WHY DATA BREACH IS A SIGNIFICANT PART OF GDPR

Kim Brushaber, IDERA, Senior Product Manager

DATA BREACH BY THE NUMBERS

Over 5 million data records are lost or stolen every day

http://breachlevelindex.com/

Two Billion Files containing personal data of US Citizens were leaked in US Data Breaches in 2017

https://www.infosecurity-magazine.com/news/two-billion-files-leaked-in-us-data/

IDERA®

The median number of days that attackers stay dormant within a network before detection is 200 days

https://swimlane.com/10-hard-hitting-cyber-security-statistics/

IDERA®

DATA BREACHES IN 2017 ALONE

- Healthcare (60% of all leaks)
  - 328 breaches
  - $1.2 Billion
- Technology
  - 48 breaches
  - $1.2 Billion
  - 1.8 Billion records
- Finance
  - 40 breaches,
  - $144.8 Million
  - 146 Million records
- Retail
  - 40 breaches
  - $144K
  - 4.7 Million records

https://www.infosecurity-magazine.com/news/two-billion-files-leaked-in-us-data/

SMALL BUSINESS DATA BREACH NUMBERS

- 90% of data breaches impact small businesses
  - 60% of breaches target them directly
- 90% of small businesses don't use any data protection at all
- Attacks cost between $84K and $148K
- 31% of customers terminated their business after being notified of a breach
- 60% of small businesses close doors permanently within 6 months of experiencing a data breach

https://analyticsweek.com/content/whats-the-true-cost-of-a-data-breach/ | https://www.firstdata.com/downloads/thought-leadership/Small_Businesses_Cost_of_a_Data_Breach_Article.pdf | https://www.usatoday.com/story/money/columnist/strauss/2017/10/20/cyber-threat-huge-small-businesses/782716001/

INDIVIDUAL CONCERNS IN DATA SECURITY

- By 2020 over **30 Billion** devices will be connected to the internet

- **49%** of Americans feel that their personal information is less secure than it was five years ago
- Over **73%** of consumers in America want companies to be transparent about personal data
- **78%** of people claim to be aware of the risks of unknown links in emails, yet click on those links anyway
- **86%** of internet users are actively trying to minimize, anonymize and hide the visibility of their digital footprints

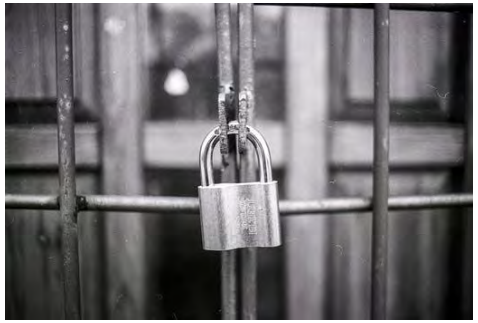
Facts pulled from: Data Privacy Day | National Cyber Security Alliance and Zogby Consumer Poll | Pew Research Center | https://blog.barkly.com/cyber-security-statistics-2017

DATA SECURITY PREPAREDNESS

- In 2014 **70% of Millennials** admitted to bringing outside applications into the enterprise in violation of IT policies
- **52%** of organizations that suffered successful cyber attacks in 2016 aren't making any changes to their security in 2017
- Only **38%** of global organizations claim they are prepared to handle a sophisticated cyberattack
- Only **37%** of organizations have a cyber incident response plan

Facts pulled from: https://blog.barkly.com/cyber-security-statistics-2017 | https://swimlane.com/10-hard-hitting-cyber-security-statistics/ | PWC Economic Crime Survey | https://www.wired.com/insights/2014/09/millennials-mobile-security/

DATA SECURITY EXECUTIVE PERSPECTIVE



- **90% of CIOs** admit to wasting millions on inadequate cybersecurity
- **90% of CIOs** have already been attacked or expect to be attacked by bad guys hiding in their encryption
- **87% of CIOs** believe their security controls are failing to protect their businesses
- **85% of CIOs** expect criminal misuse of keys and certificates to get worse

https://www.venafi.com/assets/pdf/wp/Venafi_2016CIO_SurveyReport.pdf

THE TRUE COST OF DATA BREACH

“

The average cost of a single data breach in 2020 will exceed $150 million, as more business infrastructure gets connected

https://www.juniperresearch.com/press/press-releases/cybercrime-cost-businesses-over-2trillion

IDERA®

WHAT ARE THE ODDS?

- 1 in 960,000 – odds of being struck by lightning
- 1 in 220 – odds of dating a millionaire
- 1 in 4 – odds of experiencing a data breach

https://securityintelligence.com/know-the-odds-the-cost-of-a-data-breach-in-2017/

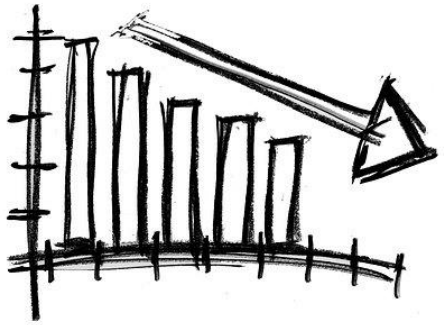
2017 COST PER DATA BREACH

- The average cost for each lost or stolen record containing sensitive and confidential information was **$141** (a 10% decrease from the year before)
- The average size of a data breach was **24,000** records (an increase of 1.8% from the year before)

- $141 x 24,000 ~ **$3.4M**

https://www.ibm.com/security/data-breach

DRIVING DOWN THE COST



For the $141 per record breached, you can reduce your cost by:

- $19.30 – create an incident response team
  - Saves money by containing the event quickly
- $16.10 – extensive use of encryption
  - Saves money by restricting access to the information
- $12.50 – employee training
  - An educated workforce helps plan for potential threats before they happen

OTHER COSTS OF DATA BREACHES

- Forensic analysis to determine the extent of the breach
  - $200 to $2000 an hour for specialists to review the data
- Written notification to affected customers
  - $5 to $50 for each customer
- Credit monitoring for affected customers
  - $10 to $30 for each customer
- Legal defense costs
  - Between $500K and $1M are typical
- Regulatory fines and judgments
  - Target paid $18.5M after a 2013 breach affecting 41M customers
- Reputational losses
  - 20% of regular customers allowing for 30% of revenue

https://analyticsweek.com/content/whats-the-true-cost-of-a-data-breach/

SHOCKING, RIGHT??

