BUSINESS of SECURITY



Laying a FAIR Foundation For Risk Based Security Management

By: Michael Radigan Presented to: 9/18/13





Management doesn't care about security... They care about risk

Laying a FAIR Foundation for RBSM

AGENDA

- Bald Tire Scenario
- What is "FAIR"?
- Where FAIR Fits In
- The FAIR Taxonomy
- FAIR Risk Analysis Example BYOD
- The Open Group FAIR Analyst Certification
- Q&A

Risk Analysis: Bald Tire Scenario

How much risk is there?

0 = None 10 = Severe



Identify the:

- * Threat
- * Vulnerability
- * Asset
- * Risk

Risk Analysis: Bald Tire Scenario



www.dwaynesworldsecurity.com

Points of Discussion

- 1) Assumptions
- 2) Terminology
- 3) High value/high risk correlation
- 4) Equating vulnerability with risk



What is FAIR?

Factor Analysis of Information Risk

Ground Breaking Discovery

- Describes how key elements of the risk landscape work
 Clearly Defines the Problem Space
- Standard nomenclature
- Risk model and taxonomy

Discipline and Methodology

- A framework for critical thinking
- A method for measuring the factors that drive risk
 Computational Engine
- Mathematical simulation of the relationship btwn factors
 Simulation Model
- Build and analyze risk scenarios

Laying a FAIR Foundation for RBSM

AGENDA

- Bald Tire Scenario
- What is "FAIR"?
- Where FAIR Fits In
- The FAIR Risk Taxonomy
- FAIR Risk Analysis Example BYOD
- The Open Group FAIR Analyst Certification
- Q&A

Nicolaus Copernicus Observation of the Universe



FAIR

Factor Analysis of Information Risk



FAIR is referenced in the PCI DSS **Risk Assessment Guidelines**



Certification for FAIR Analyst in Nov 2013



Recognized FAIR as an established risk assessment methodology FAIR inventor Jack Jones awarded 2012 CSO Compass Award

What FAIR is Not ...

FAIR is not a Risk Management Framework

The Open Group Technical Standard: FAIR – ISO/IEC 27005 Cookbook (this document) describes in detail how to apply the FAIR (Factor Analysis for Information Risk) methodology to any selected risk management framework. It uses ISO/IEC 27005 as the example risk assessment framework. FAIR is complementary to all other risk assessment models/frameworks, including COSO, ITIL, ISO/IEC 27002, COBIT, OCTAVE, etc. It provides an engine that can be used in other risk models to improve the quality of the risk assessment results.

http://www.opengroup.org/subjectareas/security/risk

FAIR is ... Risk Quantified \$\$\$

FAIR is a set of analytic models for performing Quantitative Risk Analysis and deriving a financial representation of risk (loss exposure).

FAIR enables Risk Based Security Management

"... where RBSM is defined as the application of rigorous and systematic analytical techniques to the evaluation of the risks that impact an organization's information assets and IT infrastructure."

http://www.tripwire.com/ponemon2012/

Laying a FAIR Foundation for RBSM

AGENDA

- Bald Tire Scenario
- What is "FAIR"?
- Where FAIR Fits In
- The FAIR Risk Taxonomy
- FAIR Risk Analysis Example BYOD
- The Open Group FAIR Analyst Certification
- Q&A



QUANTITATIVE RESULTS SUMMARY

Annualized Loss Exposure Current State vs. Proposed State:

		Minimum	Average	Mode	Maximum
	Current State	\$1,000,000	\$13,500,000	\$10,000,000	\$40,000,000
	Proposed State	\$10,000	\$4,500,000	\$1,400,000	\$32,000,000

Implementing [product name] is expected to reduce the annualized loss exposure by \$9M (average). At a total cost of ownership of less than \$1M, this implies a benefit to cost ratio of 9-to-1.

