Advanced Analytics in Cyber Security

Michael McFadden
Fraud, Security & Compliance
August 1, 2017

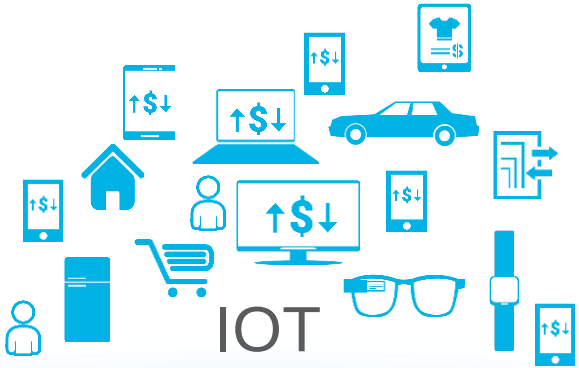
Topics for Today's Session

Streaming analytics to detect and stop cyber threats

Empirical analytics to assess cyber security posture

Streaming analytics to detect and stop threats

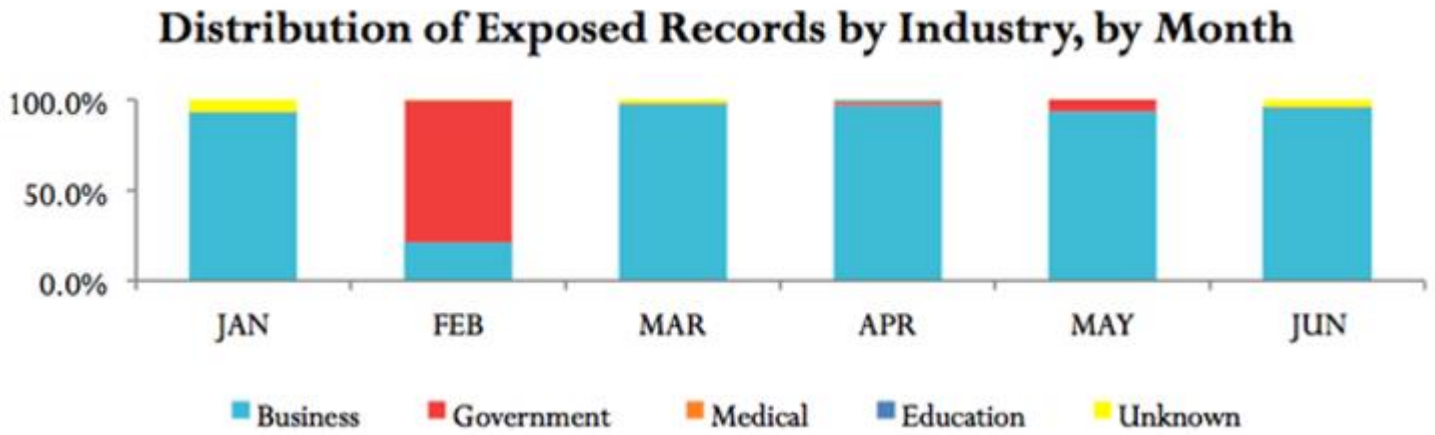
New Entry Points Bring New Risk



1994	2001	2005	2007	2011	2012	2013	2014	2015	2016
Online Banking	1Million online users	FFIEC announces regulation for online banking	Apple launches iPhone and banking by phone launches	Online Banking is now main-stream	20%+ of all smartphone users use a mobile banking app	One in three Americans state they stay with their bank because their mobile banking services makes it convenient	US m-commerce makes up 29% of web sales	57% of US smartphone owners have used their devices for online banking	Smart phone users will account for 96% of total mobile banking *Aite prediction*

