Data Breach Response and Notification

Presenters

Craig Brown

CEO, Bridgeline Solutions

cbrown@bridgelinesolutions.com

Ryan Bilbrey

Managing Director, Exiger

rbilbrey@exiger.com

VIGITRUST

What is a Data Breach?

- The unauthorized access, use, or retrieval of data by an individual, group, application, or service
- May be internal or external party
- Can involve theft and illicit use
- Can also be the *unintentional* exposure of data

Data breaches can NEGATIVELY impact businesses and consumers in many ways—costing them money, reputational damage, and time

VIGITRUST

Data Privacy

- Companies are often required to disclose data breaches to individuals whose private information was compromised, as well as various government agencies
- Reporting for—
  - ✓ PII – Personally Identifiable Information
  - ✓ PHI – Protected Health Information (HIPAA)
  - ✓ FERPA – Family Educational Rights and Privacy Act
  - ✓ PCI – Payment Card Industry
  - ✓ GDPR – General Data Protection Regulation (EU)
- Combination of state and federal laws create a confusing regulatory environment

Data Breach Response

- The data breach notification process faces increasingly rapid turnaround times, which places a premium on the quick, efficient, and cost-effective analysis of relevant data
- Most data breach response discussion revolves around—
  - ✓ Proactive planning and protection from cyber intrusions
  - ✓ Post-breach investigation and remediation of systems
  - ✓ Notifying affected individuals
- Very little information available regarding how a company gets from the investigation to the notification

The Challenge

- ❑ Address the huge amounts of email and loose files that are often exposed in a breach
- ❑ Quantify issue for law enforcement reporting
- ❑ Generate notification lists for the affected individuals

The scope of such efforts can be far greater than company or counsel anticipate, as the exposure of just 25 email boxes can yield over one million documents

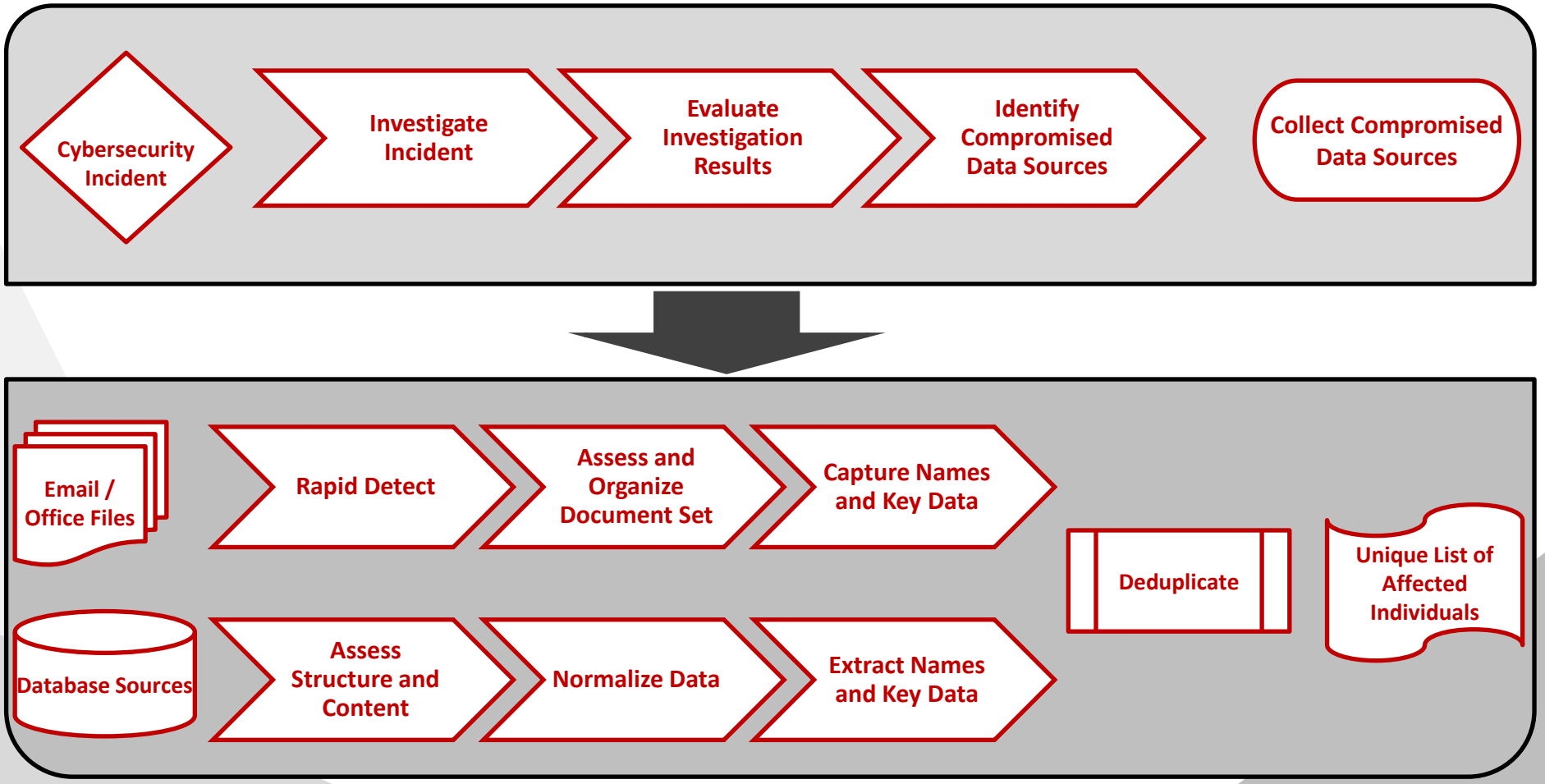
VIGITRUST

The Solution

- Quick, efficient, and cost-effective review of the huge amounts of email and loose files that are often exposed in a breach
- The key to success? Combine—
  - ✓ eDiscovery principles
  - ✓ Advanced text analytics
  - ✓ Streamlined workflows
  - ✓ Database analysis
  - ✓ Detailed understanding of privacy issues
- Critical success factor – company, counsel, and consultants working together as a TEAM

VIGITRUST

Detailed Workflow Example



VIGITRUST

Conclusions

- A workflow integrating people, processes, and technology can dramatically accelerating the Data Breach Response life cycle and provide an advantage over traditional methodologies.
- An analytics-driven approach, subject matter expertise, and availability of review resources can reduce Data Breach Response costs and timelines while materially improving the quality of results.