Cybersecurity Insider Threat Analytics

Speakers: Joel Amick, Cory Hefner, and Aysha Nahan

Disclosure

This material is for informational purposes only and should not be regarded as a recommendation or an offer to buy or sell any product or service to which this information may relate.

Certain products and services may not be available to all entities or persons. Past performance does not guarantee future results.

Who We Are

ANALYTICS FRONTIERS CONFERENCE 2018
MARCH 21, CHARLOTTE

Joel Amick
Director,
Cyber Analytics

Cory Hefner
Sr. Info Security Analyst, Cyber Analytics

Aysha Nahan
Data Analyst,
Cyber Analytics

In Partnership With

ANALYTICS FRONTIERS CONFERENCE 2018
MARCH 21, CHARLOTTE

Internship Associates

UNC CHARLOTTE
Data Science Initiative

Interns from the *Professional Masters in Data Science* program at the University of North Carolina at Charlotte (UNCC), with experience in Advanced Analytics and Machine Learning.

Graduate Students in Data Science Program at UNCC

David Milbern

Kshitij Khurana

Aysha Nahan

Abhinay Reddy

TIAA Cybersecurity Mentors

Joel Amick
Director,
Cyber Analytics

Cory Hefner
Sr. Info Security Analyst, Cyber Analytics

Who is TIAA?

FOUNDED IN **1918**

397 offices in 19 countries

More than **16,500** employees[1]

Our customers

5M individuals

More than **15,000** institutions serviced by TIAA[2]

$1T in assets under management with holdings in more than 50 countries[3]

1,050 More than 1,050 financial advisors[4]

More than **$394B** in benefits paid since 1918[5]

- According to a recent survey of 18 providers, TIAA is the largest manager of qualified plan stable value assets with **$163.5 billion** in stable value accumulation values.[6]
- TIAA is the #1 not-for-profit retirement market provider in assets and participant accounts.[7]
- Paid **$4.8 billion to retired clients** in 2016, including 31,000 annuitants over the age of 90.
- TIAA Traditional has credited interest rates higher than the guaranteed minimum under one or more contracts every year since 1948.[8]

https://www.tiaa.org/public/pdf/facts_stats.pdf

Who is TIAA?

Investment performance and ratings

98% of TIAA-CREF mutual funds and CREF variable annuities have **expense ratios below the median of their respective Morningstar categories**[9]

1st
Largest global agricultural investor[10]

2nd
Largest grower of wine grapes by acreage in the United States[11]

3rd
Largest commercial real estate manager in the world[12]

- **72%** of TIAA-CREF mutual funds and CREF variable annuities received an overall Morningstar rating of **4 or 5 stars** across all asset classes, (40% 4 stars and 32% 5 stars).[13]
- Among the highest rated insurance companies in the U.S. by the four leading rating agencies: A.M. Best, Fitch, Moody's Investors Service and Standard & Poor's[14]

https://www.tiaa.org/public/pdf/facts_stats.pdf

PHOTO FROM WIRED.COM

What is an Insider Threat?

Malicious

21.6% of Incidents[1]

Fraud

Intellectual Property Loss

Sabotage or Destruction

Negligent

78.4% of Incidents[1]

