Scaling a CRQ Program With Controls Analytics

Jack Jones, Chief Risk Scientist, RiskLens

Bryan Smith, Chief Technology Officer, RiskLens

FAIR22 CONFERENCE

Some facts…

- Cyber Risk Quantification (CRQ) can be a key enabler for effective cyber risk management.
  - Prioritization
  - ROI for security investments
  - Communicating with executive stakeholders
- The cyber risk landscape is large, complex, and dynamic.
- In order to maximize CRQ's benefit in the overall cyber risk landscape, organizations of all sizes need to be able to scale its application.

Two approaches for scaling a CRQ program…

- Staffing-up trained analysts (or outsourcing)
- Automated analyses

A quick dose of automation reality…

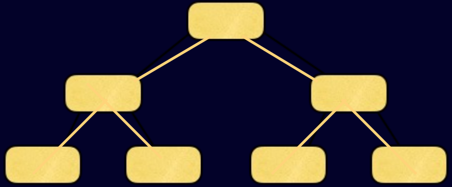
- You will never automate all of your risk analysis needs
- Automation does <u>not</u> reduce the number of assumptions that go into a risk analysis.
    - It just shifts assumption-making from the individual analysts to the automation designers.
- Done poorly:
    - Automation simply scales up poorly-informed decision-making
    - Instills a false sense of security

What’s required to do automation?

The same things that are required for manual analyses

1. Analysis scope (what’s being measured)

2. A model



3. Data

What data, from where?

- Assets
  - Physical and logical systems
    - Asset inventories
    - Active/passive discovery technologies
  - Record counts and intellectual property
    - DLP scanning
  - Revenue velocity
    - Business records

What data, from where?

- Loss
  - Organization experience
  - Public disclosures
  - Insurance claims
  - Published data (free or paid-for)

What data, from where?

- Threat
  - Frequency, Vectors, Methods
    - Logs
    - SIEM solutions
    - Loss events (public disclosures, Verizon DBIR, etc.)
    - Threat intelligence sources (govt. or commercial)
    - Information sharing (e.g., the ISACs)

What data, from where?

- Controls
  - Vulnerability scanners
  - Attack & penetration exercises
  - Auditing*
  - Policy exception records*
  - Configuration management tools
  - GRC tools
  - Etc…

Today, we're focusing
on controls...

control

Great. We have data.

^

What do we do with them?

How does patching affect risk?

How does training affect risk?

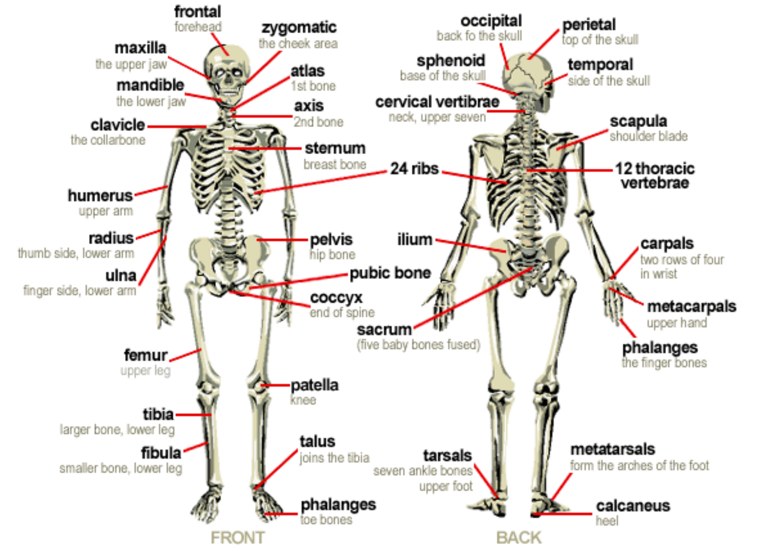
This is where “Controls Physiology” and “Control Analytics” step in…