WHAT GDPR SAYS ABOUT DATA BREACH

WHAT DATA MUST BE PROTECTED (BY GDPR)

Any information that can be classified as personal details – or that can be used to determine your identity

- Name
- Identification number
- Email address
- Online user identifier
- Social media posts
- Physical, physiological or genetic information
- Medical information
- Location
- Bank details
- IP address
- Cookies

ARTICLE 33 – NOTIFICATION OF PERSONAL DATA BREACH TO THE SUPERVISORY AUTHORITY

- Detect breaches
- Assess the impact on personal data records
- Assess whether the personal data is identifiable
- Describe the nature of the breach
- Describe your measures to remedy it
- Alert Supervising Authority within 72 hours of the breach

ARTICLE 15 – CONTROL EXPOSURE TO PERSONAL DATA

- Control accessibility - who is accessing data and how
- Minimize data being processed in terms of:
  - Amount of data collected
  - Extent of data processed
  - Storage period
  - Accessibility
- Produce safeguards for control management

ARTICLE 32 – SECURITY OF PROCESSING

Security mechanisms to protect personal data

- Employ pseudonymization and encryption
- Ensure ongoing confidentiality, integrity, availability and resilience of processing systems and services
- Restore availability and access in the event of an incident
- Provide a process for regularly testing and assessing effectiveness of security measures

GDPR PENALTIES/SANCTIONS (ARTICLE 83)

Depending on the nature of the infraction:

- A warning in writing in cases of first and non-intentional non-compliance
- Regular periodic data protection audits
- A fine of up to **10M Euro** or **2%** of annual worldwide turnover from the previous year
- A fine of up to **20M Euro** or **4%** of annual worldwide turnover from the previous year

DON’T PANIC!!

HOW TO SET UP YOUR DATA BREACH PROCESSES

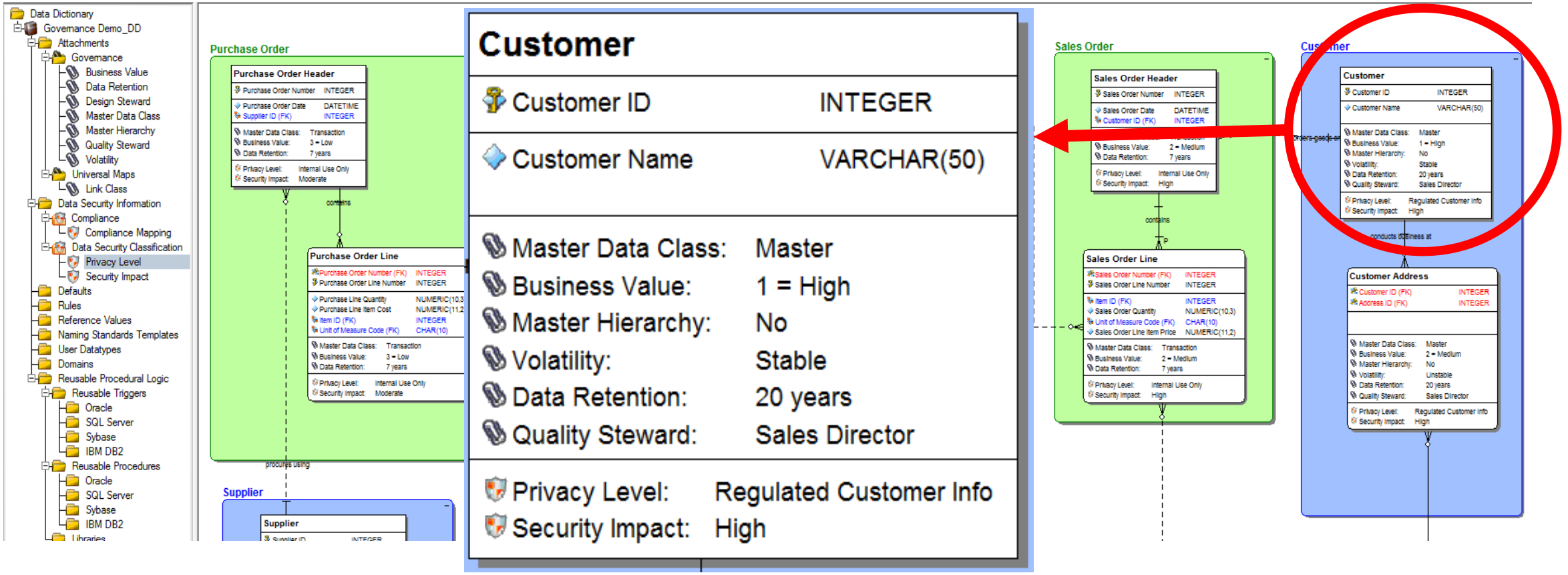
BREACH DETECTION RESPONSE PLANNING

- Plan for the attack (it is coming)
  - Know what your response will be and train all applicable employees on it
- Detect access quickly
  - Enable tools that will allow you to be able to detect the breach and know what information was access
- Create a detection response team
  - Internal or retained, create a team that can act immediately
- Establish a communications plan
  - Knowing exactly what you will say allows you to spread the word quickly and lessen the confusion

