
# Session 7: Cyber Risk Management: From the Inside and the Outside

## Moderator:

## Presenters:

Ross Albert

Damon D Levine

# *A Holistic Approach to Cyber Risk Management*

**Damon Levine, CFA, ARM, CRCMP, Open FAIR**
***Director, Focal Point Data Risk***

**ERM Symposium April 19, 2018**

FOCAL POINT
DATA RISK

**Disclaimer:**

*The views expressed herein are those of the presenter and not necessarily those of Focal Point Data Risk*

# Today's Goal: Pragmatism vs. *This…*

"Incidence response requires both situation awareness and tiered remediation actions for proportional response. Workflow is task-oriented and requires real-time alert correlation, activity log analysis, traffic capture and analysis, and suspect file detonation for security analysts to perform deep-dive evidence analysis to reach decisive conclusions. The variety of specialized multi-vendor security tools, a frictionless integration surface and ease of use with an economy of clicks is essential for total remediation at the 'compromised network' and 'infected system' level to restore normalcy and trustworthiness of operations."

***Written by AI Program?***

*- http://www.taasera.com/blog/cyber-security-essentials-enterprise-risk-management*

# What Did the “AI Writer” Get Right?

- Situational awareness: understanding exposures across LOBs, locations, & functions
- Real-time detection and response: “awareness-to-action” speed is of the essence
- Practical remediation: time, expense, and the human element
- Risk-informed decisions: risks to business objectives, including protections against downside are critical (e.g. $, reputation, operations)

# Situational Awareness

- ERM's (vaunted) *portfolio view*: because cyber risks may be correlated and/or linked causally, one needs an enterprise view of risk across:
  - LOBs, locations, products, and,
  - strategic execution, compliance, regulatory, privacy, and (other) operational risks

- Many organizations do not have an accurate, comprehensive view of their IT assets, vendors, and other third parties that can expose the company to IT risks; an organizational intelligence is needed to address these visibility challenges and leverage them in decision-making

- ERM emphasizes a risk ID and reporting mechanism which delivers: prompt and actionable information for risk prevention and/or post-event containment

# Need for Portfolio View

"As the number of connected things has grown, so has the determination of cybercriminals to exploit them. Businesses might not think about the cybersecurity settings of their photocopiers, for instance, yet 2016's Mirai malware used hundreds of thousands of IoT devices to create a botnet that took down popular proxy server Dyn and, with it, nearly one third of websites globally" – Cara Sloman, Executive Vice President, Nadel Phelan, Inc

# Technology-forward Cyber Risk Management




FOCAL POINT DATA RISK

# Business-back Cyber Risk Management




FOCAL POINT DATA RISK

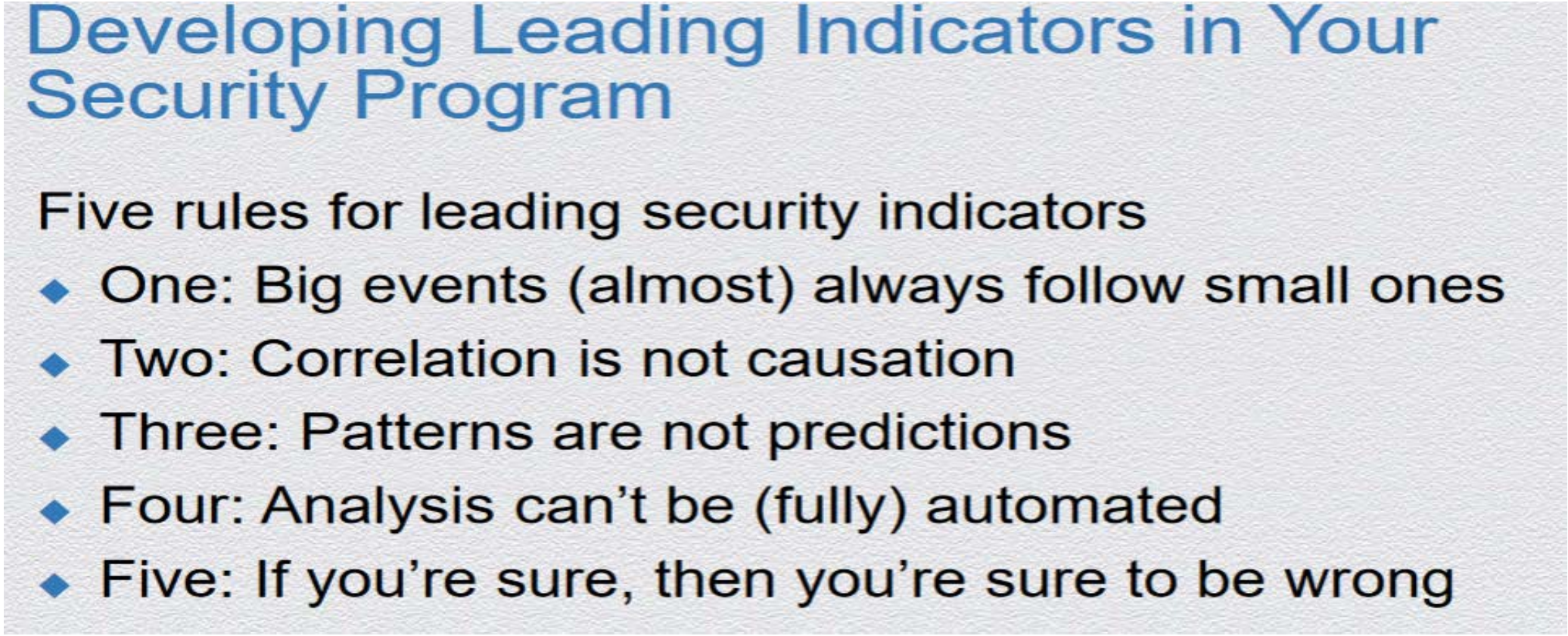
# Obsolescence of the Traditional Cyber Risk Approach