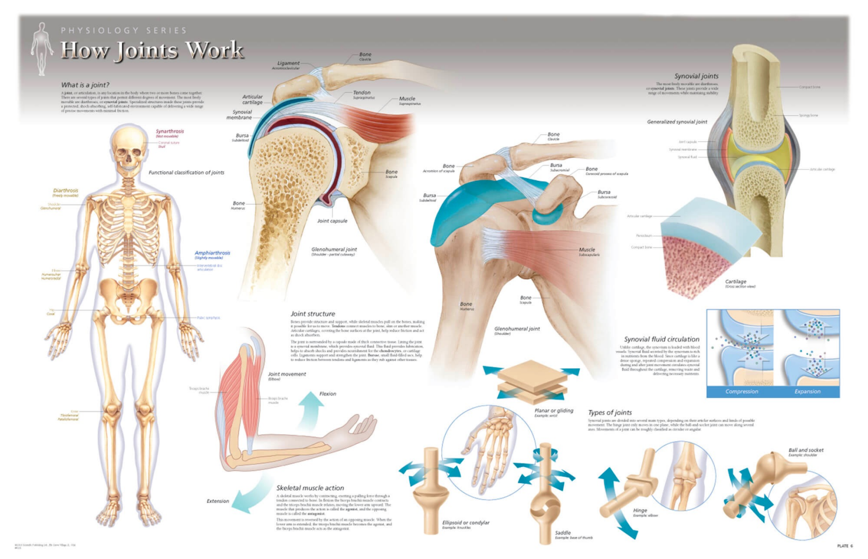
In the practice of medicine, which is more important?

Anatomy?
(The parts of the system)

OR

Physiology?
(How the system works)





Neither. You need to know both.

FAIR22
CONFERENCE

> "In the 19th century we had a relatively advanced understanding of anatomy, but we had a terrible understanding of physiology.
>
> We knew what was happening, but we didn't understand why it was happening."

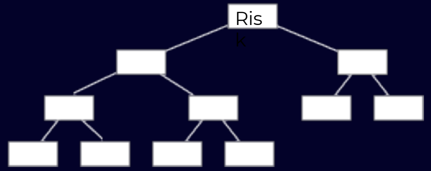
A Retired Surgeon

FAIR-CAM defines controls physiology — i.e., how the controls landscape works as a complex system of interdependent parts.

“Controls analytics” apply controls physiology to measure the efficacy and risk reduction value of controls.

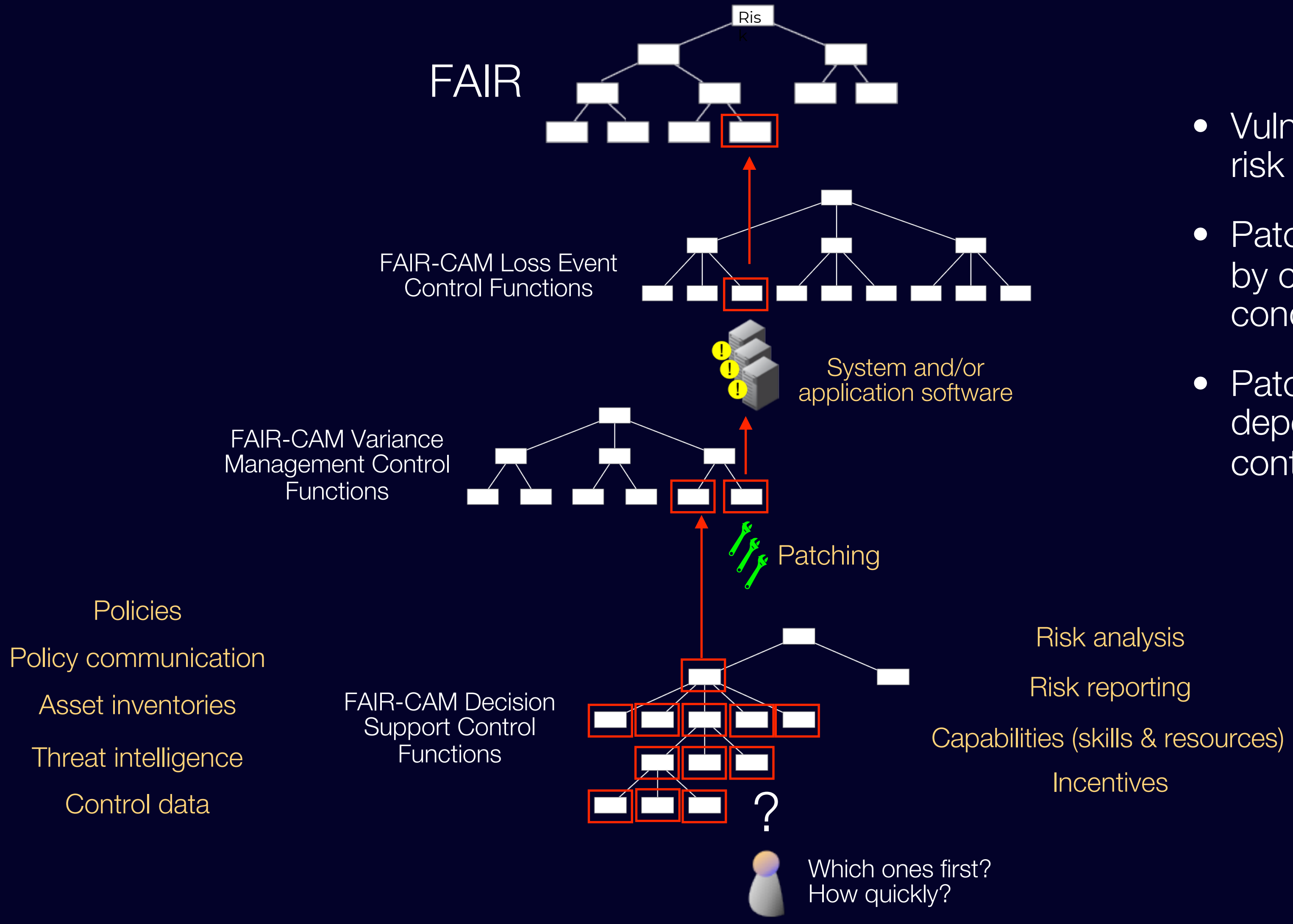
How does patching affect risk?

