Tomorrow’s Cyber Risk Analyst

**Jack Jones**
EVP Research & Development
RiskLens, Inc.
@FAIRiq
What we’ll cover...

- Current state of risk “analysis”
- Why change is necessary (and inevitable)
- Characteristics of cyber risk analysis
- The opportunities
- The challenges
- Steps you can take...
- Q&A
Current state of risk “analysis”
How would these questions typically be answered?

- “How much risk does this audit finding/policy exception request represent?”
- “What are our top ten risks?”
- “Which should we do first, improve access privilege management or improve the patching process?”
- “How much less risk will we have if we invest in the security technology/process you’re recommending?”
What is the most common cyber risk model in use?

Mental models
In most organizations, 70% to 90% of “High Risk” issues aren’t high risk
Why it matters...

Risk

- Threats
- Assets
- Impact

Risk Management

- Policies
- Resources
- Processes
- Strategies
- Initiatives
- Technology

Execution

- Awareness
- Capabilities
- Motivation

Decisions

- Prioritization
- Setting Objectives and Expectations

Intended State of Risk

Actual State of Risk

Monitoring & Testing

Analysis & Reporting

Communication

Resources

Enforcement
Why change is inevitable
Changing risk landscape

- Changes in business requirements and technology solutions are happening faster
- Budgets are tightening
- Risk management requirements are increasing
The implications...

- We need to be able to prioritize extremely well
- We need to be cost-effective in our solution choices
- We need to be able to justify our recommendations/choices
Senior executives are getting tired of...

And so are some regulators...
This IS going away

It’s umm…
“Medium risk”
Would you be comfortable with...

- A network architect performing a web application security review?
- An identity and access management professional performing forensics on a server?
- An auditor writing an encryption algorithm?
- Then why should we be comfortable with just anyone waving their wet finger in the air and proclaiming, “It’s high/medium/low risk”? 
Characteristics of cyber risk analysis
Cyber risk analysis — it isn’t everyone’s idea of a good time...

Complexity

Uncertainty

Numbers
Characteristics of tomorrow’s cyber risk analyst — not everyone need apply...

People skills

Understands basic probability concepts

Probability of rolling a 7 = 0%

Critical Thinking
Oh — and one more thing...

This applies to doing analyses...

...as well as dealing with people/cultural challenges in your organization and the profession.
The opportunities...
Characteristics of a “perfect” job...

- New field
- Pays well
- Not boring
- Moves the needle
Examples of the value proposition...

- Prioritizing well...
- Gaining support for critical improvements...
- Smart compliance...
  - PCI
  - SOX
Organizations that are taking risk analysis seriously...

...can’t find enough people with the right skills
Universities focusing on filling the need

- San Jose State University
  - Preparing economics majors for opportunities in infosec
- Examples of universities that include FAIR in their curriculum
  - Carnegie Mellon
  - Webster University
  - Ferris State University
  - Washington University in St. Louis
Challenges
Inertia

Lipstick on pigs

“YOU CAN PUT LIPSTICK ON A PIG, BUT IT’S STILL A PIG”

Complacency & ignorance
But expectations are changing...
Steps you can take...
Step 1 — right now

Ask yourself whether this is something you could enjoy.

Or is it something you’re already responsible for...?
Step 2 - today or tomorrow

Join

- FAIR Institute ([www.fairinstitute.org](http://www.fairinstitute.org))
  - Global community of professionals focused on evolving risk management
  - Non-profit, no cost to join
  - Rich blog resource
  - Special interest groups (cyber risk, operational risk, cyber insurance, data utilization, university educators, local chapters)

Check out

- Open Group’s OpenFAIR standard and professional certification ([www.opengroup.org/security](http://www.opengroup.org/security))
- Society of Information Risk Analysts ([www.societyinforisk.org](http://www.societyinforisk.org))
Step 3 — within the next week

- Evaluate your organization’s risk analysis maturity
  - Is it all about wet fingers in the air?
  - Does the organization struggle to measure and communicate risk consistently and effectively?
  - Are there endless religious debates about whether something is “high risk” or not?
  - Is risk analysis a distinct specialty in your organization and, if not, should it be?
    - And if it is a specialty, are the people doing it qualified?
Step 4 - within the next three months

5 Must Read Books to Jumpstart Your Career in Risk Management

What are the must have resources for people new to operational and cyber risk? This list outlines what books I would recommend to new analyst or manager.

They’re not ranked by which book is best. Instead, I list them in the recommended reading order. Let’s take a look at the list.

#1 - The Failure of Risk Management: Why It’s Broken and How to Fix It (Douglas Hubbard)

In The Failure of Risk Management, Hubbard highlights flaws in the common approaches to risk management. His solutions are as simple as they are elegant. (Spoiler alert: the answer is quantitative risk analysis).

http://www.fairinstitute.org/blog/5-must-read-books-to-jumpstart-your-career-in-risk-management
Step 4b - within the next three months

If your organization wants to take cyber risk analysis seriously, consider sponsoring the effort at San Jose State University

Contact Mike Jerbic <stephen.jerbic@sjsu.edu>
Effective cyber risk analysis is rare today, which has significant implications in an organization’s ability to manage risk.

Expectations are changing, and leaning strongly toward more rigorous, quantitative methods.

The need for cyber risk analysts is growing and only going to accelerate.

If analysis is your cup of tea, and if you want to contribute to the next stage of evolution in our profession, this might be the “perfect job”.

Q&A

Thank you!