| Approaches to Cyber Risk Management | |
|---|---|
| ***Traditional/Obsolete*** | ***Leading Practice*** |
| Compliance-focused | Value/strategy focused |
| Backward-looking | Forward-looking |
| Reactive | Proactive |
| Parallel/Siloed | Portfolio View/Correlation-aware |
| Technology-forward | Business-back |

# Measurement in ERM: the Primary Decision Driver

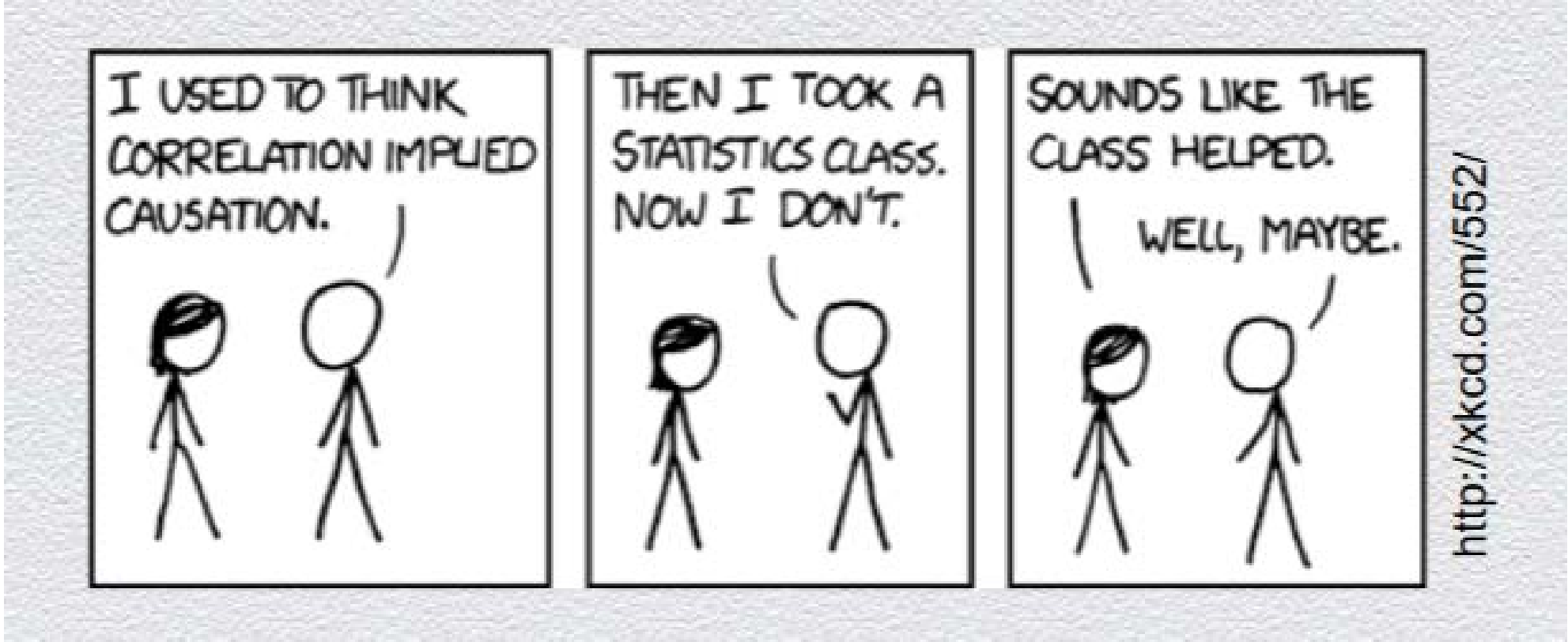
- From colors to dollars: “soft” or qualitative scales do not aggregate or compare effectively, and therefore, do not enable informed decisions
- Leading vs. lagging KRIs, dollar metrics (e.g. GAAP/STAT earnings, capital, ROE, distributable earnings, company value)
- Risk appetite/limit reporting, and remediation protocol
- Metric-driven culture

