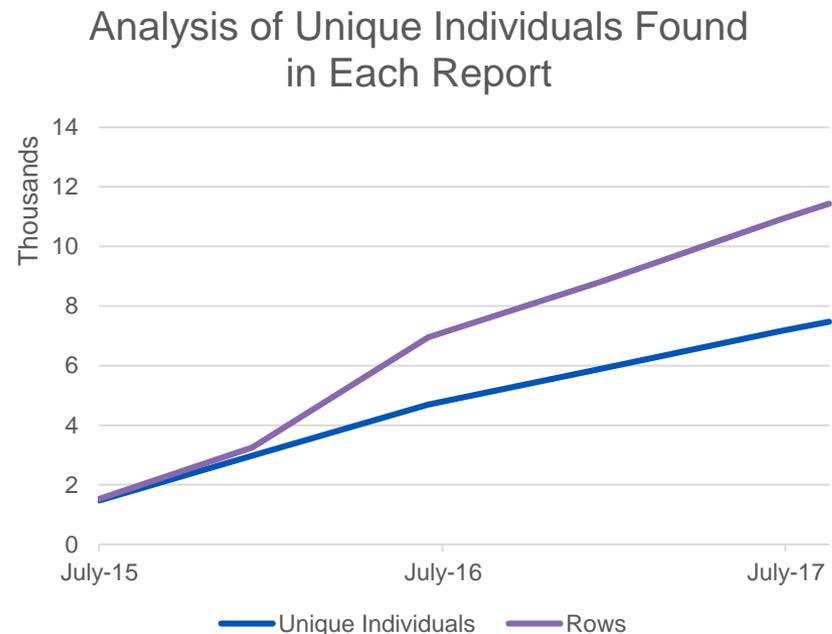
Personal data buried in unstructured data like email, file systems, and collaboration platforms is pervasive and can pose a tedious challenge

Representative Metrics from Recent Projects			
	Compromised Documents	Documents with suspect PII or PHI	Impacted Individuals
1	616,293	187,733	~ 25,000
2	284,405	155,452	~ 4,500
3	82,459	41,815	41
4	60,595	25,211	1,298
5	16,320	4,057	322

How Many Reportable Individuals Might be Impacted?