SAFEGUARDING PERSONAL DATA

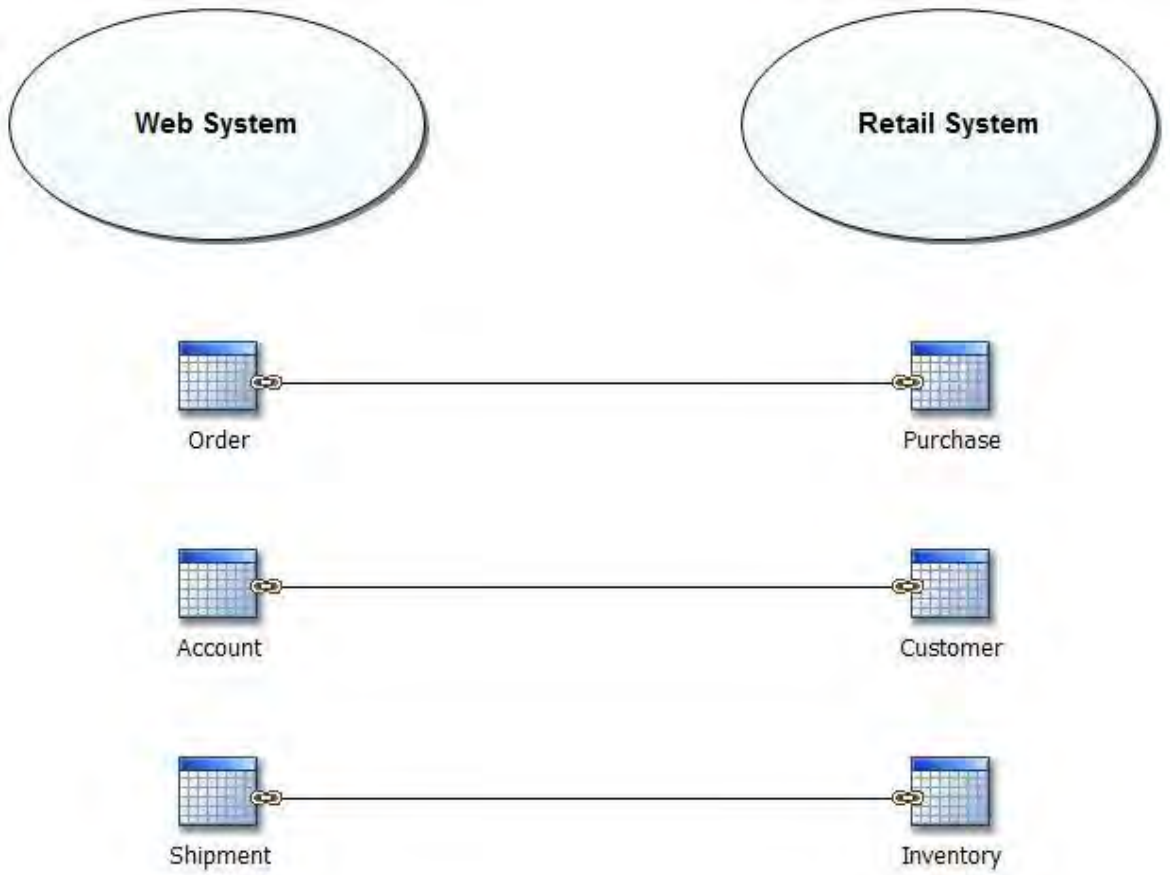
- Identify which data is Personally Identifiable Data
- Map the data in existing systems to reduce redundancy
- Keep only the data that you absolutely need
- Determine when the data should be made available
- Restrict access to only those who should have access
- Minimize the places where data is stored
- Set data encryption levels while:
  - In Use
  - In Transit
  - At Rest

IDENTIFYING DATA SECURITY PROPERTIES IN DATA MODELS



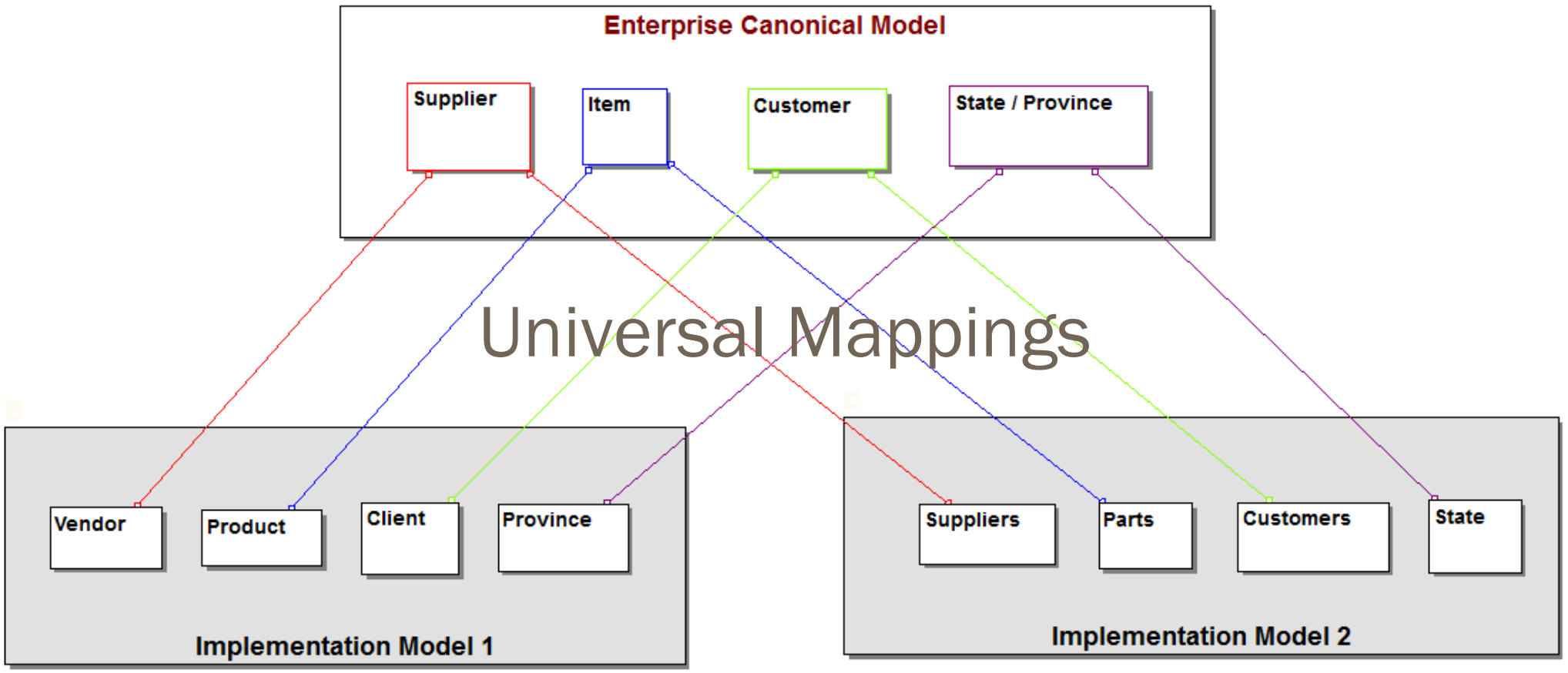
* Data Models created using IDERA's ER/Studio Data Architect