# Caveats on KRI




https://www.rsaconference.com/writable/presentations/file_upload/trm-w07-one-failure-leads-to-another-developing-leading-indicators-for-security-threats-and-risks-final.pdf

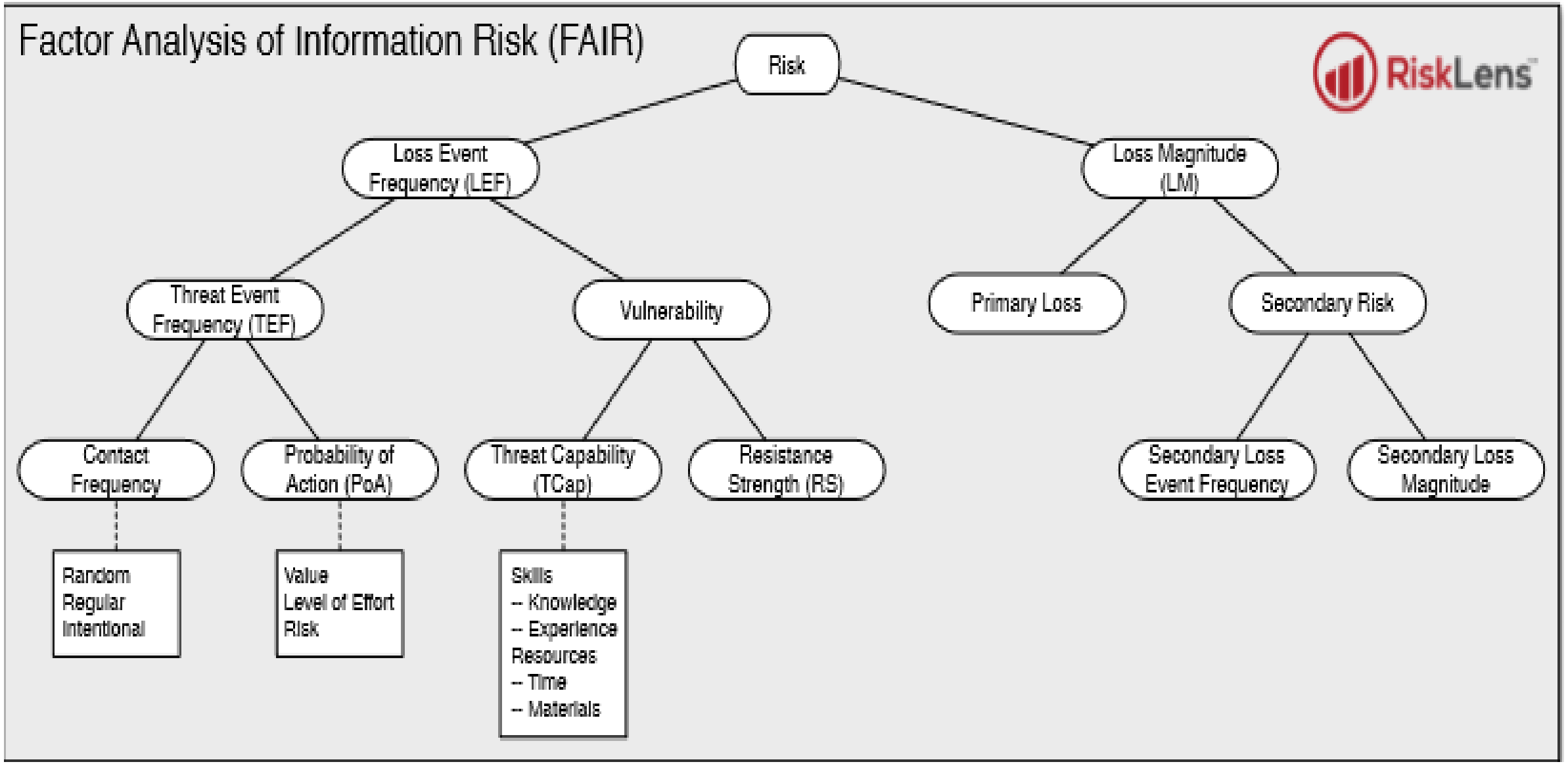
# Something for the Actuaries…






FOCAL POINT DATA RISK

# Dollar Quantification of Cyber Risk: FAIR Approach






FOCAL POINT DATA RISK

# Further Support for an Enterprise Risk Approach

- Complexity, human element, and malicious incentives drive a chaotic and rapidly evolving cyber risk profile & attack surface

- Cyber risks are therefore: difficult to effectively identify and quantify, challenging to avoid, and intertwined with previously unrelated risk exposures

- Critical operational risk events can set in motion a chain of adverse consequences including loss of business continuity, revenue loss, fines, litigation, and brand/reputational damage

# Practical Prevention of Pervasive People Problems


- The human element is a significant challenge: we all want to click things
- Tap into natural human ego and laziness: 1) test reactions and score by department, 2) make things as simple as possible, but not simpler



FOCAL POINT DATA RISK

# Walking the Walk

- Massive policies and onerous SOPs may be comprehensive but will they be followed?
- Consider tension between IT risk priorities and “*business*" objectives
- If compliance with internal guidelines is a lengthy process, you may end up with “shadow risk management” tools




FOCAL POINT DATA RISK

# Hallmarks of an ERM Approach

- Cybersecurity governance
- Executive/leadership support and defined roles and responsibilities
- Principle of least privilege
- Creation of processes, policies, and standards; linked across the company
- Inventory of IT assets and the portfolio view
- Risk ID and remediation (including identification and protection of your ‘crown jewels’)
- Quick response/containment to security events and incidents
- Continuous learning and adaptation to the threat landscape
- Pragmatic use of risk appetite/limit notions

# The 4S's of the Board: Synergies, Schooling, Survival, and Satisfaction

- The Board needs verifiable proof of robust cyber risk management and those in IT risk management can leverage this to their benefit