FAIR



Patching

How does patching affect risk?



Risk

FAIR

FAIR-CAM Loss Event Control Functions

System and/or application software

FAIR-CAM Variance Management Control Functions

Patching

Policies

Policy communication

Asset inventories

Threat intelligence

Control data

FAIR-CAM Decision Support Control Functions

Risk analysis

Risk reporting

Capabilities (skills & resources)

Incentives

?

Which ones first?
How quickly?

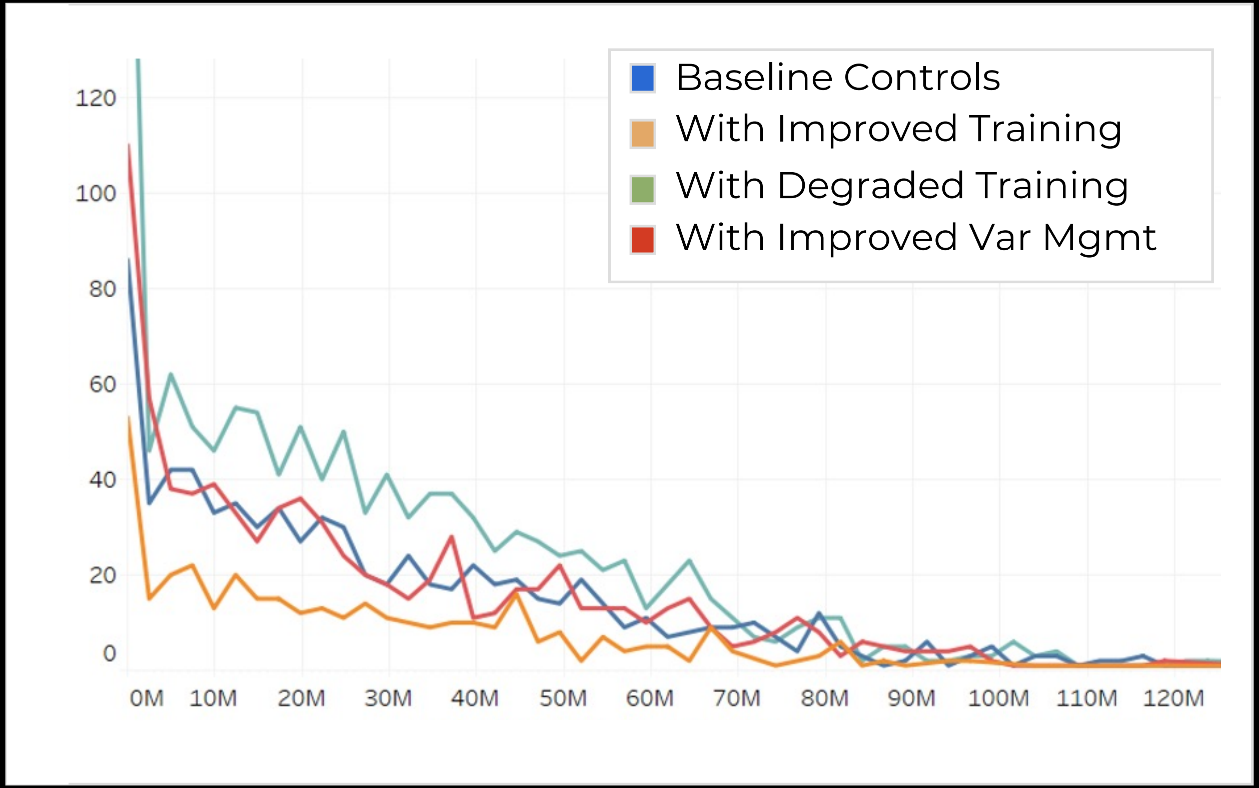
- Vulnerable software affects risk directly
- Patching affects risk indirectly by correcting vulnerable conditions in software
- Patching's efficacy is dependent on many other controls