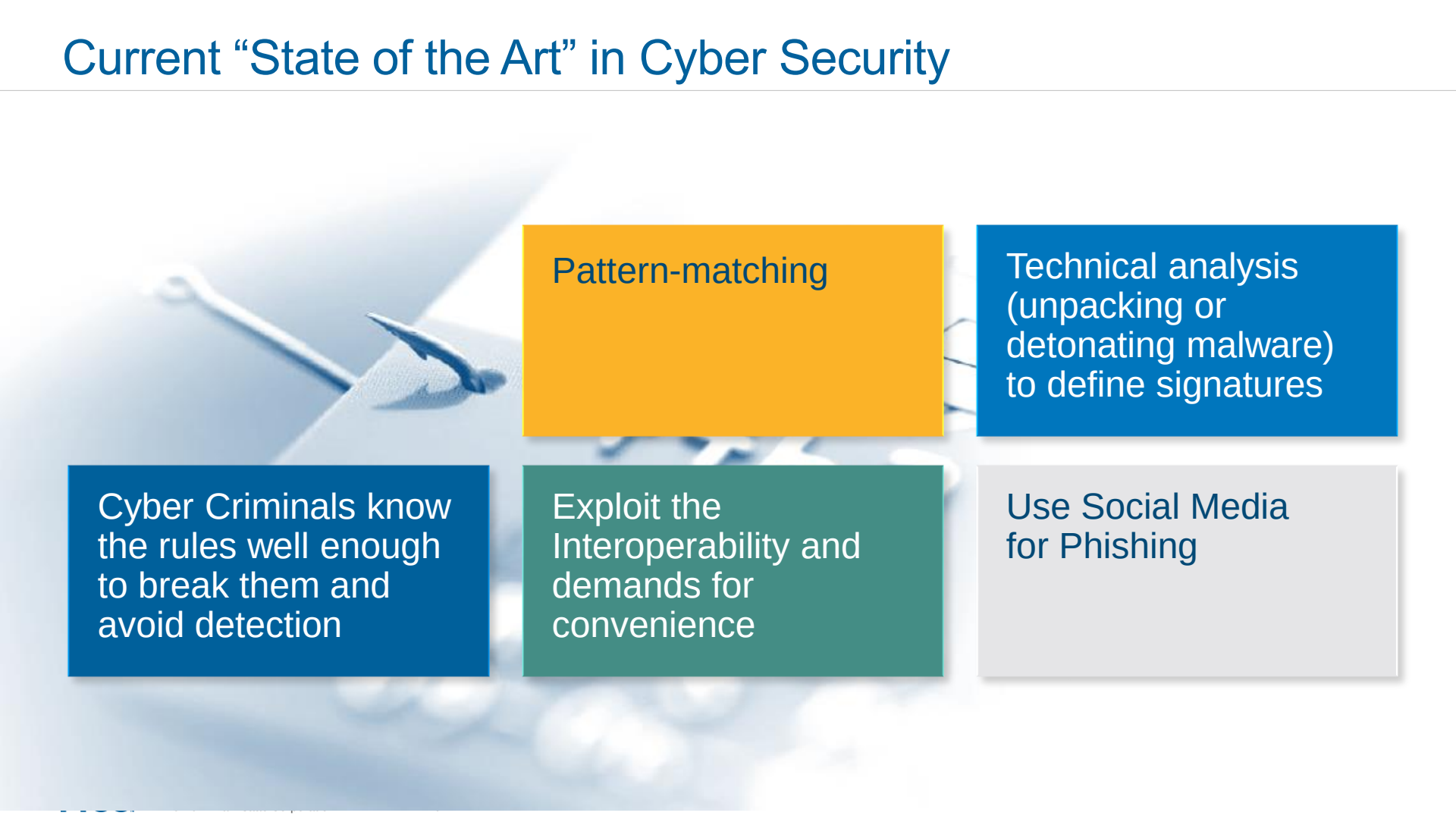
Over 6 BILLION records exposed in first half of 2017*

There has been an alarming trend in the TARGETING OF TAX DATA.
The number of confirmed successful attacks increased by 25%.