  - The Board's oversight role for risk controls and their typical focus on cyber can be leveraged to improve risk ID, assessment, and messaging
  - Most Board members need quantification which relevant and non-technical; the metrics useful to ERM (e.g., earnings, cashflow, ROE, etc.) should be used for cyber
- Education of a stakeholder is often a key foundation for effectively conveying the critical messages of your risk analysis
- Because they have investor interests in mind (not just company "survival"), Boards will view risk management as a tool to drive performance and an asset view (business-back) of cyber will resonate

# What Trump and Obama Have in Common? Golf *and …*

# NIST-CSF

- **Identify**: Use organizational understanding to minimize risk to systems, assets, data and capabilities.
- **Protect:** Design safeguards to limit the impact of potential events on critical services and infrastructure.
- **Detect:** Implement activities to identify the occurrence of a cybersecurity event.
- **Respond:** Take appropriate action after learning of a security event.
- **Recover:** Plan for resilience and the timely repair of compromised capabilities and services.

# NIST Implies a Holistic View

| *NIST Theme* | *Rationale for an Enterprise Approach* |
|---|---|
| Identify | *to assess/prioritize exposures, it is necessary to see aggregation/correlation of risk* |
| Protect | *managing risk requires full understanding of causality, correlation, and linkages* |
| Detect | *detection is most effective through a collective, organizational awareness* |
| Respond & Recover | *breach remediation and business continuity planning rely on an enterprise preparedness* |

# Is NIST *it* for IT?!

According to Gartner, more than 50 percent of U.S.-based organizations will use the NIST Cybersecurity Framework by 2020, up from 30 percent in 2015. Recently, President Donald Trump issued a cybersecurity executive order that directs all agencies to adopt and use the framework to address their enterprise risk management posture.

https://fcw.com/Articles/2017/07/25/CIO-perspective-ERM-cyber-Spires.aspx?m=2&Page=2