DATA MAPPING EXAMPLE



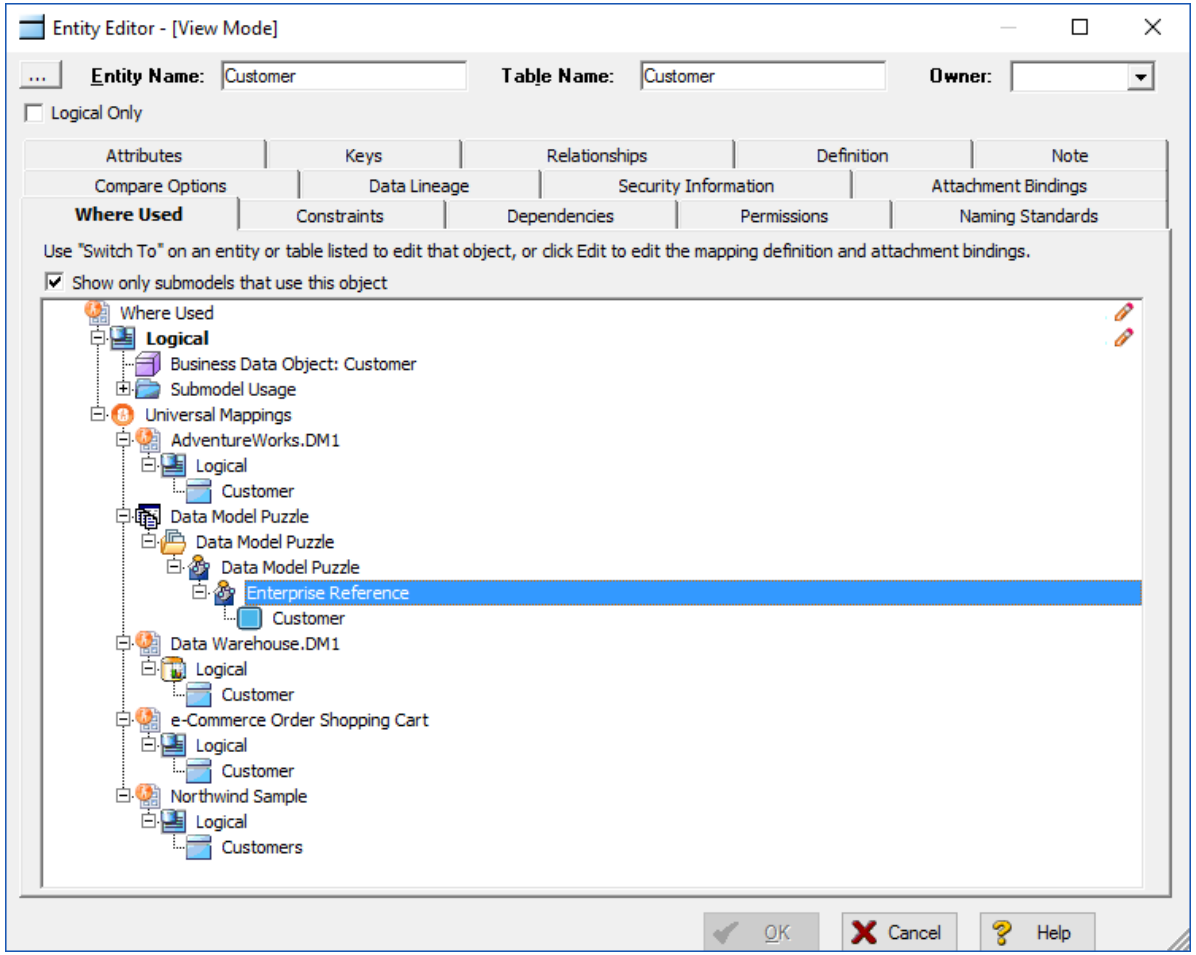
* Business Process Models created using IDERA's ER/Studio Business Architect

SET UP UNIVERSAL MAPPINGS



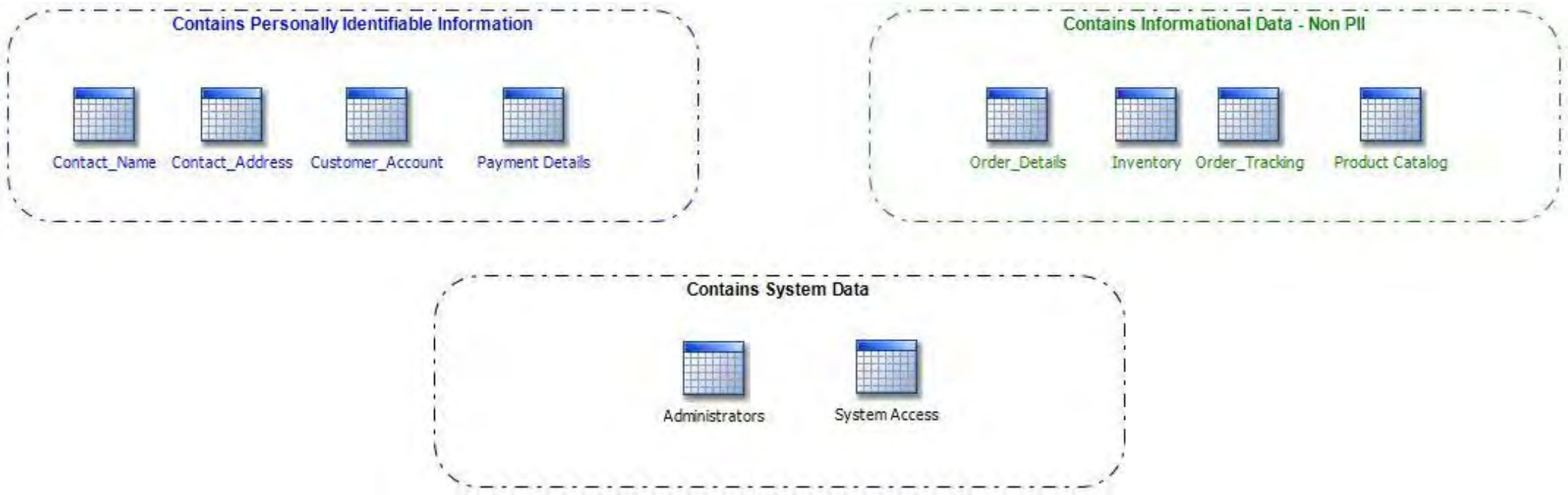
LEVERAGE ENTITY EDITORS

- Ability to link “like” or related objects
  - Within same model file
  - Across separate model files
- Entity/Table level
- Attribute/Column level



