FICO Decisions

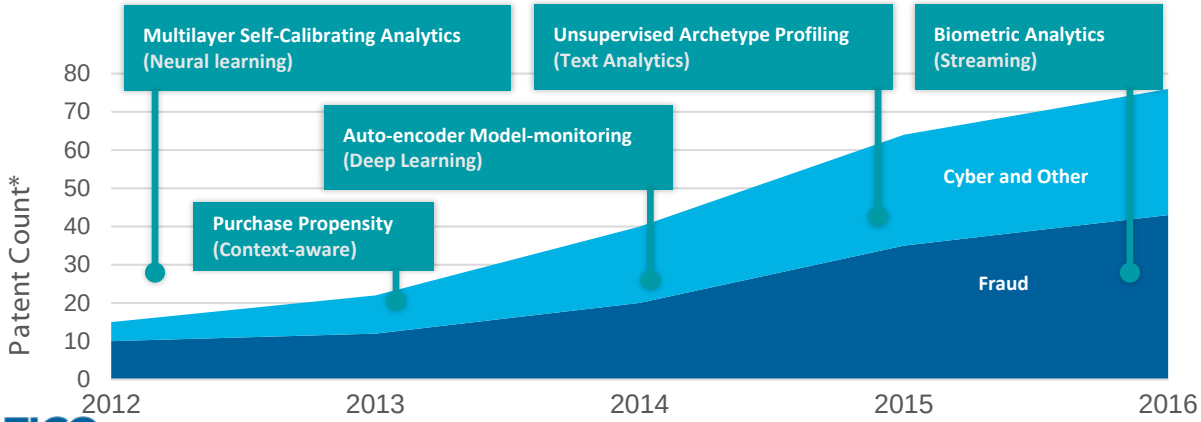
Predicting likelihood of cyber breach by analyzing external security posture of enterprises

Scott M. Zoldi, Ph.D.
Chief Analytics Officer
FICO

@ScottZoldi

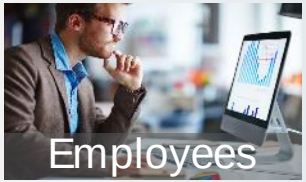
Scott Zoldi, PhD – Chief Analytics Officer

- 18 years at FICO
- Guide analytic development, across Fintech, Fraud, AML, Retail, Insurance, Healthcare, Cyber-security and IoT.
- Author of 79 patents (*39 granted and 40 in process)*
- New initiatives in Machine Learning and Streaming Analytics
- Recent focus on self learning analytics for real-time detection of Cyber attacks and mobile device analytics



*Includes published and filed

Cyber security threats: Everyone is a target and every vulnerability is exploited!