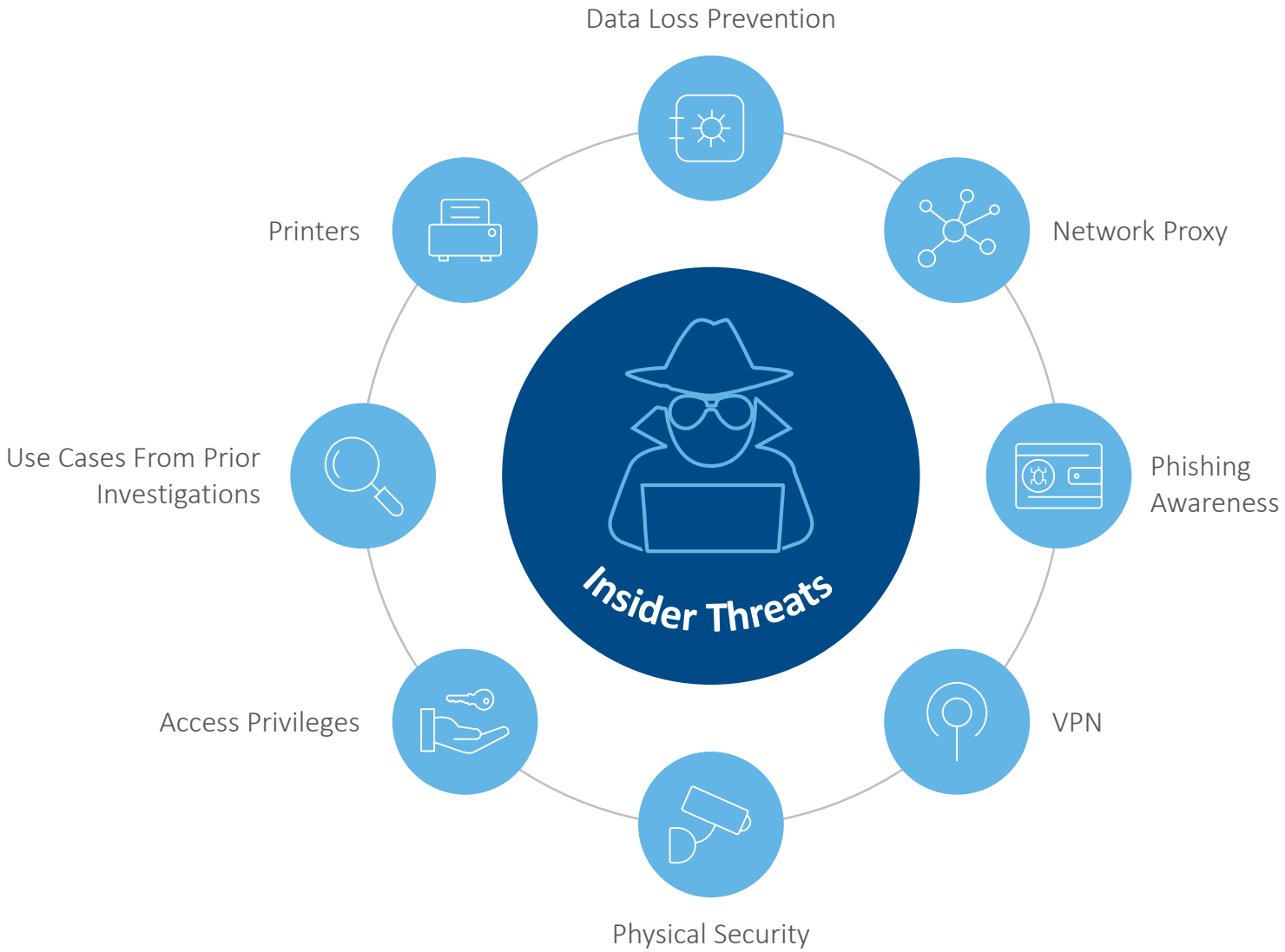
Accidental

Phishing

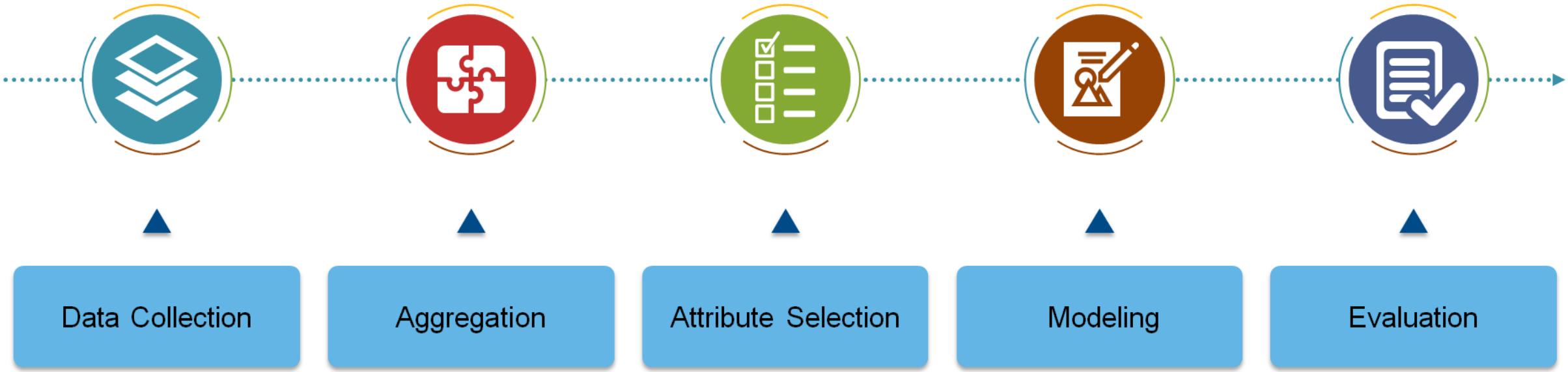
Shared/Stolen Credentials

[1]*Study by Ponemon Institute in Sep 2016*