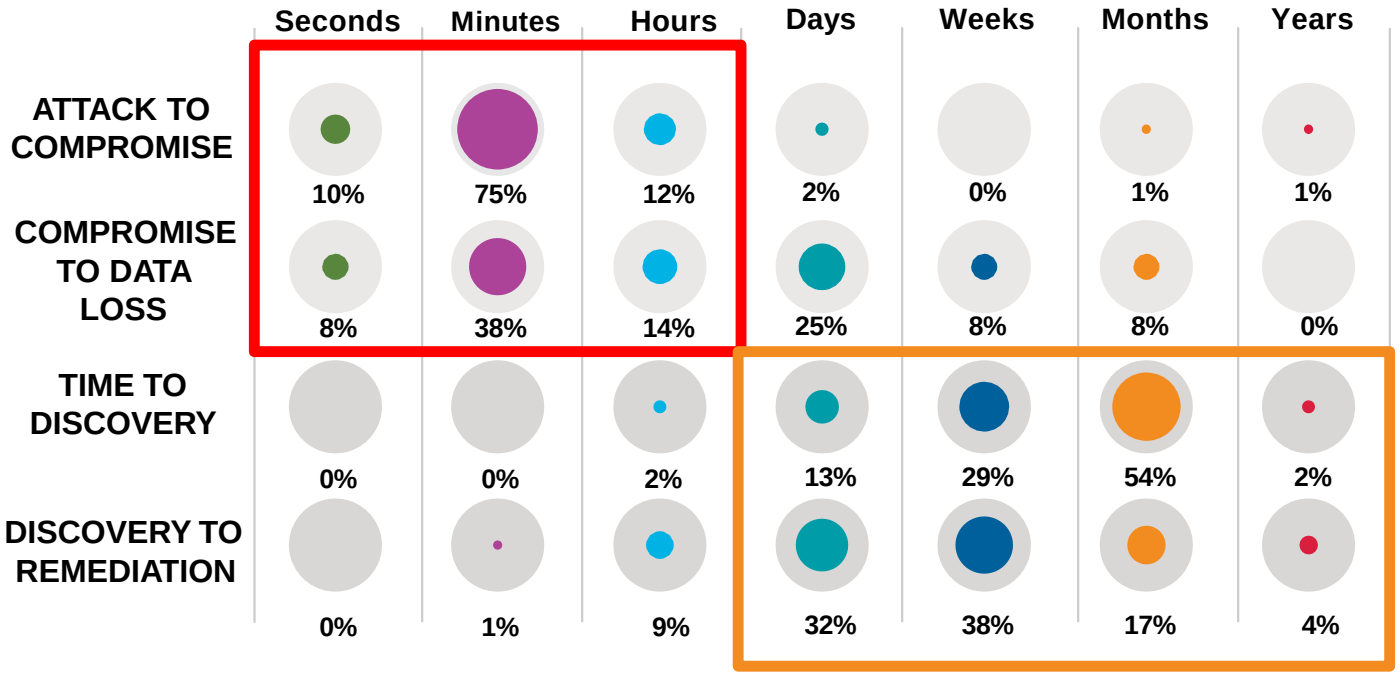
* Help Net Security – July 25, 2017
https://www.helpnetsecurity.com/2017/07/25/data-breaches-2017

Current “State of the Art” in Cyber Security



The gap between breach and discovery

When a breach occurs, the majority of sensitive data is stolen within minutes increasing this challenge



In **60% of breaches**, data is stolen within hours

54% of breaches are not discovered for months

Source: Verizon 2013 Data Breach Investigations Report

Shortcomings of the current "state-of-the-art" detection

TOO MANY UNDIFFERENTIATED ALERTS

TOO MANY NEW / MORPHING / EVOLVING THREATS SLIPPING THROUGH

TOO FEW QUALIFIED RESOURCES TO INVESTIGATE AND RESOLVE CYBER THREATS

MOST OF TODAY'S SECURITY SOLUTIONS HAVE FUNDAMENTAL FLAWS:

