June 11, 2015

Innovate Forward

Biometric Analytics Cost Estimating

Joseph Sarage and Sean McKenna

Booz | Allen | Hamilton

Biometric Analytics Cost Estimating

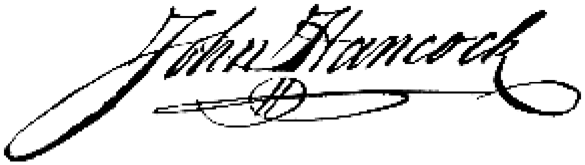
- Background
- Approach
- Case Study
- Final Words
- Q & A

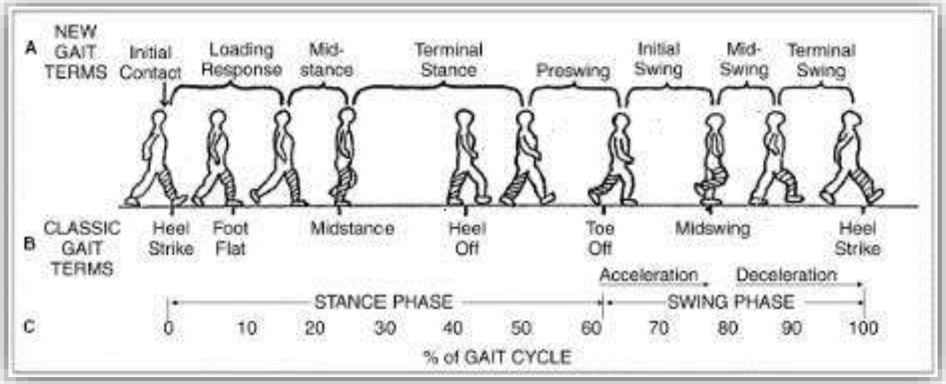
Background: Biometrics

Biometric technologies measure and analyze human physiological and behavioral characteristics

- Physiological characteristics include:
  - Fingerprints
  - Hand prints
  - Face
  - Eye retina / iris

- Behavioral characteristics include:
  - Speech
  - One’s signature
  - Gait





Biometrics are very effective personal identifiers

- Biometrics are integral to something about an individual
  - Require nothing but the individual his/herself (i.e., no ID, no password)
  - Linked to the individual
    - More reliable
    - Cannot be forgotten
    - Less easily stolen or lost
    - Less easily spoofed

- Biometric systems are typically automated, making biometric decision-making very fast
  - Can be near-real time

All biometric systems involve similar processes that can be divided into two distinct stages

- Enrollment
  - The system is populated with the information needed to identify a specific person

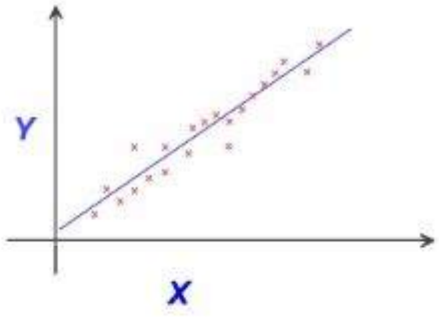
- Verification or identification
  - For verification, the objective is to verify that a person is who he or she claims to be (i.e., the person who enrolled)
    - Often 1:1 matching
  - For identification, the objective is to identify who a person is
    - Often 1:N matching

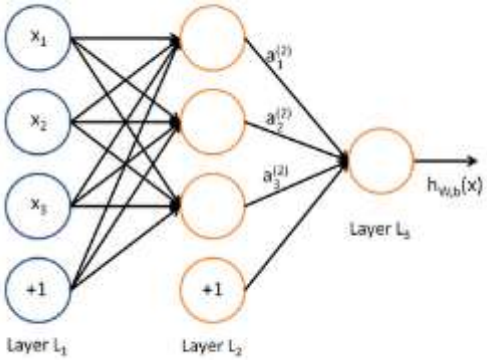
Background: Advanced Analytics

Analytics is the discovery and communication of meaningful patterns in data

- Analytics relies on the simultaneous application of
  - Statistics
  - Mathematics
  - Computer programming
  - Data manipulation

- As simple as fitting a line to a set of points, or as complex as using an artificial neural network for speech recognition