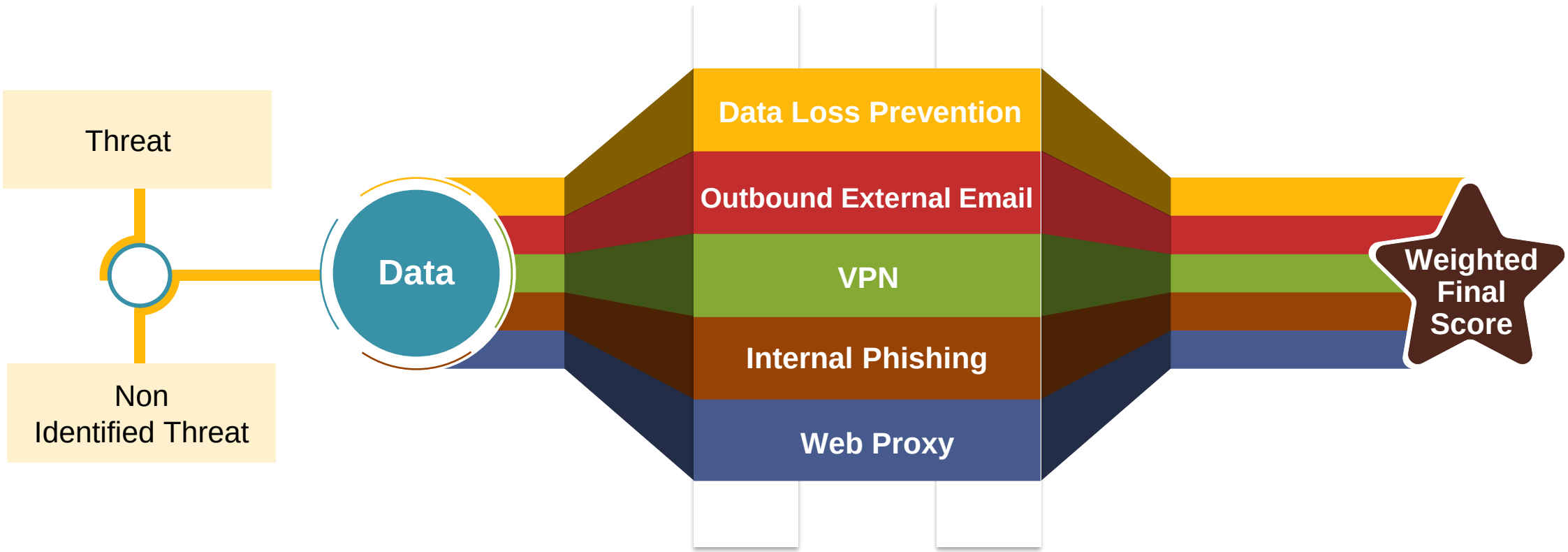
Insider Threat Detection



Proof of Concept



Scoring Approach

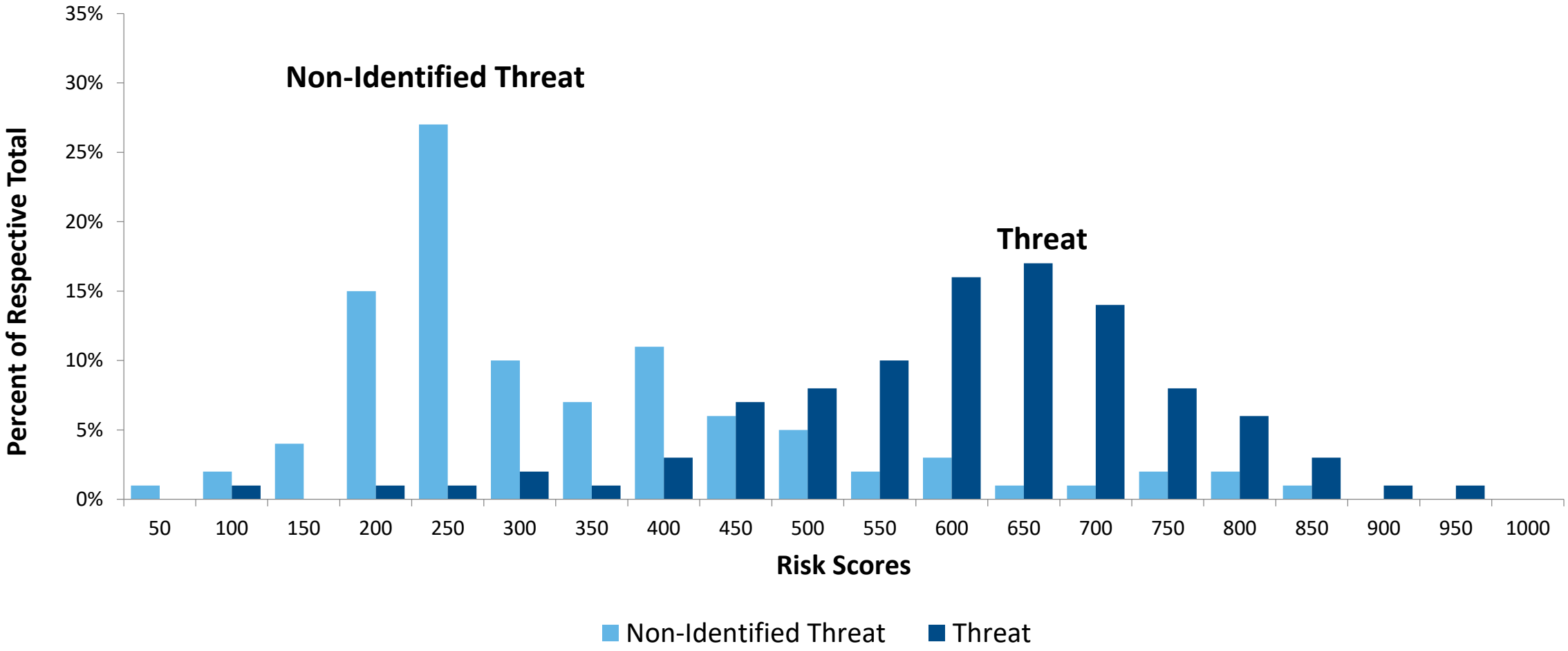


Easily Scalable