- Based on what happened yesterday (or last week or last year)
- Require human interpretation of events
- Lack the means to adapt and self-correct
- No effective method to differentiate alerts
- Threats have become dynamic, making rule-based approaches less effective
- Devices, access points, and use cases have grown exponentially
- Network complexity has evolved beyond expert capacity to understand


Machine Learning Analytics
are the New Imperative in Cyber
FICO

Cybersecurity Analytics

Streaming data analysis

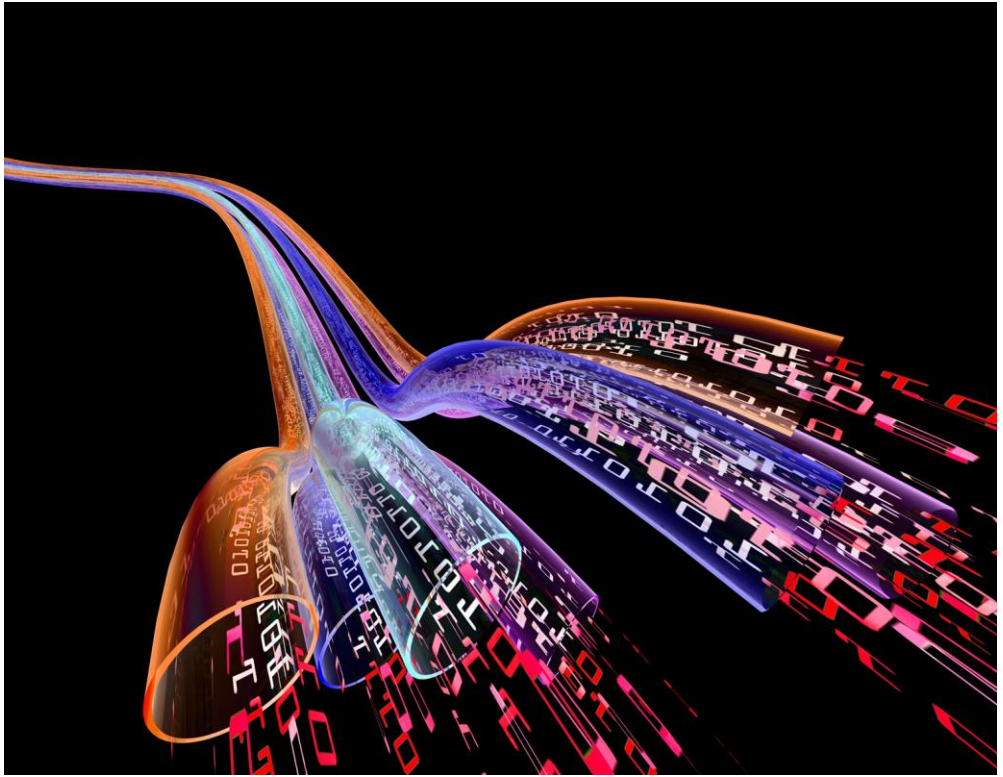
- Real-time threat detection
- Enables automated containment and faster remediation
- Scalable distributed processing

Self-learning UEBA

- Emerging threat detection
- Layered analytics model - Not limited to heuristics or peer group comparisons
- Responsive to analyst feedback through global consortium
- Continuous adaptation reduces false positives

Continuous entity scoring

- Entity profiling – devices, users, etc.
- Precise risk ranking with score range
- Simple results - score with detailed reasons to guide triage and response



Adaptive real-time analytic models for accurate anomaly and threat detection

Cyber Security Analytics – Key Highlights

Addresses Major Security Gaps

- ✓ Reduces threat dwell time through real-time detection
- ✓ Reduces false positives – precise detection using self-learning analytical model
- ✓ Improves efficiency of security professionals
  - Prioritizes threat risks through granular scoring
  - Simple Results – Score plus detailed reasons to guide analyst in investigation

Adaptable

- ✓ Self-learning AI technology
- ✓ Flexible model - Accommodates new data sources and entity types (IoT)
- ✓ Scalable - Doesn't require large data store, fast streaming engine
- ✓ Modular design - Integrates with existing security eco-system solutions

Proven Technology

- ✓ Analytic Models have been used across industries to detect and stop fraud
- ✓ Numerous threat behaviors detected such as:
  - Reconnaissance activity
  - Command and Control (C&C) communication
  - Data Exfiltration

Empirical analysis to assess cyber security posture

Can your vendors and partners be trusted with your data?