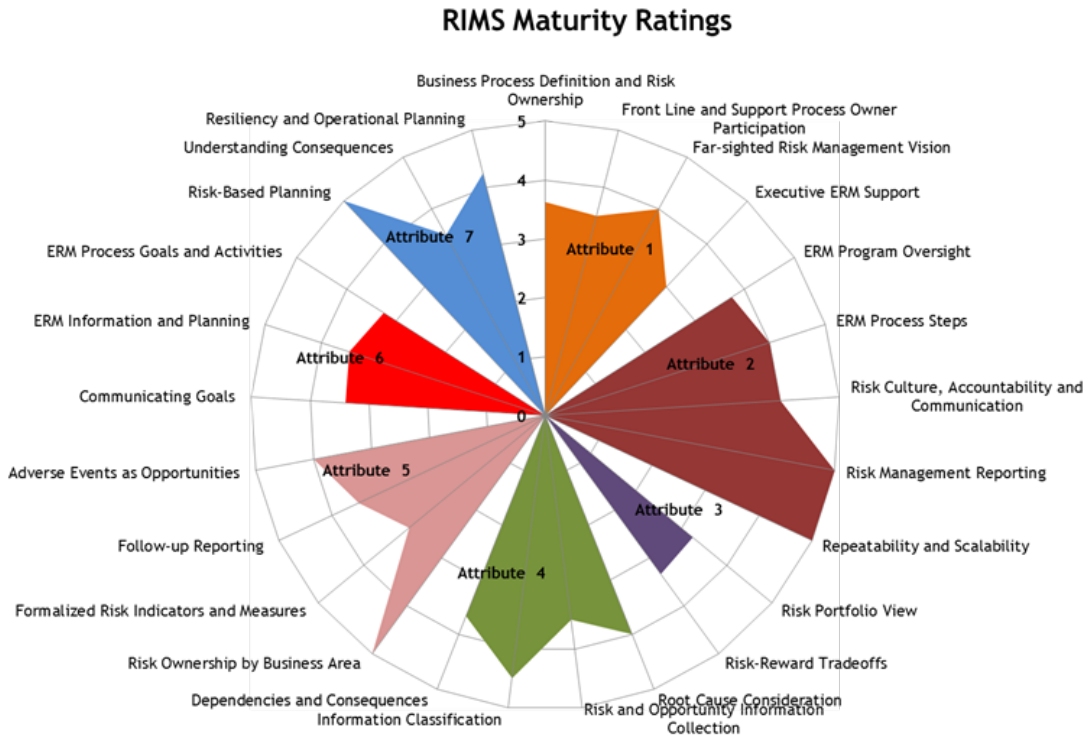
# Holistic (Cyber) Health

- The limitations of vaccination

- Wellness
  - Educated Employees
  - Advanced Prevention
  - Faster Recovery

# Adapting the RIMS Risk Maturity Model (RMM)

| 7 Key Attributes | 25 Competency Drivers |
|---|---|
| Adoption of ERM-based Approach | Business Process Definition and Risk Ownership |
| | Front Line and Support Process Owner Participation |
| | Far-sighted Risk Management Vision |
| ERM Process Management | Executive ERM Support |
| | ERM Program Oversight |
| | ERM Process Steps |
| | Risk Culture, Accountability and Communication |
| | Risk Management Reporting |
| | Repeatability and Scalability |
| Risk Appetite Management | Risk Portfolio View |
| | Risk-Reward Tradeoffs |
| Root Cause Discipline | Root Cause Consideration |
| | Risk and Opportunity Information Collection |
| | Information Classification |
| | Dependencies and Consequences |
| Uncovering Risks | Risk Ownership by Business Area |
| | Formalized Risk Indicators and Measures |
| | Follow-up Reporting |
| | Adverse Events as Opportunities |
| Performance | Communicating Goals |
| | ERM Information and Planning |
| | ERM Process Goals and Activities |
| Resiliency and Sustainability | Risk-Based Planning |
| | Understanding Consequences |
| | Resiliency and Operational Planning |