Separate Scores by Data Source

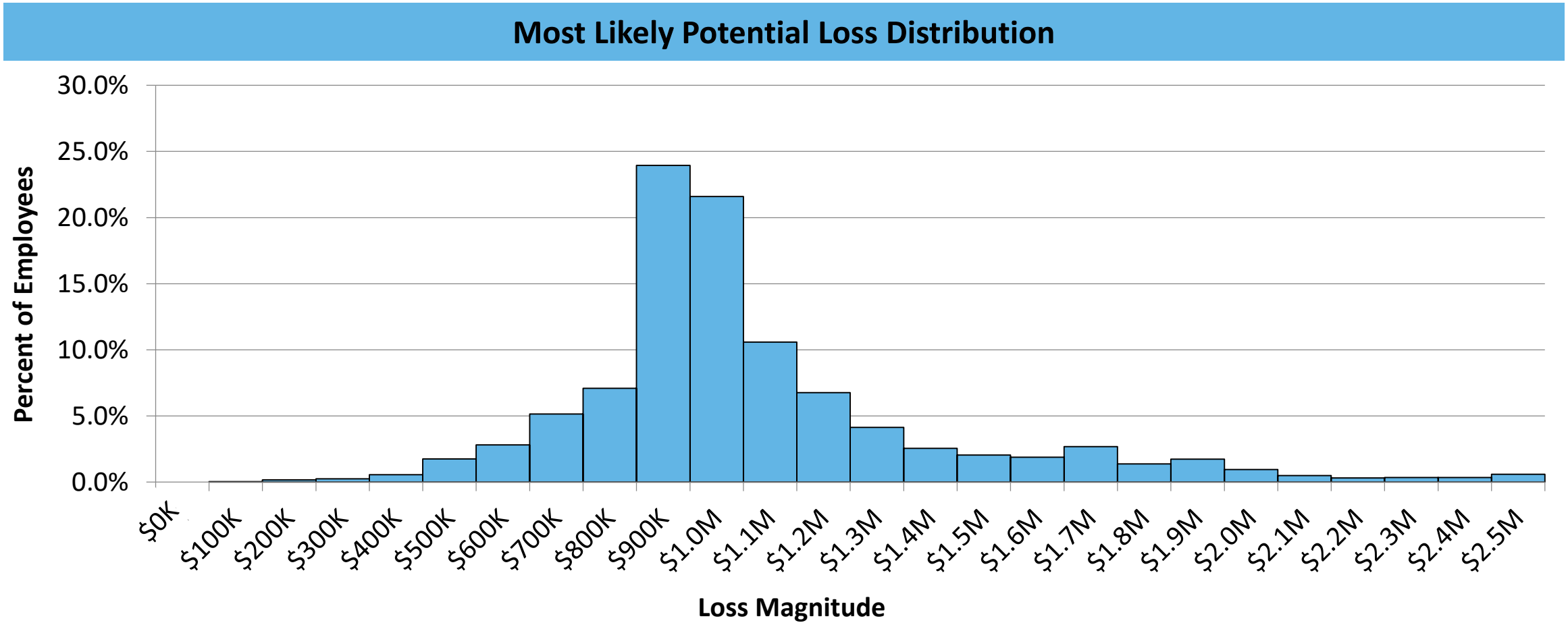
Weighted Ensemble Approach to Scoring

Success of Scoring Algorithms