Security experts warn of account risks after Verizon customer data leak

- Customer records for at least **14 million subscribers**, including phone numbers and account PINs, were exposed.
- Records were found on an unprotected Amazon S3 storage server controlled by an employee of Nice Systems, a **vendor of Verizon**
- **Over a week** before the data was eventually secured.

Key challenges in cyber risk quantification

- The space is nascent, and commercial solutions are just coming on the scene.
- Available metrics are expert-driven, lacking an empirical, quantitative connection between conditions, behaviors, and outcomes.
- Typical scores or ratings are backwards-looking assessments, or focus on current state rather than future outcomes - which is what is actually needed to drive business decision making.
- As good metrics evolve, transparency will be key in allowing market forces to increase our collective security posture.
- The state of the art in cyber breach insurance is pre-actuarial, and currently more art than science. A large proportion of cyber risk remain un-quantified and un-covered, or are “silent cyber” risks, not expressly excluded from other E&O policies.

Parallel Paths – a Historical Perspective

1990s Consumer Credit Scoring

Opportunity

- Apply predictive analytics to drive efficiency and scale in consumer credit underwriting and portfolio management

Solution

- Consumer Credit Scoring
- Rank-order consumers based on likelihood of paying their credit obligations

Result

- Adoption of Credit Scoring now ubiquitous in credit decisions
- Greatly expanded access to consumer credit

2017 Enterprise Security Scoring

Opportunity

- Apply predictive analytics to drive efficiency and scale in active vendor management and executive-level security oversight

Solution

- Enterprise Security Scoring
- Rank-order organizations based on likelihood of suffering a material data breach