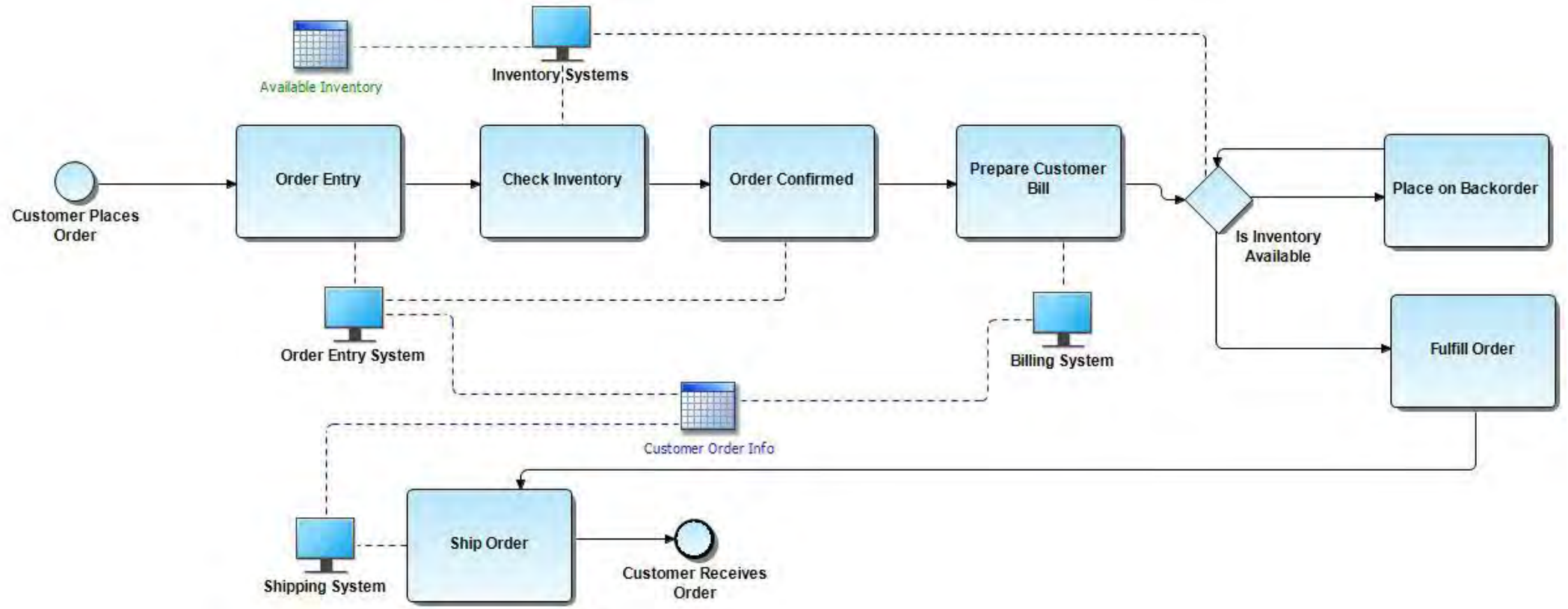
* Entity Editor using IDERA’s ER/Studio Data Architect

KEEP ONLY THE DATA THAT YOU NEED



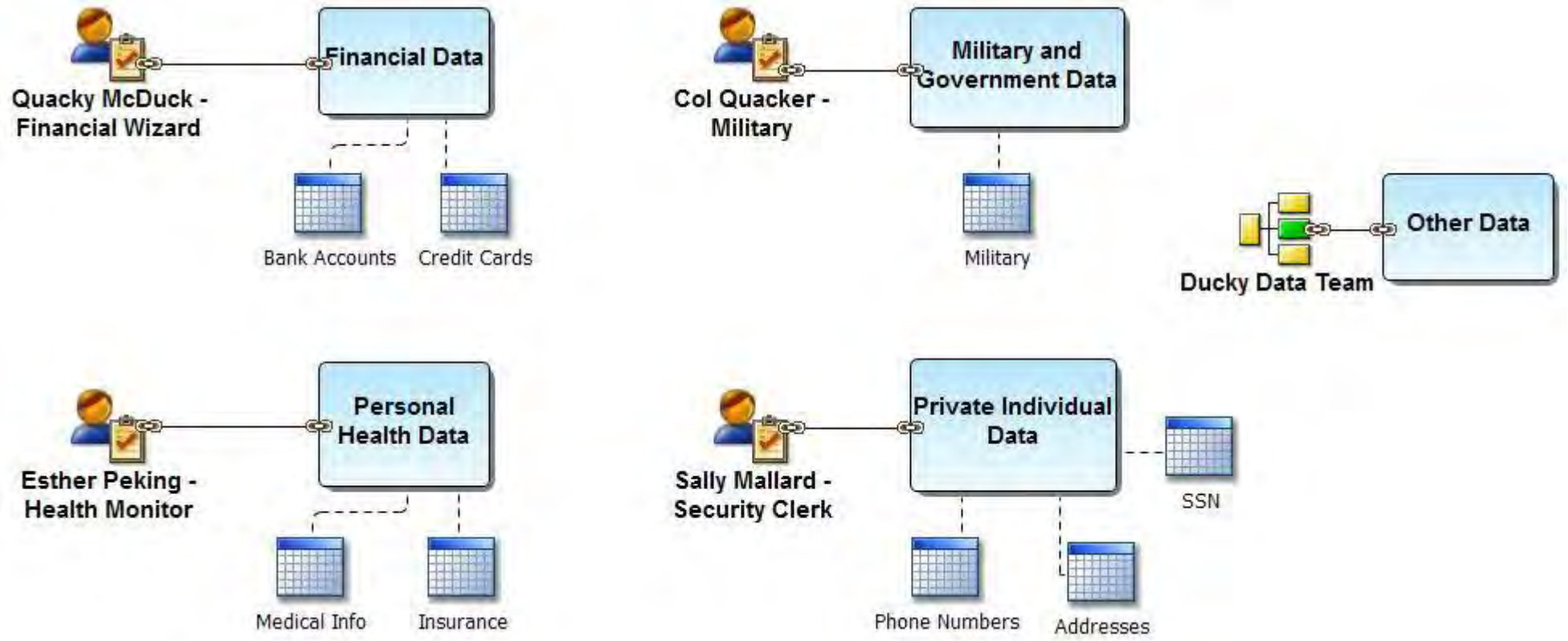
* Business Process Models created using IDERA's ER/Studio Business Architect