Vulnerability

Skim / Highjack

SS7 / DDoS

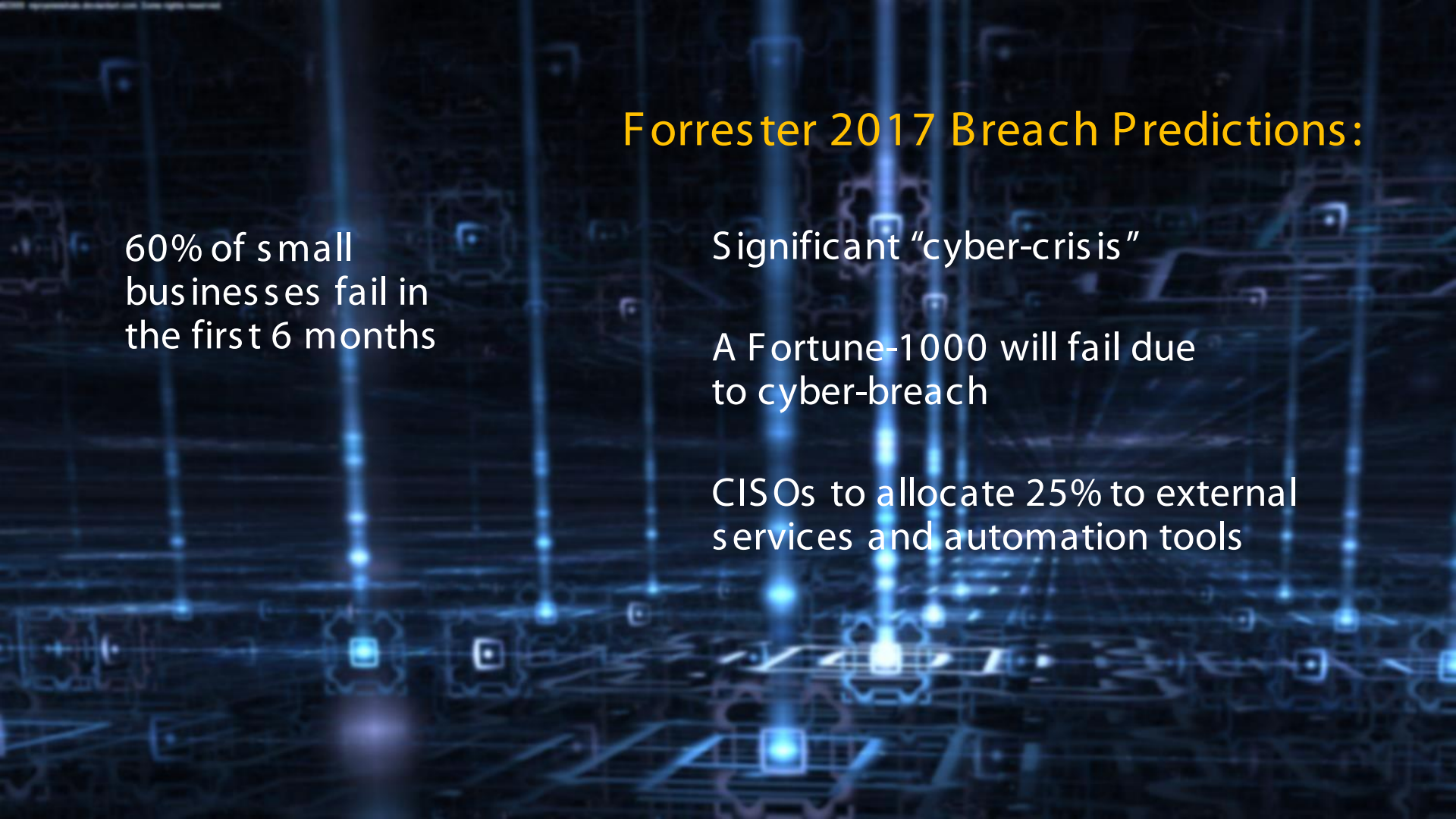
Breach / Skim

Phishing

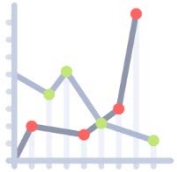
Fake Apps

Obfuscation / Delay

DNS Redirection


Forrester 2017 Breach Predictions:
60% of small businesses fail in the first 6 months
Significant “cyber-crisis”
A Fortune-1000 will fail due to cyber-breach
CISOs to allocate 25% to external services and automation tools

What is facilitated by Cyber Risk Score



Quantifies how an organization appears to a cyber criminal

A single, easily interpreted, commonly understood score of an organization's potential breach risk – a reference metric used enterprise-wide: Board of Directors, CEO, CISO, and security professionals alike.