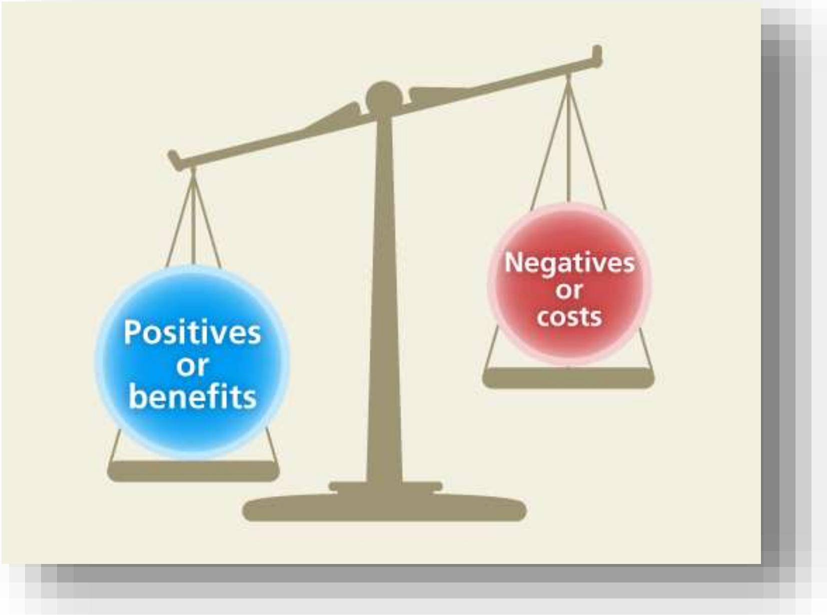
Background: Motivation

Biometric systems are vulnerable to attacks at various stages in the biometric recognition process

- Large biometric databases pose challenges to testing and protecting the integrity of collected data
  - For example, fingerprint databases may be vulnerable to cyberattacks aimed at impersonating or concealing an individual’s identity through the use of synthetically generated fingerprint images (spoofs)
- A number of advanced analytics techniques (e.g., machine learning approaches) have been proposed to address the problem of spoofed biometric detection
  - Leverage the rapid growth of fields such as data science and the ability to mine and exploit massive data stores
- The goal of implementing a biometric analytics capability would be to reduce, in an automated fashion, the instances of fraud within a system

Do the benefits of a biometric analytics capability outweigh the costs?

- Realized cost savings would include
  - Readily quantifiable savings (e.g., reducing welfare abuse)
  - Less tangible cost reductions such as reducing occurrences of illegal entry or access (e.g., illegal entry into the Unites States by someone on a watch list)
- Costs would include
  - Development costs
  - Implementation costs
  - Maintenance costs



Approach

We follow a systematic approach to determine if deploying a biometric capability is a worthwhile investment

- To quantify the costs of biometric vulnerabilities, our approach assesses the impact at a number of levels:
  - Individual
  - Company
  - Country

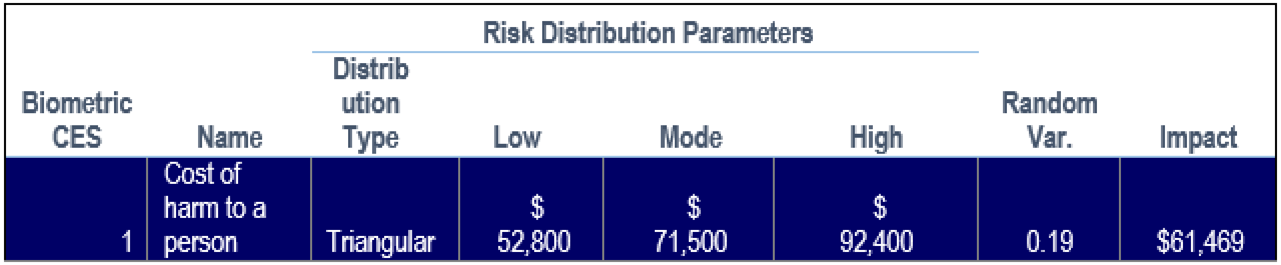
ARGO
Simulation for Decision Support

- For the cost estimates, we used a Booz Allen Hamilton simulation tool called Argo$^{\text{TM}}$, fitting the data with a triangular distribution and employing random variable generation for impact value estimation
- For each of the cost element structure items, a “low,” “mode,” and “high” value was used to bound the variable set and run a 5,000-trial Monte Carlo simulation analysis

Case Study

Case Study: Spoofs within a large data store of fingerprint records

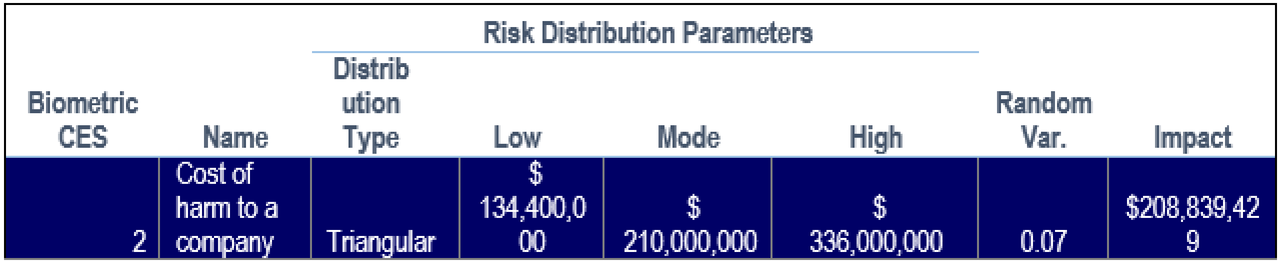
- We quantified what the cost is as a result of there being a chance of a person exploiting the spoof and gaining entry illegally
- For cost estimating purposes, a triangular distribution was used to estimate the cost of harm to a **person** if a biometric feature was compromised
- The table below shows the impact in U.S. dollars:



		Risk Distribution Parameters					
Biometric CES	Name	Distribution Type	Low	Mode	High	Random Var.	Impact
1	Cost of harm to a person	Triangular	$ 52,800	$ 71,500	$ 92,400	0.19	$61,469

Case Study: Spoofs within a large data store of fingerprint records, continued

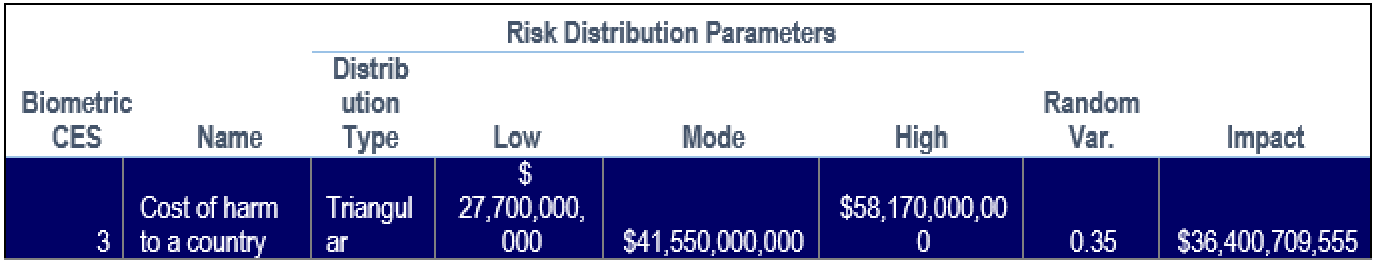
- For cost estimating purposes, a triangular distribution was used to estimate the cost of harm to a **company** if a biometric feature was compromised
- The table below shows the impact in U.S. dollars:



		Risk Distribution Parameters					
Biometric CES	Name	Distribution Type	Low	Mode	High	Random Var.	Impact
2	Cost of harm to a company	Triangular	$ 134,400,000	$ 210,000,000	$ 336,000,000	0.07	$208,839,429

Case Study: Spoofs within a large data store of fingerprint records, continued

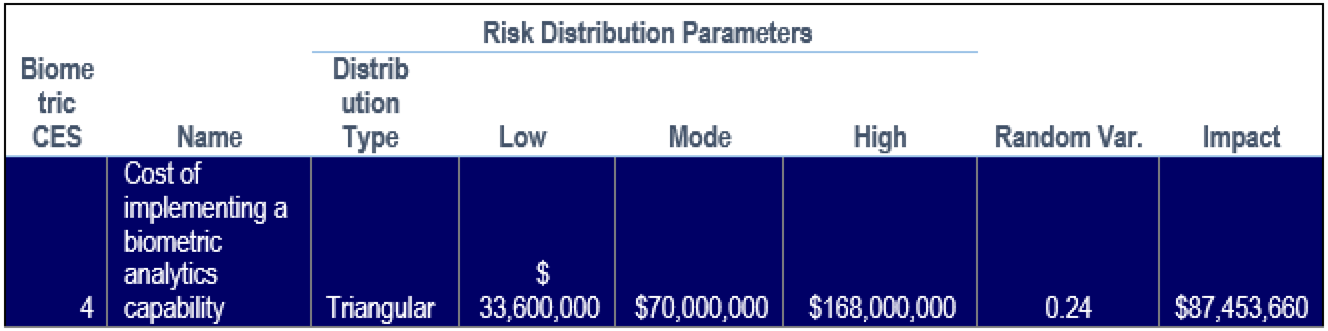
- For cost estimating purposes, a triangular distribution was used to estimate the cost of harm to a **country** if a biometric feature was compromised
- The table below shows the impact in U.S. dollars:



		Risk Distribution Parameters					
Biometric CES	Name	Distribution Type	Low	Mode	High	Random Var.	Impact
3	Cost of harm to a country	Triangular	$ 27,700,000,000	$41,550,000,000	$58,170,000,000	0.35	$36,400,709,555

Case Study: Spoofs within a large data store of fingerprint records continued

- For cost estimating purposes, a triangular distribution was used to estimate the **cost** to implement a biometric analytics capability
- The table below shows the impact in U.S. dollars:



		Risk Distribution Parameters					
Biometric CES	Name	Distribution Type	Low	Mode	High	Random Var.	Impact
4	Cost of implementing a biometric analytics capability	Triangular	$ 33,600,000	$70,000,000	$168,000,000	0.24	$87,453,660

Final Words

We have outlined a process for evaluating the financial merits of implementing a biometric analytics capability

- Biometric systems are vulnerable to attacks at various stages in the biometric recognition process, including attacks on the database in which enrolled entries are stored
- Through our research and analysis, it is evident there are numerous costs that impact individuals, companies, and countries if biometric data is compromised
- One of the key challenges is determining whether or not adopting such a capability is ultimately worthwhile and this is an important decision that requires a systematic analysis

There is significant opportunity for future work in the biometric analytics cost estimating space

- Deriving new and innovative ways to reduce the overall cost of implementing a biometric capability at the individual, company, and country level
- As technologies improve and become more accessible, development and implementation costs should diminish, making these capabilities more accessible to a broader user base

Questions?