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

![Graph showing patent count across different categories from 2012 to 2016.

- Multilayer Self-Calibrating Analytics (Neural learning)
- Unsupervised Archetype Profiling (Text Analytics)
- Biometric Analytics (Streaming)
- Auto-encoder Model-monitoring (Deep Learning)
- Purchase Propensity (Context-aware)
- Fraud
- Cyber and Other

*Includes published and filed
Cyber security threats: Everyone is a target and every vulnerability is exploited!
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-breaches
- 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
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

**FICO Enterprise Security Score**

- **Internet Presence**
- **Compiled Sources**
- **Breach Events**
- **Commercial Sources**
- **Passive Scan Info**
- **Details of global breaches incidents**
- **E.g., Spamhaus**
- **Firm demographics**
- **Exposure**

E.G., open ports, version / patches, expired certs

Commercial Sources

Breach Events

Compiled Sources

Passive Scan Info

Internet Presence

Exposure

Firm demographics

Details of global breaches incidents

E.g., Spamhaus

Exposed

E.G., open ports, version / patches, expired certs
Cyber Breach Risk: Building an Empirical Model

Data elements collected on observation date:
- Malware/Spam/Phishing
- NTP/DNS/SNMP/SSDP
- Certificates/configs
- Demographic Data

Observation Date (ex: 12-15-2015) → + TAG + FEATURES → Scorecard Model(s) → Performance Date (ex: 12-15-2016)

Breached??

Scorecard Model(s)

FICO: 24 X others: 5X

300 350 400 450 500 550 600 650 700 750 800 850

Goods Bads

Odds Ex: 50:1

50 non-breaches to every 1 breach
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

![Organization Score Graph]

- Very bad (300-500): 5.6%
- Bad (500-650): 11.6%
- Fair (650-775): 18.1%
- Good (775-850): 64.7%
Does Size Matter? Identification of Riskiest Network Assets

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
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