Inform breach insurance underwriting process

Ascertain security risk of partner organizations and the vendor supply chain

Cyber Risk – Leveraging a Credit Risk Playbook

FICO® SCORE | 25 YEARS

90% Top lenders using FICO® Scores when making lending decisions

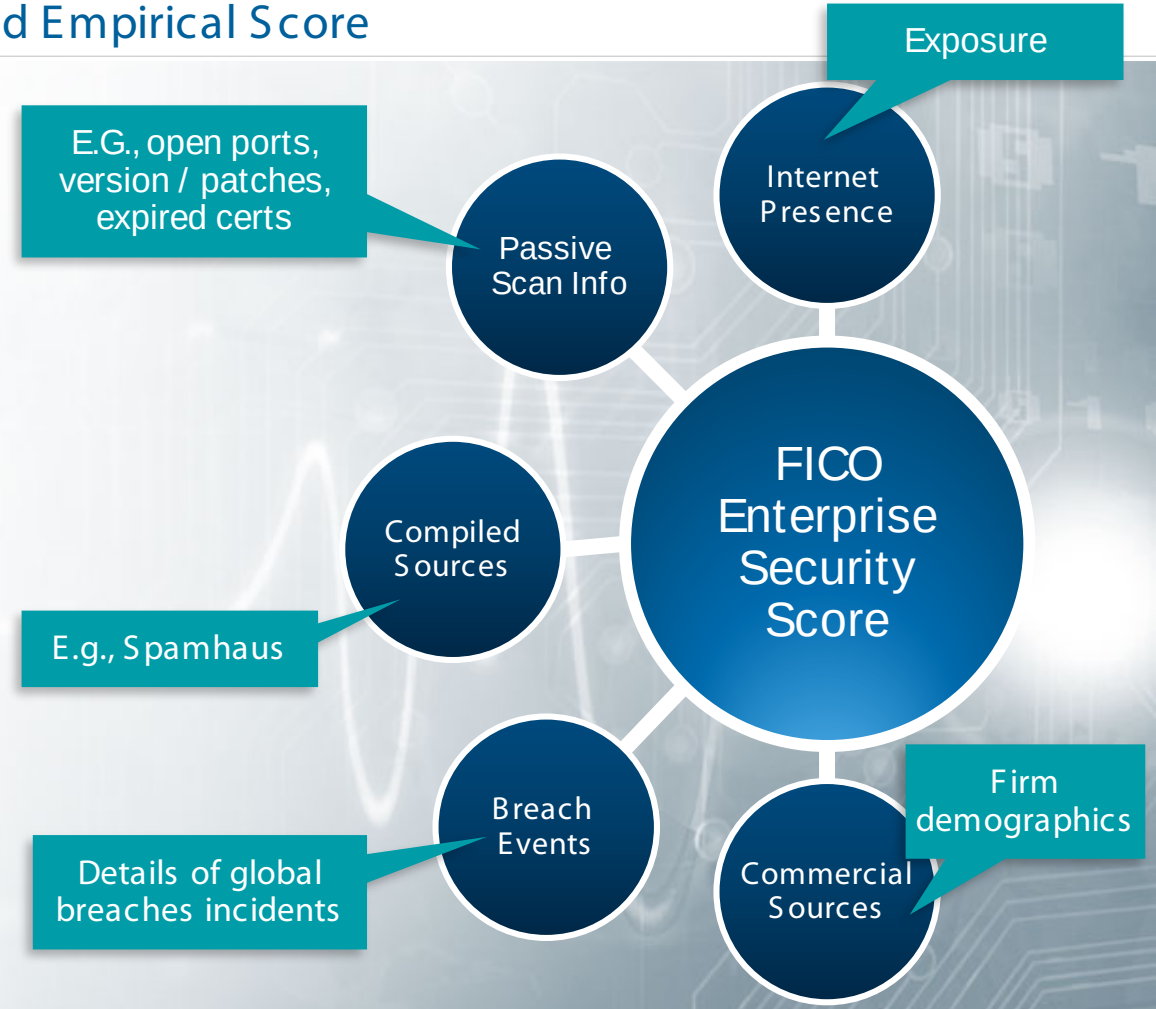
10B FICO Scores purchased in US annually