Result

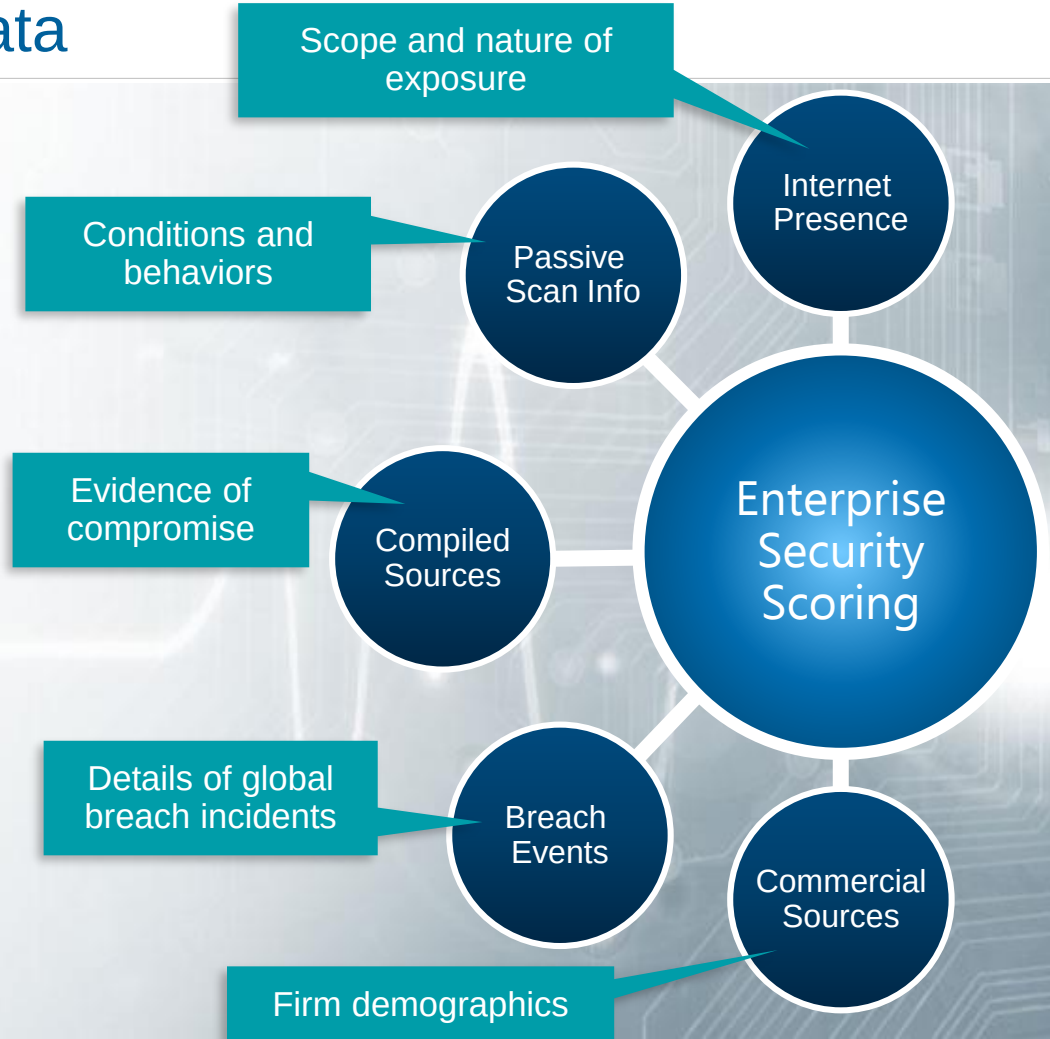
- Empirically-derived assessment of risk
- Trusted metric for active vendor management
- Consistent breach insurance underwriting and portfolio monitoring

Enterprise Security Scoring

- Predictive score based on supervised, empirical analysis of continuously updated data collected at internet scale
- Score or Grade encapsulates the future likelihood of a significant breach event
- Compares external network observations to previously breached networks
- Combines condition and behavior signals
- Reason codes detail primary risk vectors – enabling contextual explanation of results
- Accessed “on-demand”

Security Scoring – The Data

- Data elements continually monitored at internet scale, reflecting:
  - Policy effectiveness
  - Management behaviors
- Data richness that supports empirical analysis, not judgment-based grades
- Data utilized reflects historical risk indicators from global organizations
  - Machine learning used to evaluate historical risk indicators to understand correlated pre breach behaviors
  - Risk indicators are then used in the predictive model as labels



Different Views of your Risk Posture

Internal Self Assessment

- Enable CISOs to demonstrate security performance over time
- Provides detailed threat info across all evaluated network assets
- Supports drill-down to primary threat vectors
- Strengthens defenses with actionable information
- Supports investment decisions and resource allocation

Third Party/Vendor Risk Assessment

- Supports CROs and CISOs in active vendor management
- Vet the risk of potential partners
- Monitor the risk of your entire partner portfolio
- Benchmark across categories or segments of partners
- Supports breach insurance underwriting

Profile Name	Network Assets	Security Score	Endpoint Security	Infrastructure Security	Services Security	Last Updated
Octondo Golf Resort	3.02 in 5 prefixes	620	1	77	244	2017-07-05 02:08
Eaveo Recording Company	1.09 in 9 prefixes	750	30	19	9	2017-07-05 02:08
Isova Football Club	0.06 in 1 prefix	800	7	340	23	2017-07-05 02:08
Coragen Fitness World	12.01 iin 7 prefixes	510	300	1	38	2017-07-05 02:08