DETERMINE WHEN DATA SHOULD BE AVAILABLE



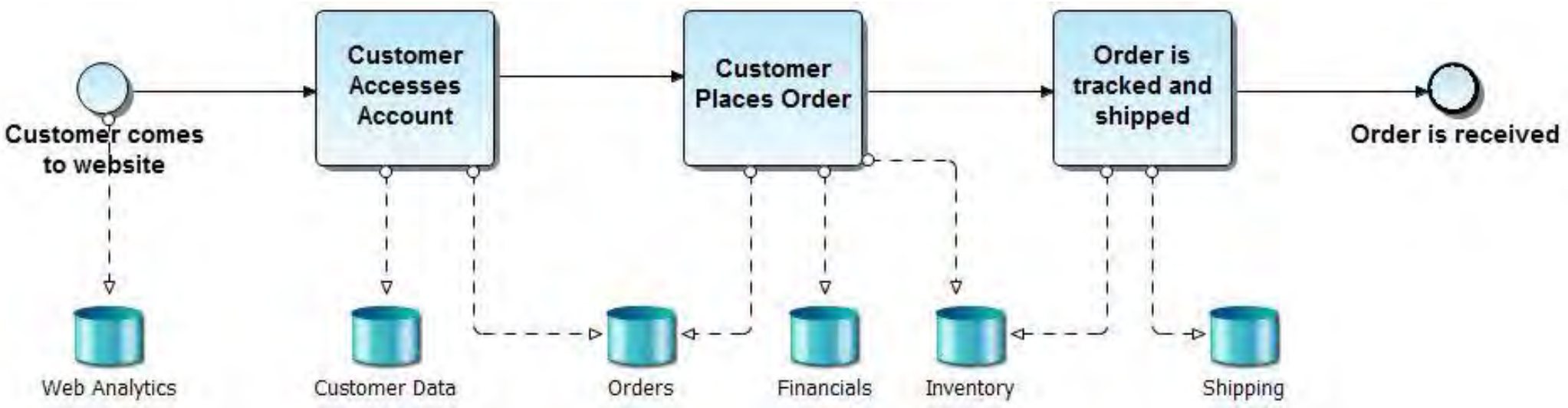
* Business Process Models created using IDERA's ER/Studio Business Architect

WHO HAS ACCESS TO THE DATA?



* Business Process Diagram created using ER/Studio Business Architect

WHERE IS DATA STORED?