Annualized Loss Exposure

Current State:



Proposed State (with advanced anti-malware):



Laying a FAIR Foundation for RBSM

AGENDA

- Bald Tire Scenario
- What is "FAIR"?
- Where FAIR Fits In
- The FAIR Risk Taxonomy
- FAIR Risk Analysis Example BYOD
- The Open Group FAIR Analyst Certification
- Q&A

The Open Group Technical Standard Risk Taxonomy



FAIR enables Technical Analysts to communicate with Business Analysts

Laying a FAIR Foundation for RBSM

AGENDA

- Bald Tire Scenario
- What is "FAIR"?
- Where FAIR Fits In
- The FAIR Risk Taxonomy
- FAIR Risk Analysis Example BYOD
- The Open Group FAIR Analyst Certification
- Q&A

Analysis Process

- Define (model) the scenario
 - Basic conditions and assumptions
- Gather data & estimates
 - Document sources, rationale, and assumptions
 - Refine the scenario definition (if necessary)
- Derive risk

Define and Model the Scenario

What are we trying to prevent?

- Compromise of customer information
- Compromise of corporate information
- Financial fraud
- Other ...?

How might the loss occur?

- Loss/theft of the device
- Malware compromise
- Transmission interception
- Other ...?

Scenario Table

	Device Loss/Theft	Malware Compromise	Transmission Interception
Customer information	Х		
Corporate information			
Money (financial fraud)			

- Additional considerations...
 - -BYOD access will be limited to e-mail
 - Differentiate by type of device (e.g., iOS vs Android)?
 - Differentiate with/without an MDM solution?

Gathering Data

- What variables do we need to find data for?
 - Loss event frequency (or threat event frequency and vulnerability)
 - Primary loss
 - Secondary loss
 - Secondary loss event frequency
 - Secondary loss magnitude



• What data do we have?

- Loss history (frequency, impact, control conditions)
- Surface area and volume of PII at risk
- Control conditions
- The magnitude of loss when/if PII is compromised

Analysis Input



- Loss event frequency
 - 15 lost/stolen devices per year from a population of 1200 corporate devices (device surface area)
 - The number of BYOD devices is expected to be between 1200 and 1300 (includes conversions from corp to personal)
 - Estimated BYOD loss event frequency
 - Min: 10 yr
 - Max: 25 yr
 - Most likely: 18 yr



Analysis Input



- * Asset surface area
 - Review of sensitive customer information in e-mail found:
 - 7% of colleagues had sensitive customer information in e-mail
 - The volume of sensitive customer information per colleague:
 - Min: 1 sensitive record
 - Max: 50,000 sensitive records (spreadsheets)
 - Mode: 35 sensitive records
 - These values play a role in:
 - The probability that a lost/stolen device would contain customer information in e-mail

Analysis input



* Loss magnitude

- Primary loss
 - Comprised of person-hours responding to the event (\$100 hr) and/or lost revenue
 - Min: \$100
 - Max: \$25,000 (includes lost revenue and response person-hours)
 - ML: \$240
- Secondary loss event frequency
 - Driven by the probability that a device will contain sensitive customer information (7%). Because that percentage may vary over time:
 - Min: 5%
 - Max: 10%
 - ML: 7%

Analysis input



* Loss magnitude

- Secondary loss magnitude
 - Largely tied to volume of exposed records
 - Response (notifications, credit monitoring, legal defense, CIRT)
 - Notification: \$5 per affected customer
 - Credit monitoring: \$25 per affected customer
 - CIRT logistics:
 - » Min: \$2k (20 person-hours)
 - » Max: \$50k (500 person-hours)
 - » ML: \$3.5k (35 person-hours)
 - Legal defense
 - » Min: \$0 (best-case no legal action results)
 - » Max: \$500k (class action defense costs)
 - » ML: \$0 (assumes no legal action from a compromise of 35 customer records)

Analysis input



* Loss magnitude

- Secondary loss magnitude (continued)
 - Fines and Judgments
 - Min: \$0
 - Max: \$1M (primarily reflects regulatory actions)
 - ML: \$0
 - Reputation damage
 - Materialized through reduced market share, reduced stock price, and/or increased cost of capital
 - Note that even the max breach size is not expected to affect stock price or cost of capital
 - » Min: \$0
 - » Max: \$75k
 - » ML: \$3.5k

Computing your results.....

Individual analysis results

 Annualized loss exposure for device loss/theft where customer PII is at risk...

	Minimum	Average	Mode	Maximum
Total Loss Exposure	\$6,500	\$62,000	\$39,000	\$300,000



Example only - your results WILL differ!