70K Businesses that rely on the FICO Score

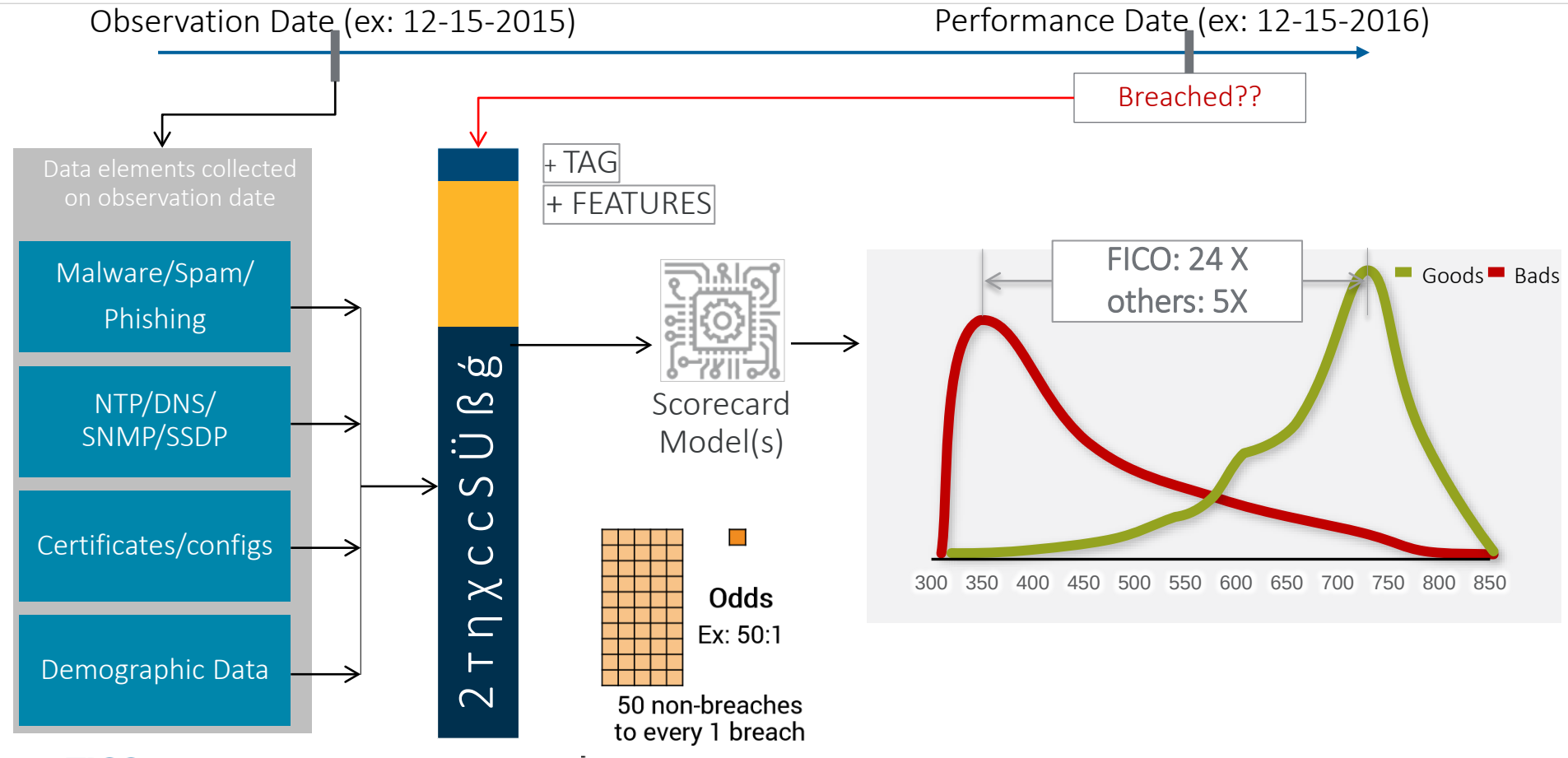
20 Countries where the FICO Score is deployed

ESS Delivers a Passively Obtained Empirical Score

- Millions of data elements continually monitored at internet scale
- Historical depth to reflect security posture of breached networks prior to the incident
- Measurements that serve to assess policy effectiveness and management behaviors
- Data richness that supports empirical analysis, not judgment-based grades



Cyber Breach Risk: Building an Empirical Model



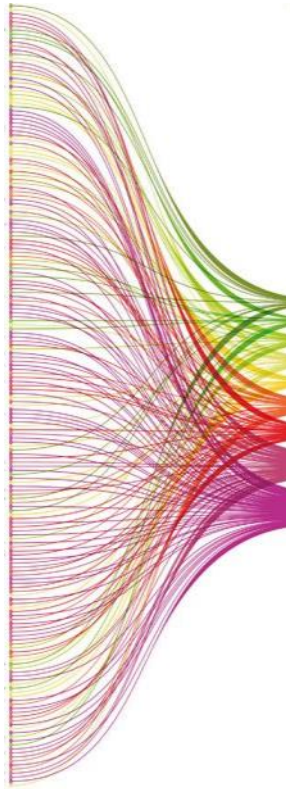
Data Collected; Operationalized via Score and Reason Codes