Enterprise Security Scoring – Key Highlights

Empirical

- ✓ Leverages an extensive array of **analytic techniques**
- ✓ **Supervised** modeling approach correlates signals with real outcomes
- ✓ Evaluates both **condition** *and* inferred **behavior**
- ✓ An **empirically-derived** benchmark of cyber risk, rather than an opinion-based ranking

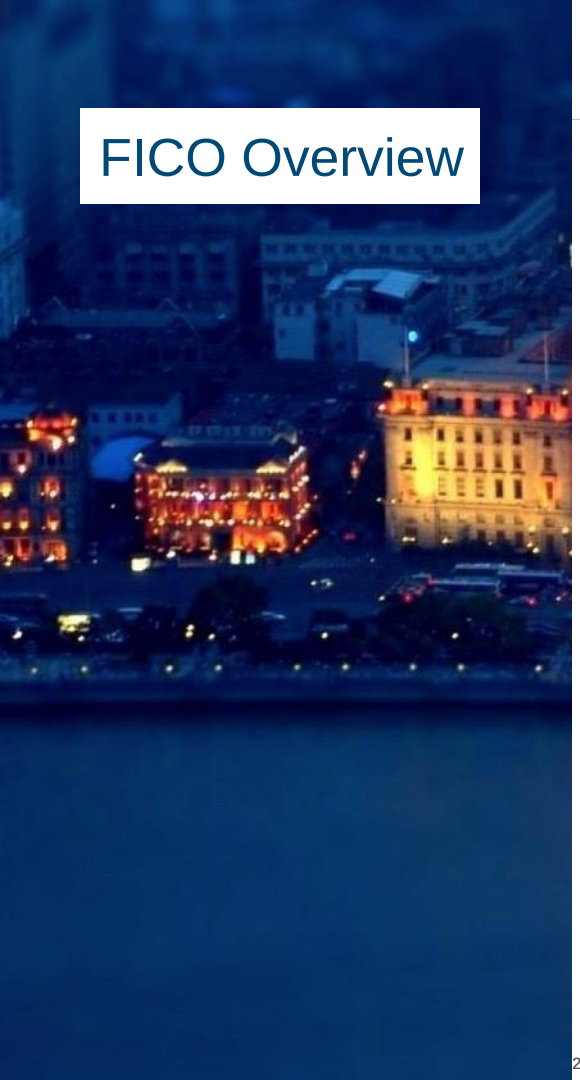
Predictive

- ✓ Predictive model focuses on **future outcomes** rather than transient threats
- ✓ Visibility into enterprise security behaviors to **mitigate future potential failures**
- ✓ Aligns to **forward-looking** business objectives and outcomes

Actionable

- ✓ **User controls** scope of analysis and definition of enterprise
- ✓ Enables **sharing** and **collaboration**
- ✓ Integrates with ticketing and workflow systems for systematic **remediation**
- ✓ NIST controls cross-reference supports **compliance** initiatives