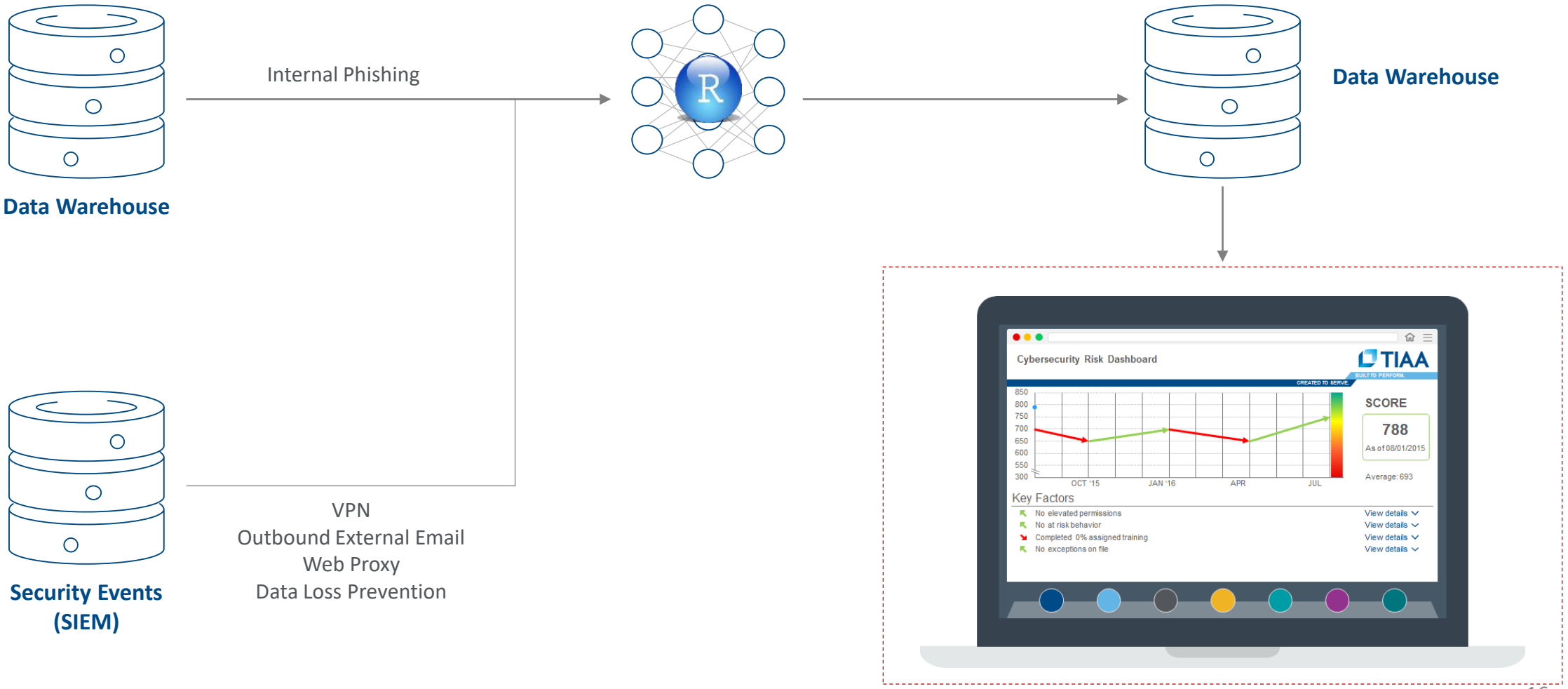
*Distributions are representative of actual data, but numbers are anonymized

Quantifying the Threat



*Distributions are representative of