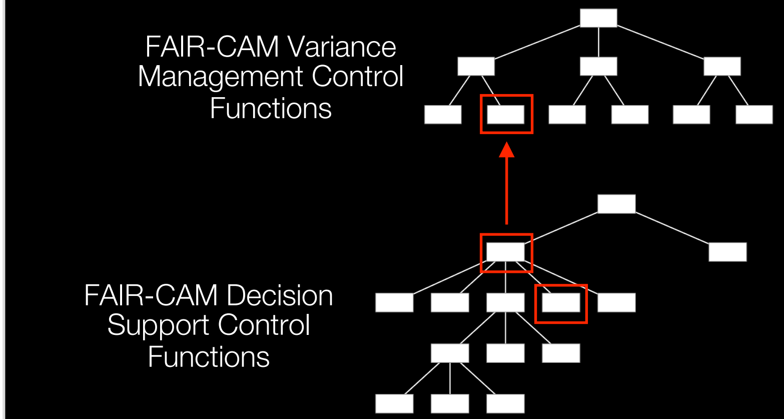
Demo

How does training affect risk?

How does training affect risk?

Well-qualified personnel can matter. A lot.

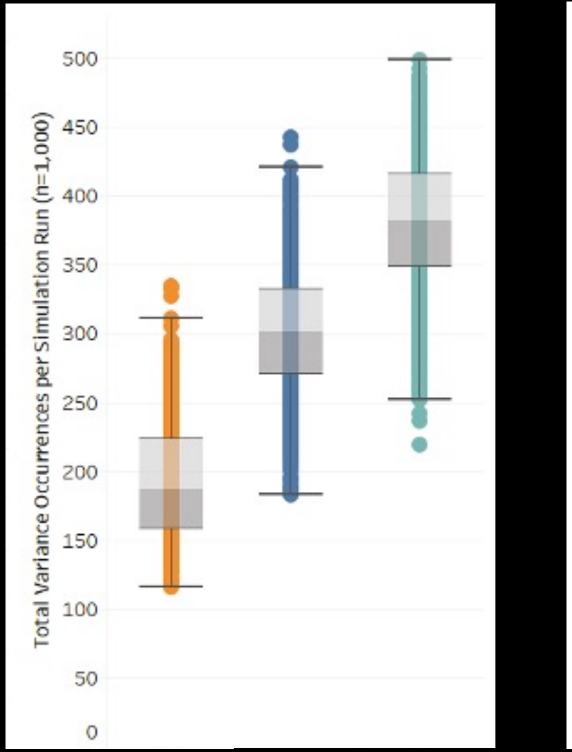



FAIR-CAM Variance Management Control Functions
FAIR-CAM Decision Support Control Functions