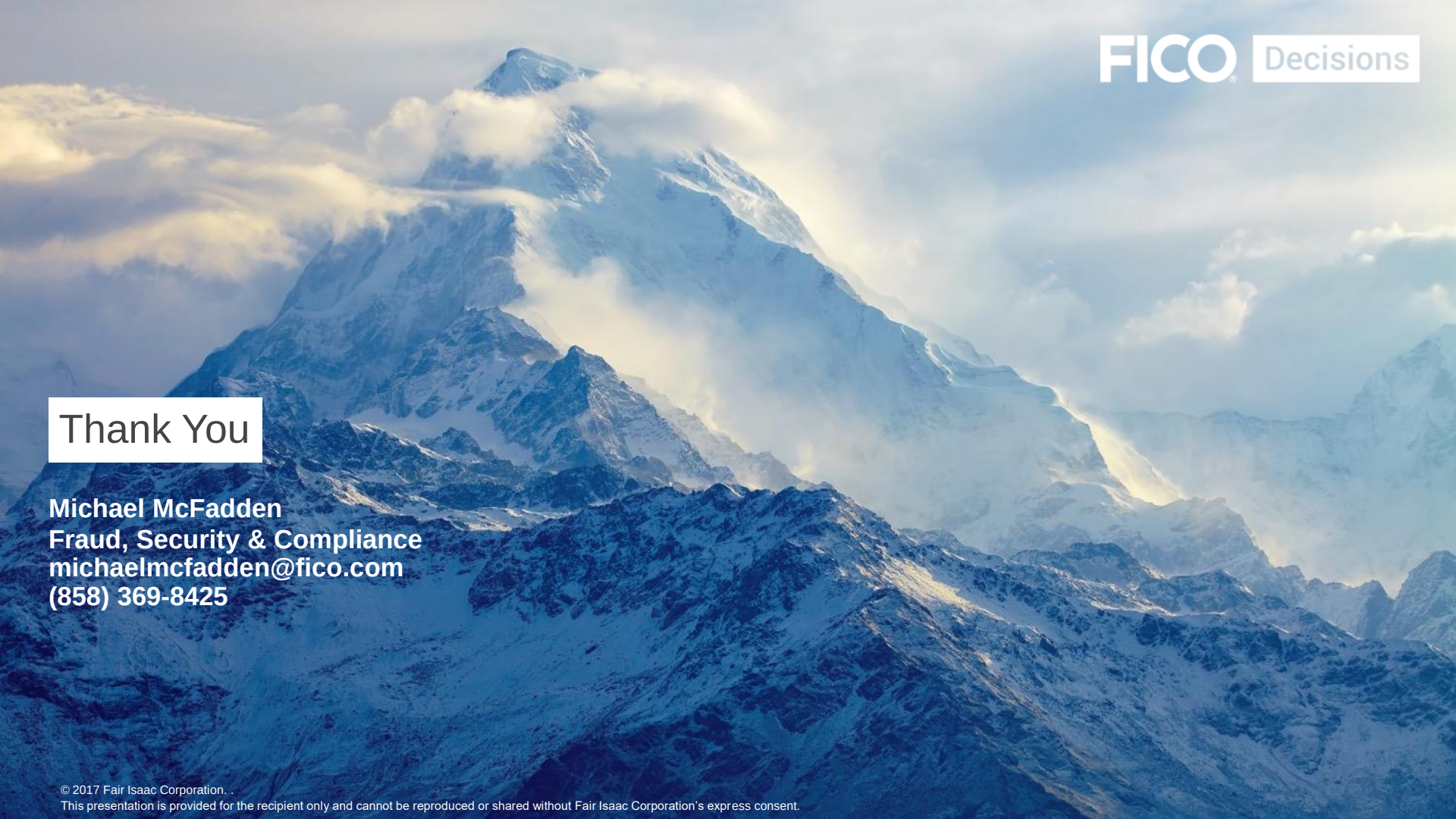
Inform, Predict Odds of Breach, Remediate, Repeat



FICO Overview

FICO Decisions

Profile	The leader in advanced analytics and decision management Founded: 1956 • NYSE: FICO / $881M revenue FY2016 • Analytics and decision management systems • Reducing the time from insight to action
Products and Services	• FICO Scores – used for 96% of US credit underwriting • Predictive analytics for risk management • AI systems for security threat and fraud detection • Advanced analytics for cyber risk quantification • Tools for analytics authoring and decision management
Clients and Markets	10,000+ clients in 90+ countries Industry focus: Banking, government, insurance, logistics
Offices	20+ offices worldwide, HQ in San Jose, California 3,100 employees Regional Hubs: San Rafael and San Diego (CA), New York, London, Birmingham (UK), Johannesburg, Milan, Moscow, Bensheim, Munich, Madrid, Istanbul, Sao Paulo, Bangalore, Beijing, Singapore



Thank You

Michael McFadden
Fraud, Security & Compliance
michaelmcfadden@fico.com
(858) 369-8425