actual data, but numbers are anonymized

Implementation

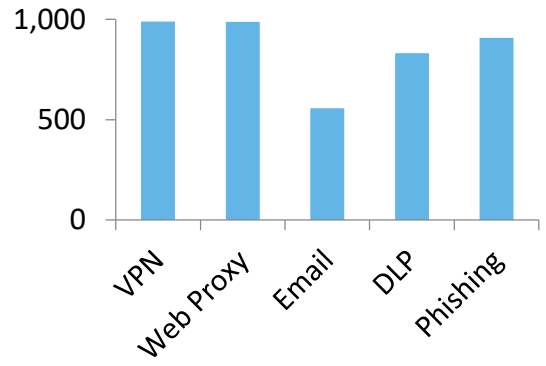


Case Study

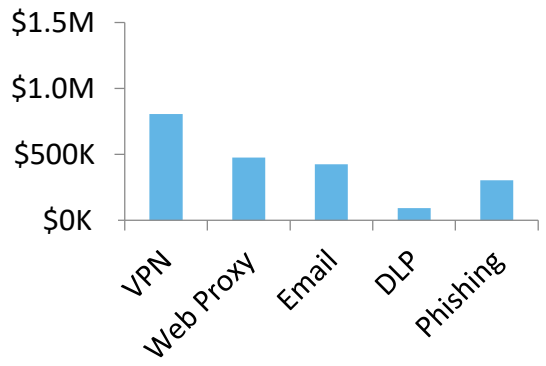
"Joey Jobsearch"