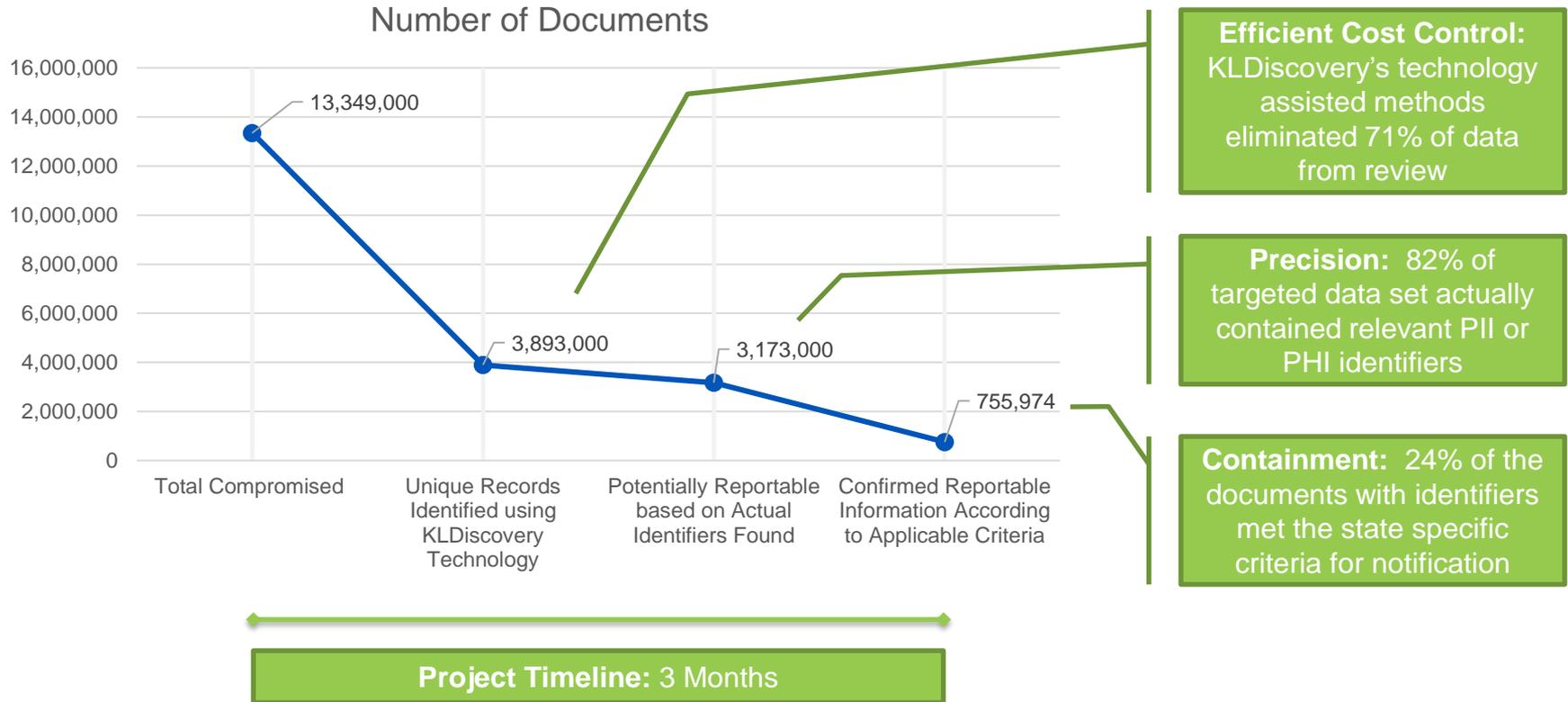
We find client data tends to contain many reports with duplicative and overlapping customer information

- 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



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.

KLDiscovery 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: KLDiscovery 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, KLDiscovery's work enabled counsel to enhance compliance training.

5 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 al ³
- 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 breached ⁵
- 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's ⁶
- But punitive damages in other courts aren't easily accepted
 - In Re: Yahoo! Inc. Customer Data Security Breach Litigation ⁷



Aranowitz et al. v. Hackensack Meridian Health Inc., (No. 2:20-cv-01409, N.J.)

- 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

Does the risk of harm alone support a lawsuit?

No

Peters v. St. Joseph Services Corp., S.D. TX.

Dyson v. Sky Chefs Inc., N.D. TX.

U.S. Court of Appeals for the Third Circuit

Yes

Perrill v. Equifax, W.D. TX.

U.S. Court of Appeals for the Seventh Circuit

U.S. Court of Appeals for Ninth Circuit

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 2021⁸
 - Responding to breaches is laborious, leading to an average cost of \$141 per lost or stolen record or \$3.6 million per incident.⁹
- 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 2021¹⁰
- Technology is still on the chase
 - Employment talent gap signals unsolved innovation
 - Talent, technology and innovation will need to come together

6 Conclusions

What should we do next?