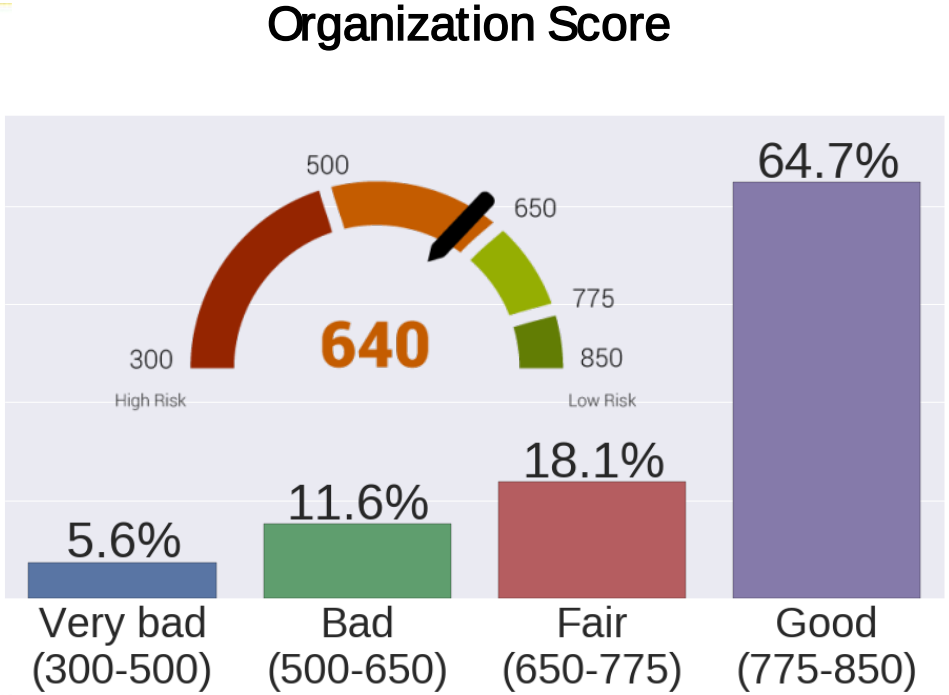
Three categories of monitored issues with corresponding reason codes

Endpoint Security
Malware/ Spam/ Phishing

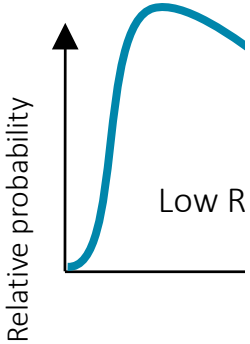
Infrastructure Security
NTP/ DNS/ SNMP/ SSDP

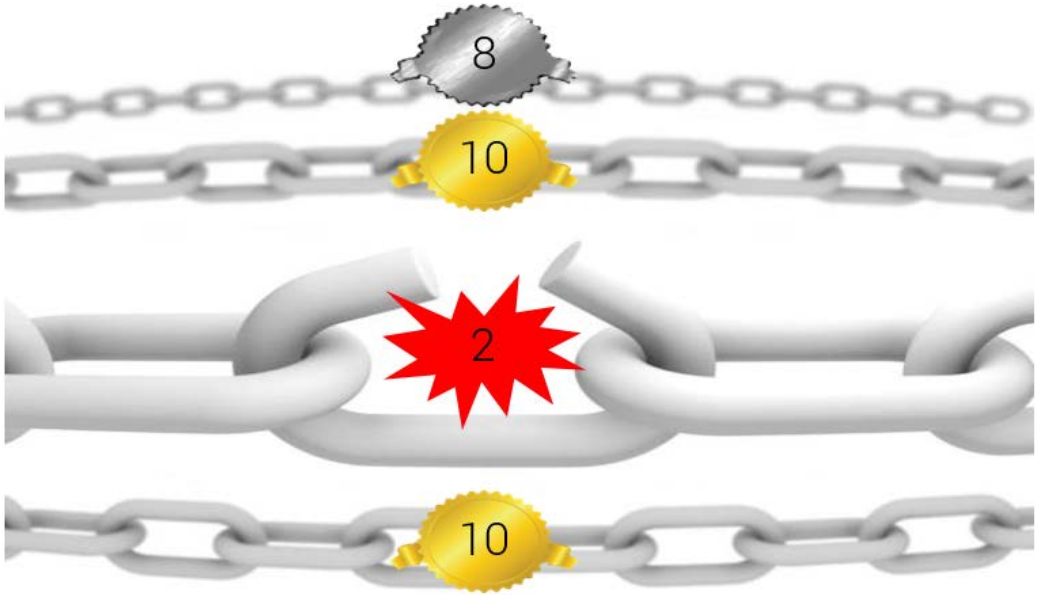
Services & Software
Certificates/ Configurations