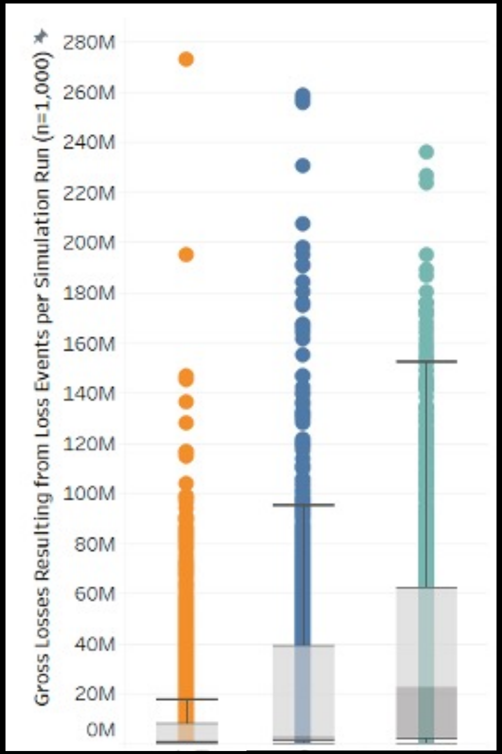
How does training affect risk?

🟦 Baseline Controls
🟧 With Improved Trainin
🟩 With Degraded Trainir

Variance Frequency

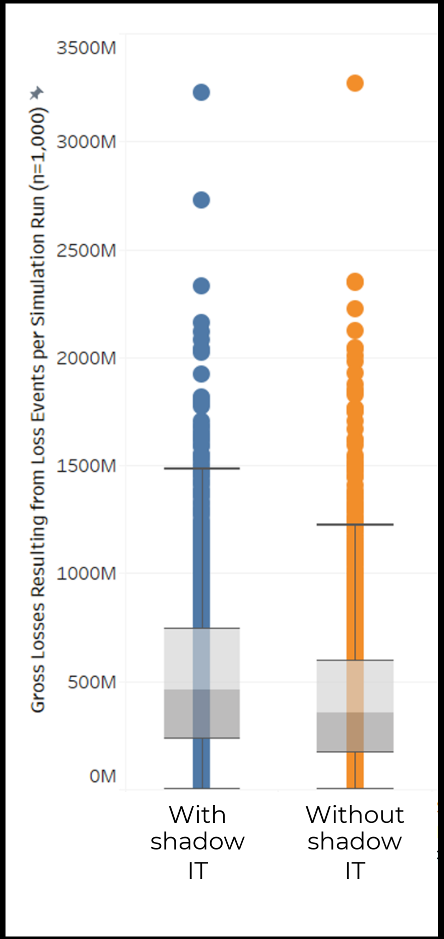


Losses

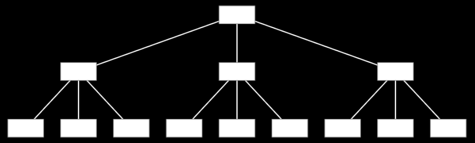


One last example

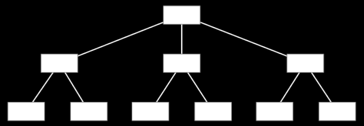
How does shadow IT affect risk?



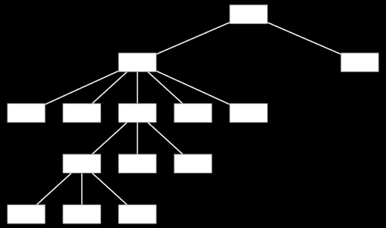
Scope warning!



FAIR-CAM Loss Event Control Functions



FAIR-CAM Variance Management Control Functions



FAIR-CAM Decision Support Control Functions

Wrapping it up…

- Scaling risk measurements is crucial in order to realize CRQ’s full potential

- Automation can be a key enabler of scaling, but it has to take into account the complex interdependent nature of the risk landscape

- FAIR-CAM explains and organizes the complex interdependent nature of the cybersecurity landscape, which enables reliable risk measurement automation

Questions?

FAIR22
CONFERENCE