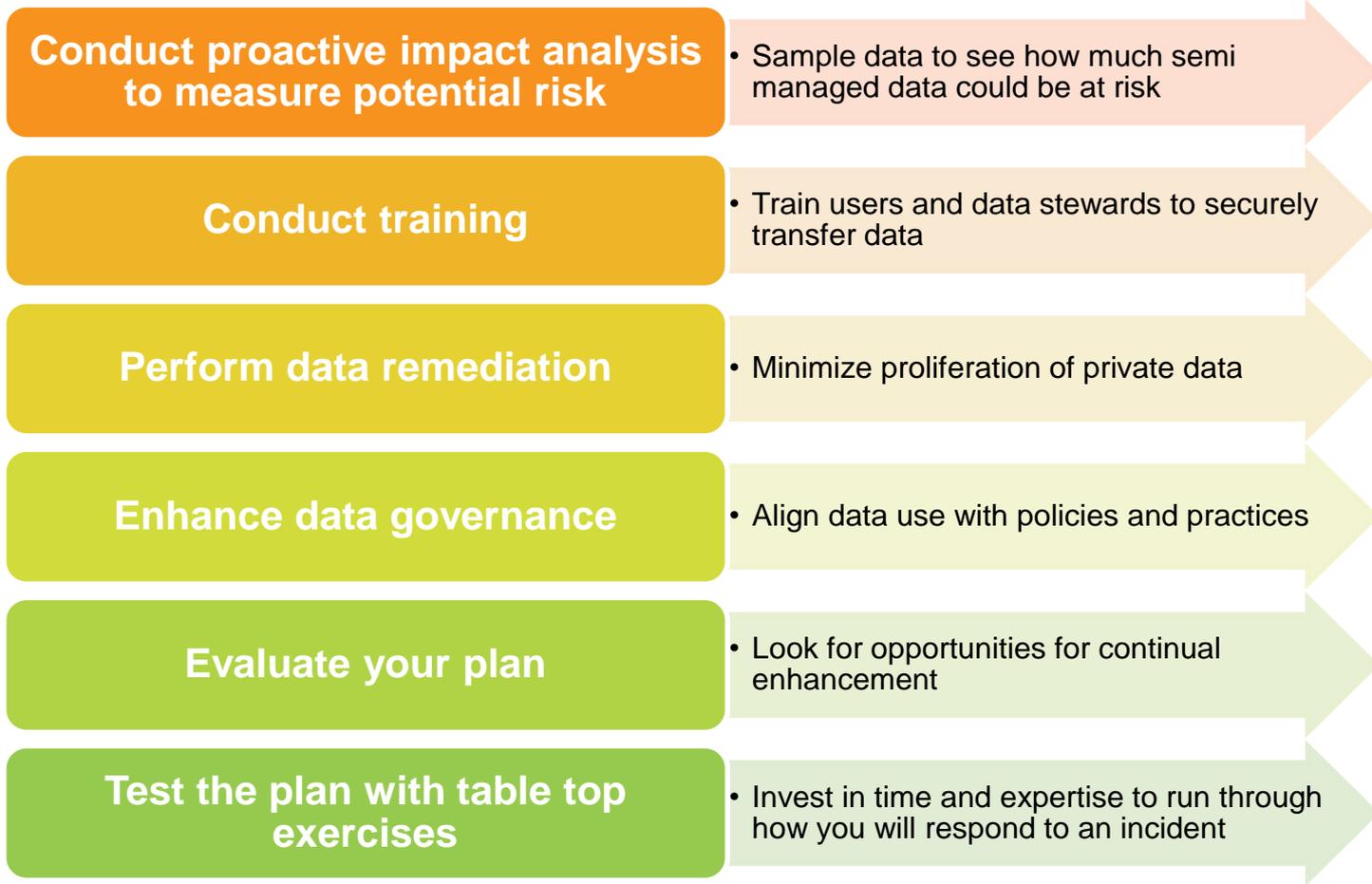
What's Next?

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



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)?

Q&A What Questions Do You Have?



Thank You..



We will be hosting a series of webinar events throughout 2021

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

Aubrey L. Owens, Jr.