Threat Score: 821 Potential Loss: $2.1M

Insider Threat Score



Loss Magnitude

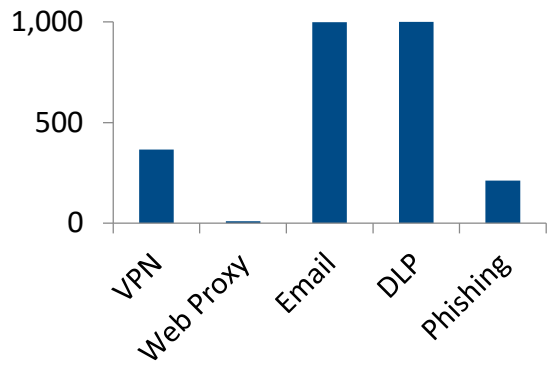


VPN	25 Connection Failures in the last month
Web Proxy	83 Job Searches in the past day 32 File Sharing web pages visited in the past week
Data Loss Prevention	10 Email Attachments blocked in the past 6 months 14 Cybersecurity Policy Violations in the past 6 months
Internal Phishing	1 Internal Phishing Training Email opened in the past year

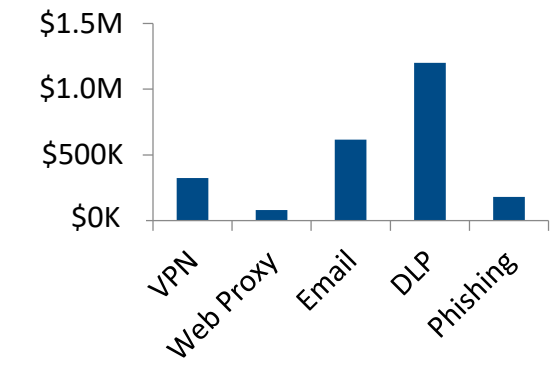
"Blocked Bobby"