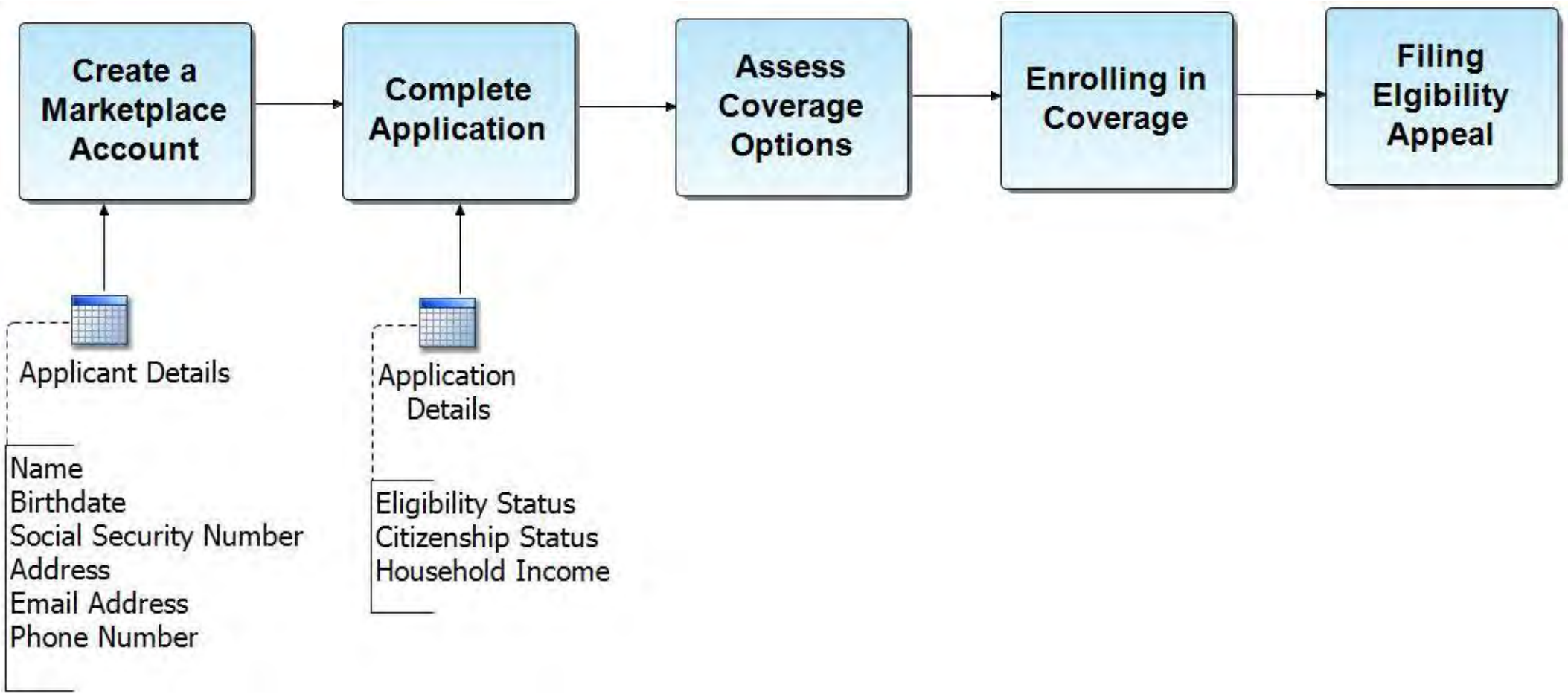


* Business Process Diagram created using ER/Studio Business Architect

CREATE DATA BREACH PROCESSES

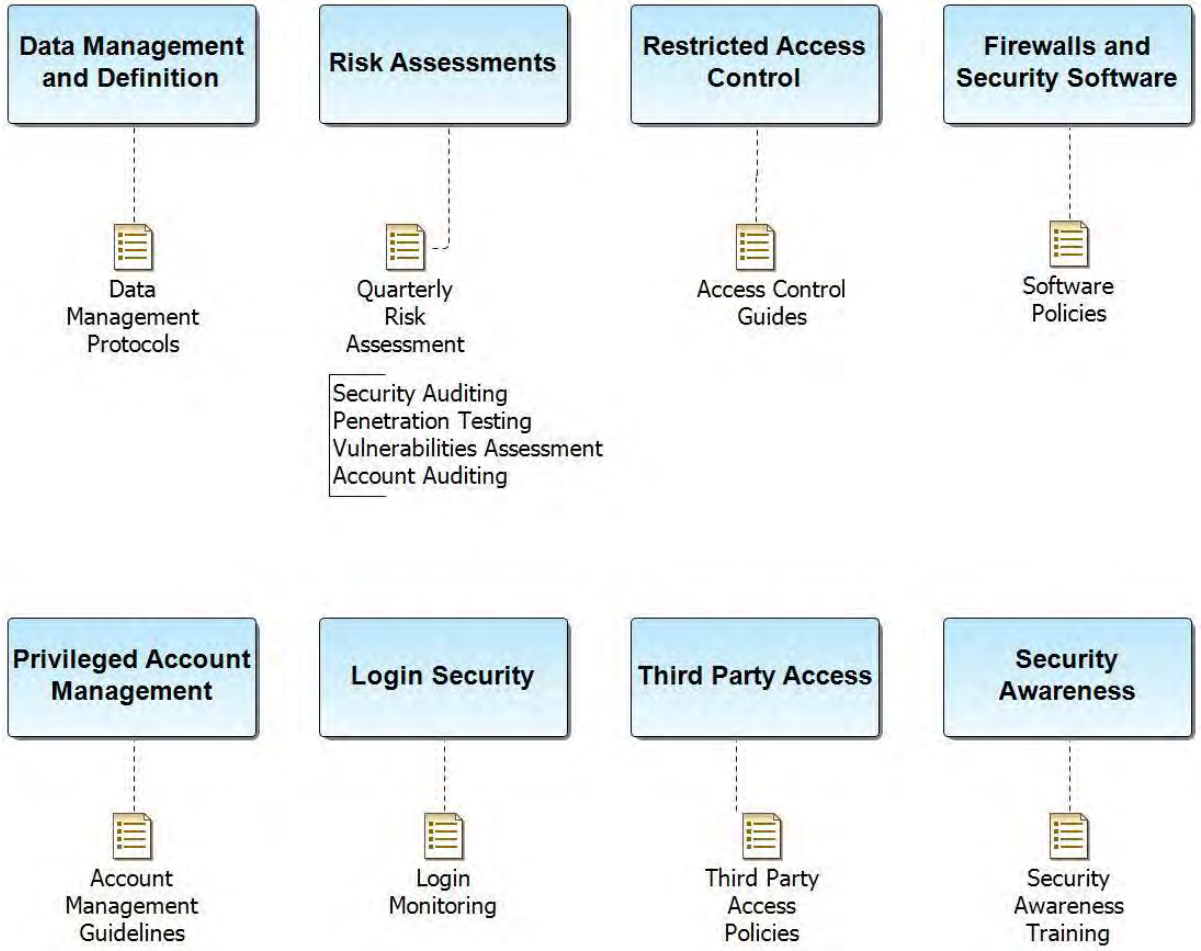
- What are your procedures for handling PII Data?
- What security protocols are in place to protect the data?
- How will you respond to a data breach?
- How do you detect that a breach is occurring?
- How will you notify affected customers?
- How will you train your teams on your processes?

HANDLING PII DATA



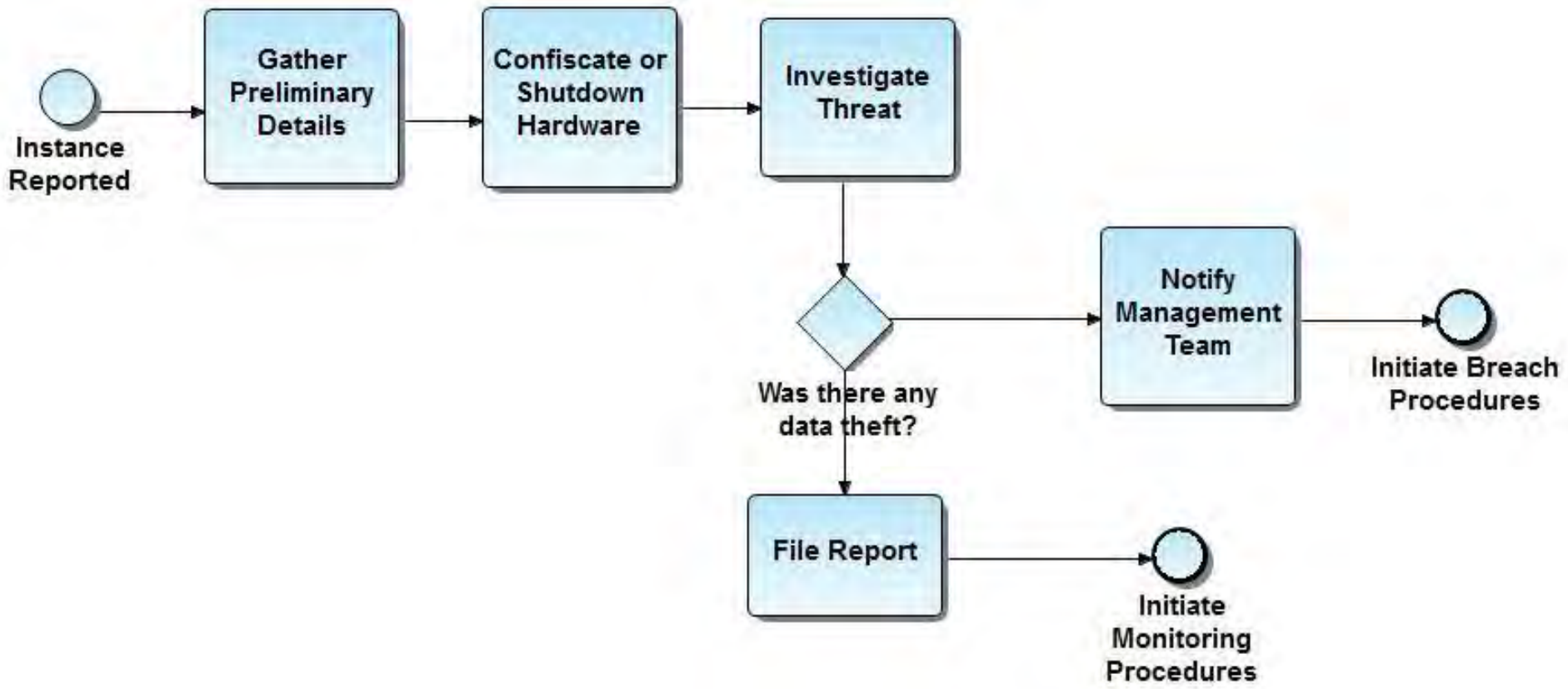
* Business Process Diagram created using ER/Studio Business Architect