FOCAL POINT DATA RISK

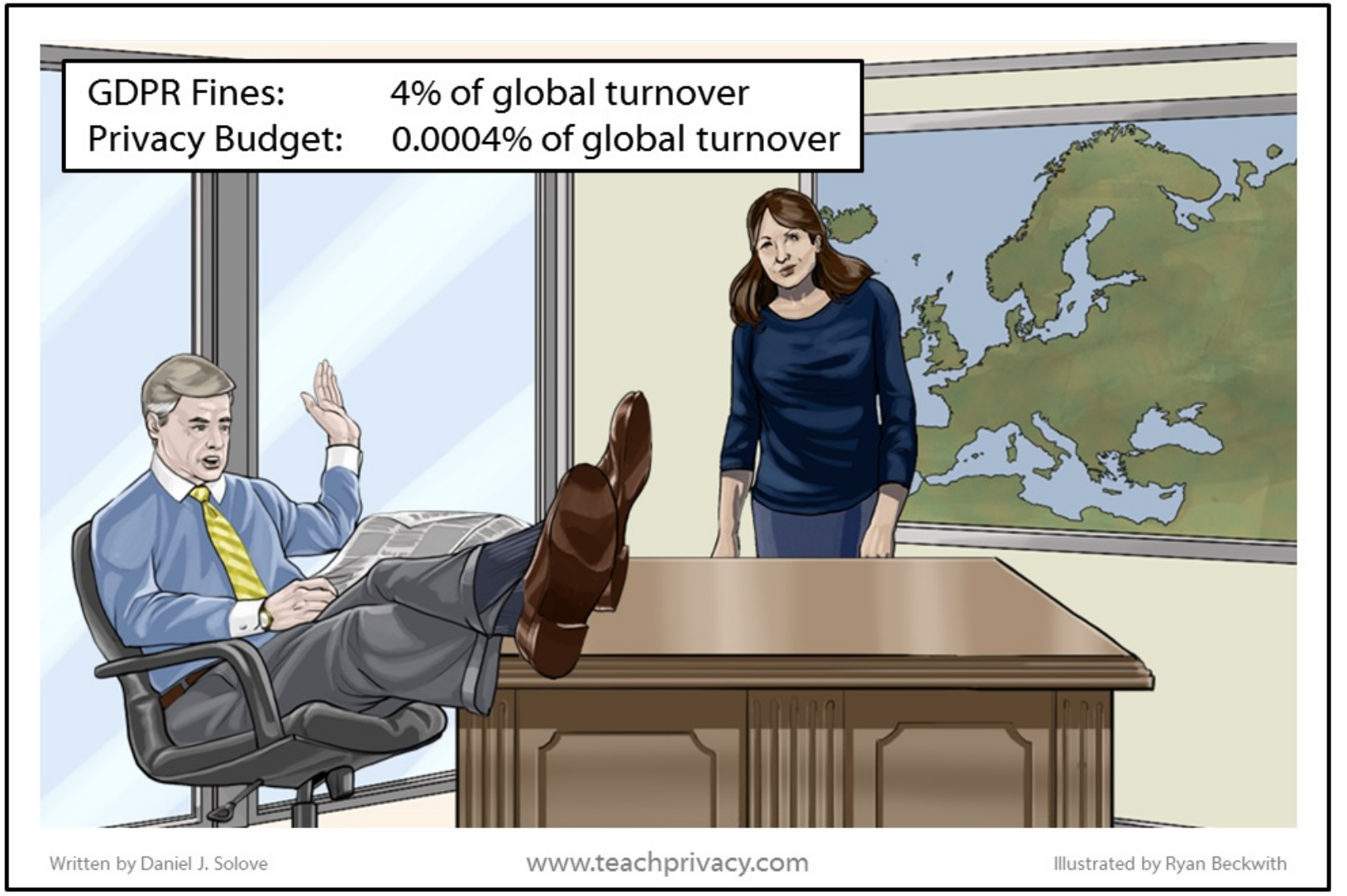
# Strategic Context

- Treating cyber risk apart from other business risks renders it overly technical, mysterious and separate

- Placing it in a strategic context shows how cyber risk relates to other risks. It also shows how management's acceptance of specific cyber risks will assist — or fail to assist — in creating value

- Enables senior managers to define and align their interests and roles in cyber risk management, leading to informed cyber risk response decisions

# oh yeah…GDPR






FOCAL POINT DATA RISK

# Additional Cyber Risk Management Reading

- https://cyberbalancesheet.com/
- https://focal-point.com/services/advisors/audit-and-advisory/enterprise-risk-management
- https://www.linkedin.com/pulse/nobody-expects-spanish-inquisition-gdpr-you-damon/
- http://ermvalue.com/

# References


- https://www.cfoinnovation.com/white-paper/12360/taking-aim-cyber-risk
- http://www.isaca.org/cyber/cyber-security-articles/Pages/maintaining-a-holistic-risk-based-cybersecurity-program.aspx?utm_referrer=
- https://www.cybrary.it/0p3n/holistic-risk-based-approach-cybersecurity/
- https://www.darkreading.com/vulnerabilities---threats/a-holistic-approach-to-cybersecurity-wellness-3-strategies/a/d-id/1326120?