Threat Score: 680 Potential Loss: $2.4M

Insider Threat Score



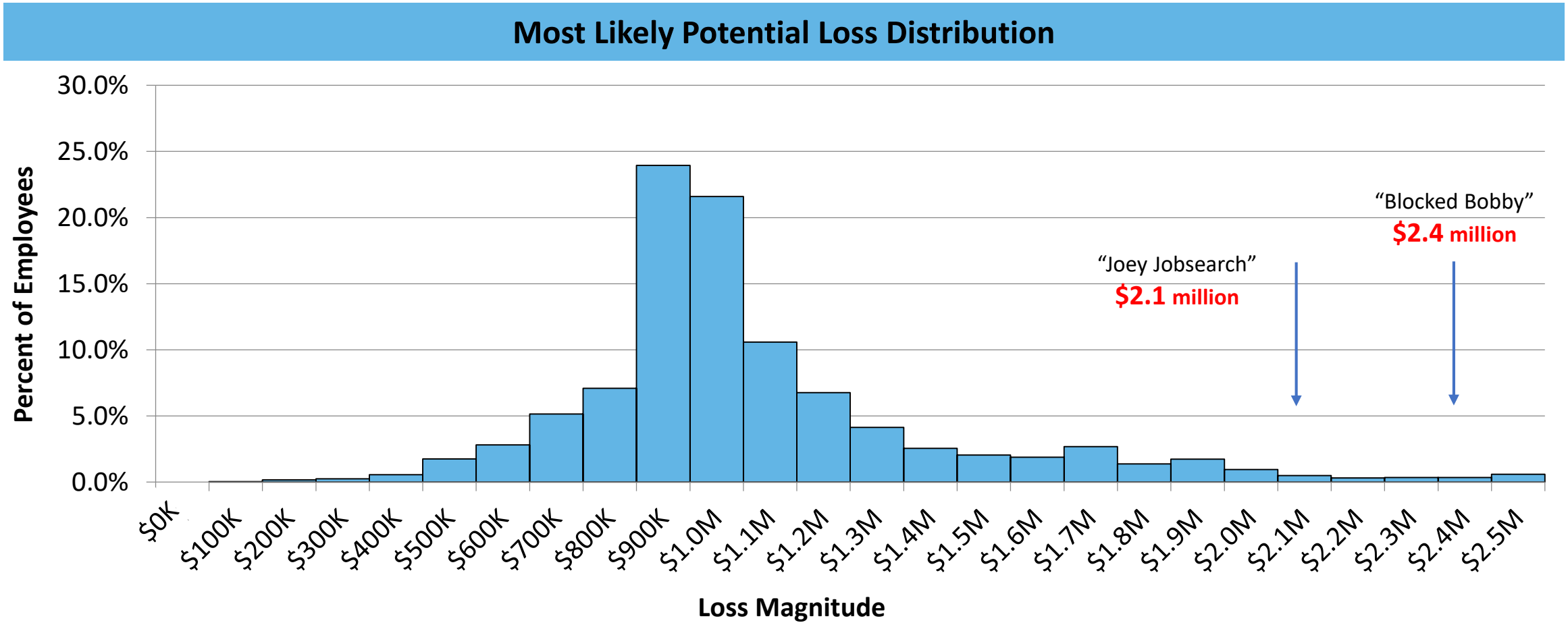
Loss Magnitude



VPN	5 Connection Failures in the last month
Outbound External Email	2 Blocked Emails in the past week
Data Loss Prevention	293 Files Loaded to USB in the past quarter 2 Email Attachments blocked in the past week
Internal Phishing	2 Internal Phishing Training Emails reported in the past year

*Distributions are representative of actual data, but numbers are anonymized

Actionable Intelligence



*Distributions are representative of actual data, but numbers are anonymized

Impact and Successes

Business Impact	Successes
1 Insider Threat and Detection Teams can use scores to prioritize incidents	1 Collaborated with Cyber Risk team for Projected Loss
2 Quantifiable value of the Insider Threat Program	2 Actionable intelligence was identified & escalated to the Insider Threat team
3 Matures Cybersecurity Investigations and Operations	3 Process is robust and allows for easy tuning or additions of new data sources
	4 Provided new exploratory information about Insider Threat data sources

Challenges and Opportunities

ANALYTICS FRONTIERS CONFERENCE 2018
MARCH 21, CHARLOTTE

Challenges	Identified Opportunities
1 Algorithms are trained predominantly with negative behavior. Opportunity to incorporate positive attributes in future tuning efforts.	1 Complete dashboard visualizations for Investigations
2 Structured and unstructured data stored in disparate data sources	2 Generate “Harm-Ability” scores based on the capability (permissions and exceptions) of employees potential for impact to the company
3 Managing scope	3 Incorporate additional data sources to further improve the accuracy of the Insider Threat score

Next Steps


Cybersecurity Risk Dashboard
TIAA
1000
900
750
700
650
600
550
300
L7
L6
L5
Significant Contributing Factors
No elevated permissions
View details
No at risk behavior
View details
Completed 0% assigned training
View details
No exceptions on file
View details
Detailed Scores
Name of Direct Report
Ability
"Joey Jobsearch"
820
233
"Blocked Bobby"
680
586
Sly Sarah
250
Arnold Attachment
605
Suspicious Sam
422
Confidential Connie
905
Risky Rick
179
"Joey Jobsearch" SCORE: 821
Insider Threat Score
1000
800
600
400
200
0
VPN
Web Proxy
Email
DLP
Phishing
Loss Magnitude
$2.0 M
$1.5 M
$1.0 M
$500 K
$0 K
VPN
Web Proxy
Email
DLP
Phishing
VPN
25 Connection Failures in the last month
Web Proxy
77 Job Searches in the past day
22 File Sharing websites visited in the past week
Data Loss Prevention
10 Email Attachments blocked in the past 6 months
14 Cybersecurity Policy Violations in the past 6 months
Internal Phishing
1 Internal Phishing Training Email opened in the past year

Questions?