ESTABLISHING SECURITY PROTOCOLS



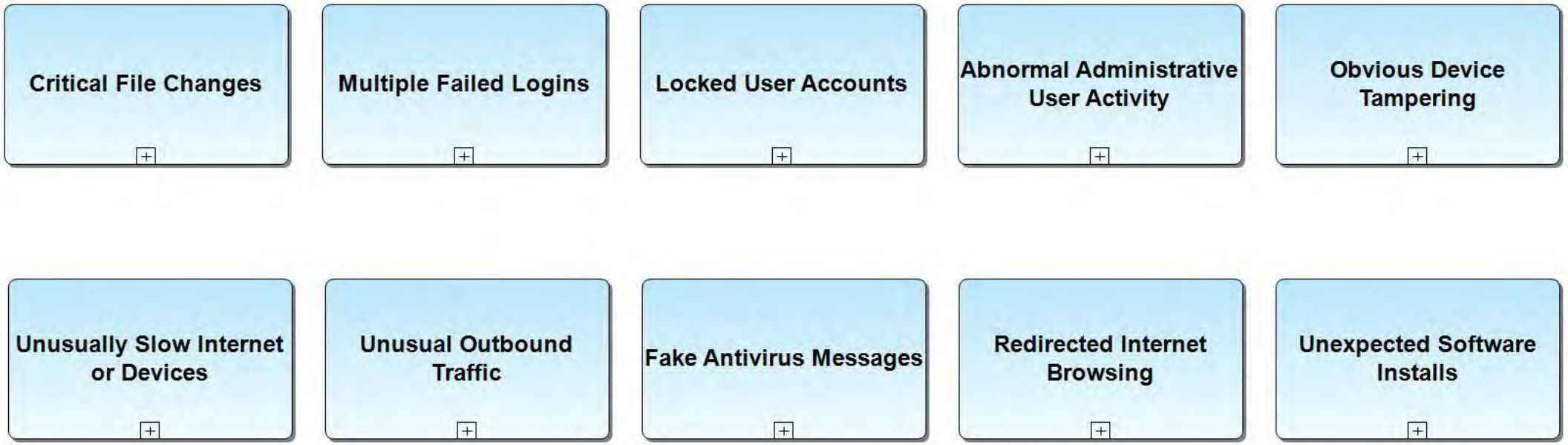
* Business Process Diagram created using ER/Studio Business Architect

HOW TO RESPOND TO A BREACH



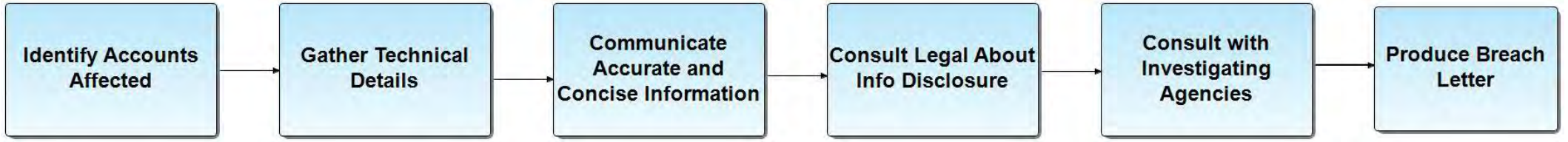
* Business Process Models created using IDERA's ER/Studio Business Architect

DETECT DATA BREACH IN PROGRESS



* Business Process Models created using IDERA's ER/Studio Business Architect

DATA BREACH NOTIFICATION



* Business Process Models created using IDERA's ER/Studio Business Architect

HOW IDERA CAN HELP

IDERA PRODUCTS FOR GDPR PREPARATION

- ER/Studio Enterprise Team Edition can help you to document your data processes and incorporate data standards into your data architecture
- SQL Compliance Manager can help to detect breaches and audit your information to make sure that the wrong people aren't accessing your data
- SQL Safe Backup can help to encrypt the data in your backups
- SQL Inventory Manager can verify that your servers are patched and up to date
- SQL Secure can audit privacy and encryption standards

Download a trial copy of our products at https://www.idera.com/

FOR MORE DETAILS ON GDPR PREPARATION

- White Papers
  - How our products help with GDPR
  - Governing GDPR – Challenges with Enterprise Data Architecture
- Blogs
  - Getting prepared for GDPR
  - Looking towards 2018 – GDPR Impact

IN CONCLUSION

- Data breaches are common and will continue to become more common
- While companies improve their data breach processes, costs continue to climb
- Because data breach processes are so common, GDPR is taking deliberate steps to ensure that companies take serious efforts to protect people's personal information
- Knowing what to do in the case of a breach will help to drive down costs should a data breach occur
- There are tools out there that can help you limit your chances for breach and help you quickly detect and respond to a breach should it occur.

THANKS!

Any questions?

You can find me on Twitter at:

Kim Brushaber
@Brushaber_IDERA