Senior Manager

Business Development

Aubrey.Owens@kldiscovery.com

+1 (804) 601-3301

Renee Covington

Vice President

Business Development

Renee.Covington@kldiscovery.com

+1 (804) 836-5477

Eric Robinson, JD/PMP

Senior Consultant

Advisory Services and Client Solutions

Eric.Robinson@kldiscovery.com

+1 (804) 615-0278

Endnotes

1. <http://www.businessinsurance.com/article/20180309/NEWS06/912319751/Federal-appeals-court-9th-circuit-reinstates-Zapposcom-data-breach-litigation-i>
2. <https://www.law360.com/articles/1002326/high-court-must-weigh-in-on-breach-standing-carefirst-says>
3. <https://www.law360.com/articles/1003963/ny-judge-reverses-standing-ax-in-excellus-breach-row>
4. <https://www.law360.com/articles/1025880/abm-hit-with-class-action-over-employee-data-breach>
5. <https://www.law360.com/cybersecurity-privacy/articles/1027914/states-foray-into-breach-suits-will-spur-change-attys-say>
6. https://www.law360.com/cybersecurity-privacy/articles/1034762/7th-circ-opens-up-path-for-cos-to-ditch-data-breach-suits?nl_pk=7725c61b-43e4-49b8-b5d7-8d237cd27a36&utm_source=newsletter&utm_medium=email&utm_campaign=cybersecurity-privacy
7. <https://www.law360.com/articles/1020903/yahoo-email-users-see-their-data-breach-claims-trimmed>
8. <https://www.statista.com/statistics/595182/worldwide-security-as-a-service-market-size>
9. <https://securityintelligence.com/know-the-odds-the-cost-of-a-data-breach-in-2017>
10. <https://www.csoonline.com/article/3200024/security/cybersecurity-labor-crunch-to-hit-35-million-unfilled-jobs-by-2021.html>
11. *Resources and commentary about the economic value of data:*
 - a. <https://www.weforum.org/agenda/2017/09/the-value-of-data/>
 - b. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/731349/20180730_HMT_Discussion_Paper_-_The_Economic_Value_of_Data.pdf
 - c. <https://www.gartner.com/en/publications/infonomics>



UPCOMING EVENTS

2021 Virtual Commonwealth of Virginia Information Security Conference

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).

Conference website: <https://www.vita.virginia.gov/information-security/security-conference/>

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.

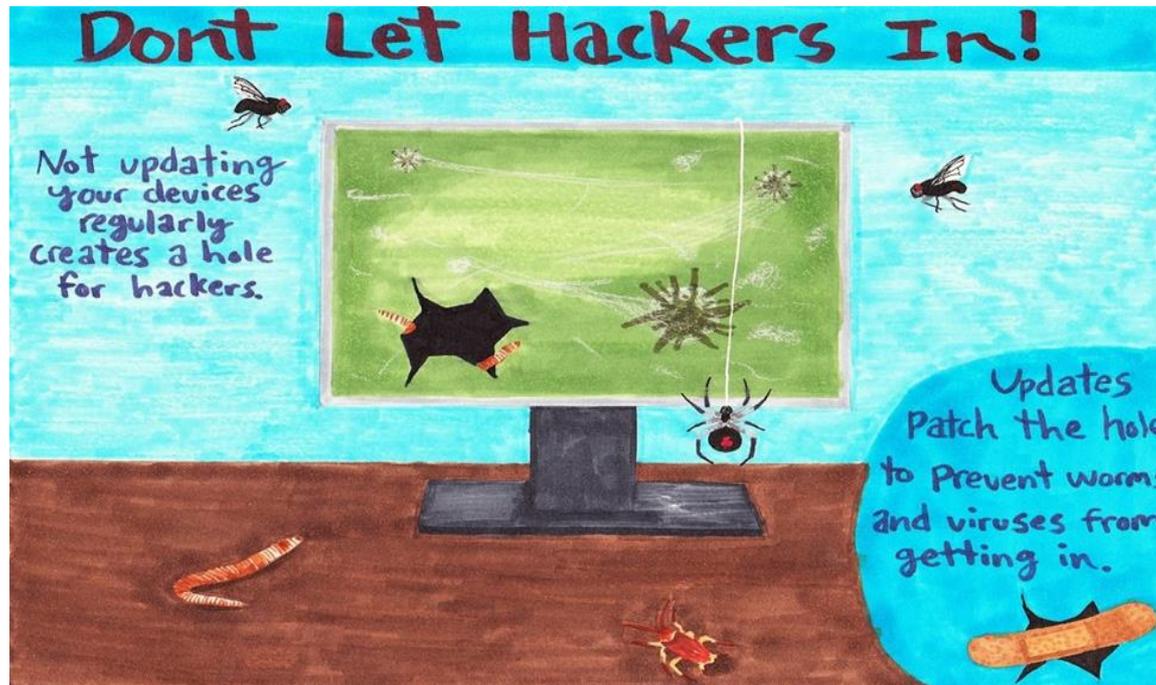
If you do not have access to Archer, you may submit your completed form to Commonwealthsecurity@vita.virginia.gov.