Does Size Matter? Identification of Riskiest Network Assets





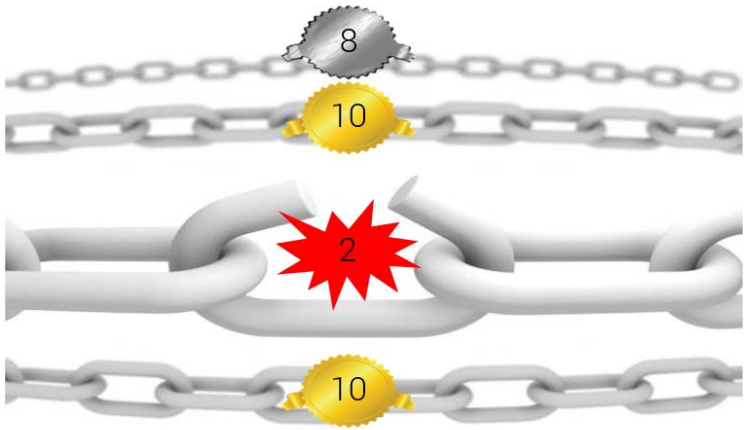
Multi-Layer Self Calibrating Score

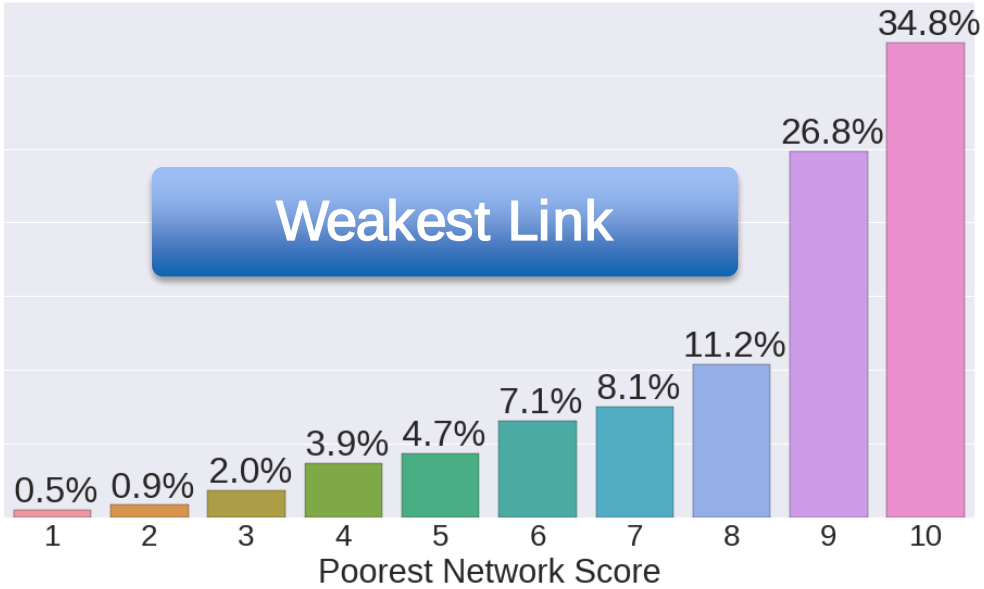
$$q(x_i \mid s) =$$

Security posture of the organization informed by its weakest link using patent-pending technology