Aggregate analysis results

Scenario	Min	Avg	Mode	Мах
Loss/Theft - PII	\$6500	\$62,000	\$39,000	\$300,000
Malware - PII	\$16,000	\$150,000	\$98,000	\$750,000
Transmission - PII	\$1200	\$2,500	\$1 <i>,</i> 900	\$57,000
Loss/Theft - Corp Data	\$300	\$600	\$400	\$43,000
Malware - Corp Data	\$450	\$1,100	\$900	\$65,000
Transmission - Corp Data	\$100	\$250	\$200	\$12,000
Loss/Theft - Financial Fraud	\$100	\$300	\$150	\$9,000
Malware - Financial Fraud	\$150	\$400	\$300	\$5000
Transmission - Financial Fraud	\$50	\$200	\$100	\$1200
TOTAL	\$24,850	\$217,350	\$140,950	\$1,242,200

Example only - your results WILL differ!

Comparing with/without an MDM product

Scenario	Min	Avg	Mode	Мах
Without MDM	\$25,000	\$217,000	\$141,000	\$1,200,000
With MDM	\$6,000	\$55,000	\$30,000	\$350,000
Difference	\$19,000	\$162,000	\$111,000	\$850,000

Example only - your results WILL differ!

Laying a FAIR Foundation for RBSM

AGENDA

- Bald Tire Scenario
- What is "FAIR"?
- Where FAIR Fits In
- The FAIR Risk Taxonomy
- FAIR Risk Analysis Example BYOD
- The Open Group FAIR Analyst Certification
- Q&A

The Open Group FAIR Analyst Certification

Certification: "FAIR Analyst Foundation"

- TOG owns the certification
- November, 2013

Authorized Training Partners Provide Course

- On-line eCourse from CXOWARE
- On-site training from multiple partners

Computational Engine by CXOWARE

• One year subscription to FAIR "U"

FAIR Analyst Training

eCourse Outline

- Risk concepts and terminology
- The FAIR taxonomy
- How to evaluate risk scenarios using FAIR
- Which data are required to perform risk analyses
- Where to find the data you never knew you had
- How to generate defensible quantitative estimates
- The principles of calibration





Training – FAIR Analyst Basic Training http://www.cxoware.com/training/

White Papers, Bald Tire, Open Group links etc http://www.cxoware.com/resources/

Training Discounts through Business of Security

Michael Radigan 614.942.0919 mradigan@businessofsecurity.com



Steps to Practical Application



Define or adopt a framework that makes sense

FAIR represents a paradigm shift for many security professionals

- What risk is (and isn't)
- Scenario analysis
- Calibration

Get stakeholders on board

- Apply risk analysis where it matters
- Show value

Steps to Practical Application



Start simple. For example:

- "How much risk does this policy exception represent?"
- "Which of these audit findings truly represents high risk?"

Perform peer reviews

 Requires people to explain their analyses

Leverage external expertise

Selective use, where it matters most

Six Forms of Loss

- Replacement
- Response
- Productivity
- Reputation
- Competitive Advantage
- Fines & Judgments



The Business Case for FAIR

Tangible Benefits:

- Reduce annual financial loss from IT security incidents.
- Reduce costs by identifying policies and controls that are obsolete or not optimized.
- Avoid costly fire drills and non-budgeted projects by challenging audit and assessment findings.
- Avoid costs by selecting alternatives to expensive "best practice" solutions.
- Reduce personnel costs associated with compliance efforts with risk based justifications.
- Determine IT risk economic capital requirements
- Avoid cost resulting from FUD generated concerns
- Improve efficiency of risk analysts



The Business Case for FAIR: Enabling well-

informed IT security risk management decisions

Intangible Benefits:

- Senior management and board of directors can understand and manage IT security risk.
- CISO can define and effectively communicate the business value of IT security.
- CISO can improve C-suite credibility, enabling business decisions for IT security investments.
- IT security gains better alignment with the business.
- Create a compelling business case for security initiatives.
- IT security team is on the same page, can more effectively collaborate on risk issues.
- Risk analysts will generate accurate, credible and consistent results across the team.