The form is located at the link below:

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

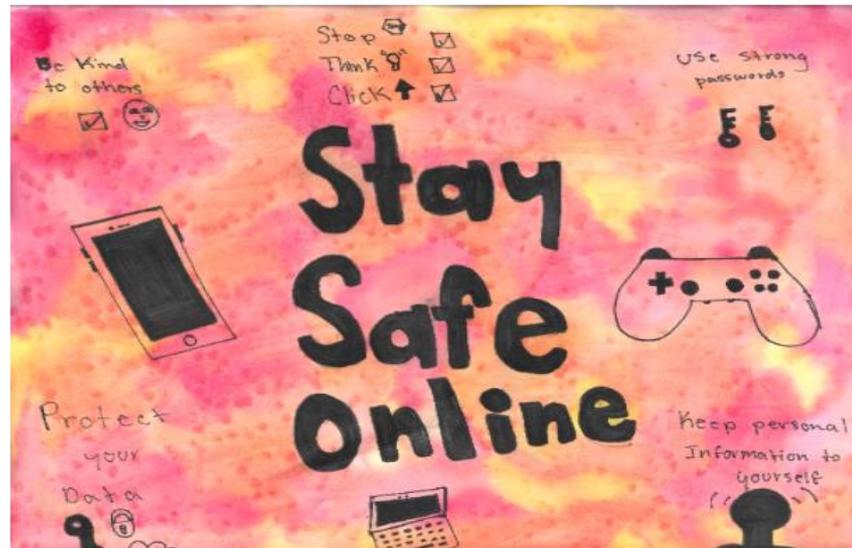
If you questions about completing the form, contact:
Tina.gaines@vita.virginia.gov

2021 National Security Poster Contest Winner!



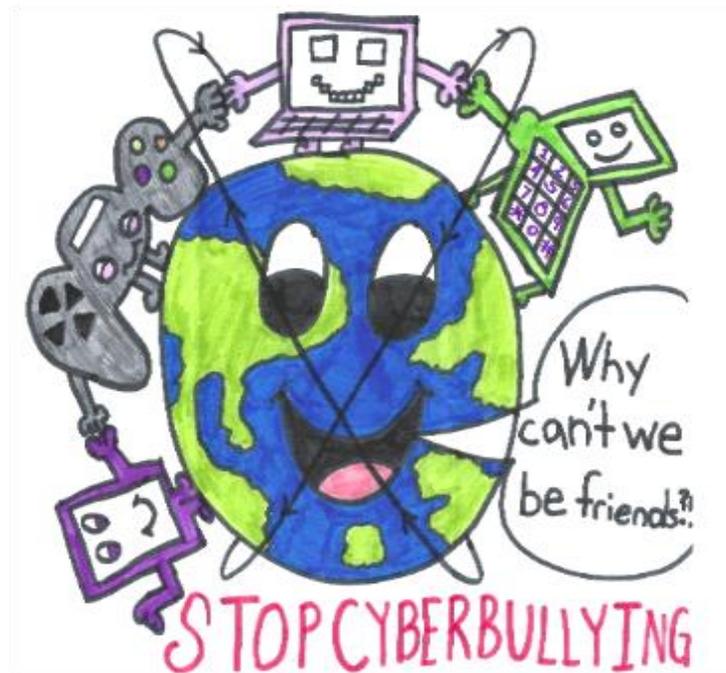
Melia – Spotsylvania High School

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 Encinias, Dell

Mark Martens & Jon Smith, VITA



**THANK YOU FOR
ATTENDING!**