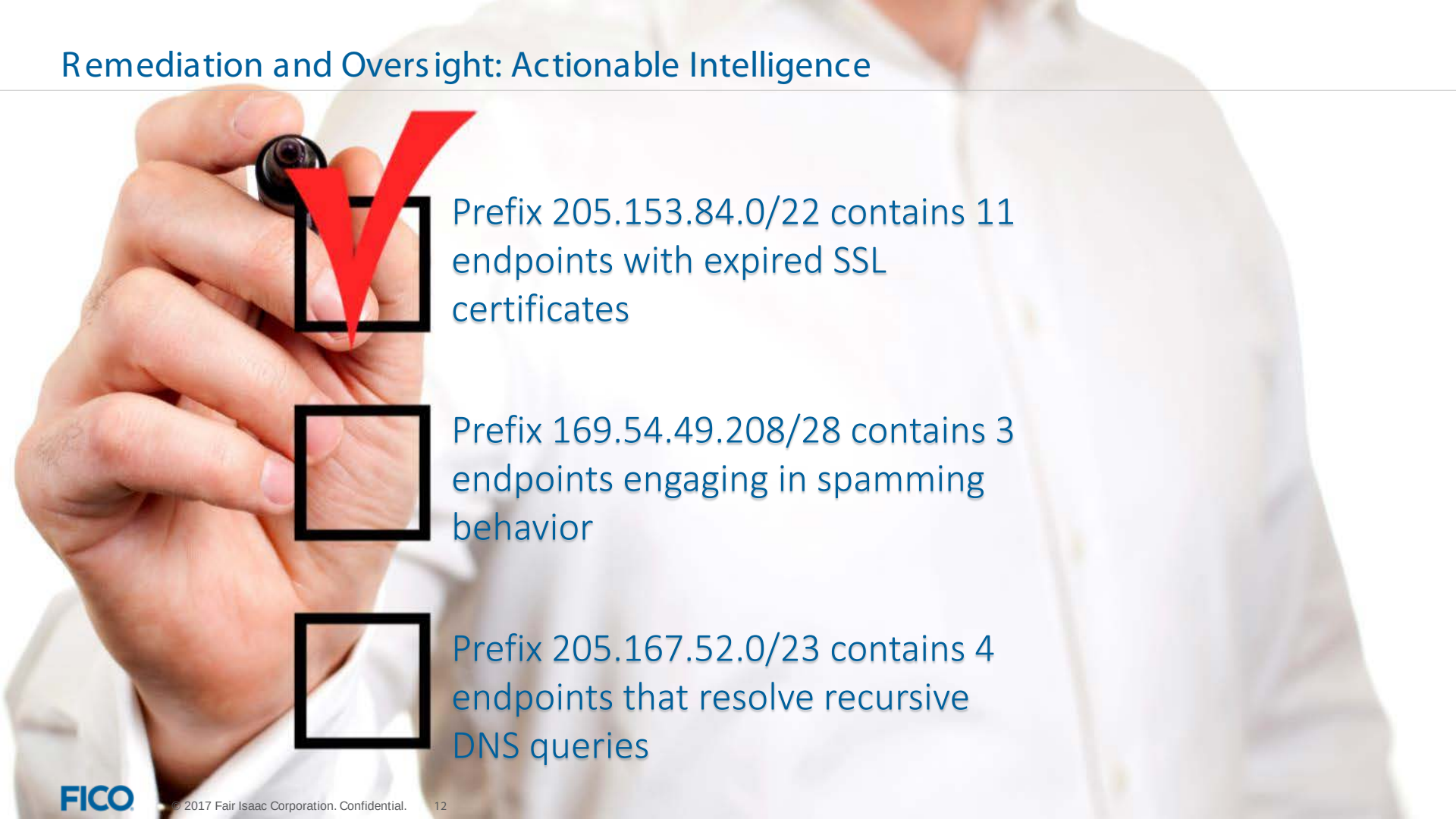
US Patent 8,027,439; 8,041,597; 13/367,344; 15/463,420

Asset scoring and remediation : Where's my weakest links





Remediation and Oversight: Actionable Intelligence



- Prefix 205.153.84.0/22 contains 11 endpoints with expired SSL certificates
- Prefix 169.54.49.208/28 contains 3 endpoints engaging in spamming behavior
- Prefix 205.167.52.0/23 contains 4 endpoints that resolve recursive DNS queries

1. **A single risk metric**: ESS continuously quantifies the likelihood of a future data breach

2. **Utility**: In addition to breach prediction, ESS can be used to inform the breach insurance underwriting process

3. **Liability**: Know your vendors' and partners' risk along the entire vendor supply chain prior to data exchange

Thank you!

Scott M Zoldi

Chief Analytics Officer, FICO

@ScottZoldi