Understanding and evaluating controls

Jack Jones - Chairman of the FAIR Institute
Ask yourself these questions…

• What’s the most valuable control in your cybersecurity program?

• What’s the least valuable control?

• What are the most cost-effective changes your organization can make to improve its risk posture?

Would your answers be the same as someone else’s in your organization?
What do we mean by “value”?

The value proposition of any control boils down to this:

*How much it reduces the frequency or magnitude of loss from one or more loss event scenarios*
A simpler question…

How much less risk will we have if we improve this NIST CSF subcategory from a “2” to a “3”?

PR.AT-1: “All users are informed and trained”

Who are these users? What does a “2” represent, or a “3”? Trained in what?

How does training affect risk?
Warning…

The approach we’re about to cover is more complex than common practice in our profession.
What’s been missing?
In the practice of medicine, which is more important?

Anatomy? (The parts of the system)

Physiology? (How the system works)

Neither. You need to know both.
“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
Control frameworks such as NIST CSF, ISO27001, NIST 800-53, PCIDSS, CIS, etc. represent cybersecurity controls anatomy.

There has been an almost complete absence of anything resembling cybersecurity controls physiology.
The FAIR Controls Analytics Model (FAIR-CAM) defines controls physiology — i.e., how the controls landscape works as a complex system of interdependent parts.

This will enable us to reliably evaluate and empirically measure the efficacy and risk reduction value of controls.
Direct vs. indirect effects on risk

Indirectly affect risk

- Asset management
- Threat intelligence
- Awareness training
- Risk analysis
- Etc.

- Scanning
- Patching
- Auditing
- Change management
- Etc...

Directly affect the frequency or magnitude of loss

- Decision Support Controls
  - Enable well-informed decisions

- Loss Event Controls
  - Authentication
  - Access privileges
  - Logging
  - Data recovery processes
  - Etc...

Affect the reliability of other controls

- Variance Mgmt. Controls

Enable well-informed decisions

Asset management

Threats

Assets

Risk

Etc.
Direct vs. Indirect example…

Indirectly affect risk

- Asset management
- Threat intelligence
- Anti-phishing training
- Risk analysis
- Incentives
- Etc.

Directly affect the frequency or magnitude of loss

- Trained personnel
- Anti-malware
- Access privileges
- Data recovery processes
- Etc...

Decision Support Controls

Variance Mgmt. Controls

Loss Event Controls

Assets

Risk

Loss exposure from a ransomware event

Patching

Auditing

Etc...

Threats
Loss Event Control (LEC) functions

Functions that directly affect the frequency or magnitude of loss

Loss Event Prevention
- Avoidance
- Deterrence
- Resistance

Loss Event Detection
- Visibility
- Monitoring
- Recognition

Loss Event Response
- Event Termination
- Resilience
- Loss Minimization

%  %  %  %  Time  %  Time  Time  $
Variance Management Control (VMC) functions

Functions that affect the frequency or duration of variant conditions

- Variance Prevention
  - Reduce Change Frequency
  - Reduce Variance Probability
- Variance Identification
  - Threat Capability Monitoring
  - Controls Monitoring
- Variance Correction
  - Prioritization and Solution Selection
  - Implementation
**Decision Support Control (DSC) Functions**

- **Prevent mis-aligned decisions**
  - Define expectations and objectives
  - Communicate expectations and objectives
  - Provide situational awareness
  - Ensure capability
  - Provide incentives
  - Provide data
    - Asset data
    - Threat data
    - Controls data
  - Analysis
  - Reporting

- **Detect mis-aligned decisions**
  - Functions that affect the frequency or duration of mis-aligned decisions
Back to our question…

How much less risk will we have if we improve this NIST CSF subcategory from a “2” to a “3”?  

PR.AT-1: “All users are informed and trained”
How does training affect risk?

- Training and awareness is dependent on the existence of clearly defined expectations and objectives.
- Training and awareness reduces the probability of mis-aligned decisions…
- …which reduces the probability of variant conditions.
- …which reduces risk.

Policies

Education & awareness training
How much can training affect risk?

Well-qualified personnel can matter. A lot.

- Baseline Controls
- With Improved Training
- With Degraded Training
- With Improved Var Mgmt

- Variance
- Frequency

FAIR

FAIR-CAM Loss Event Control Functions

FAIR-CAM Variance Management Control Functions

FAIR-CAM Decision Support Control Functions
How does patching affect risk?
How does patching affect risk?

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

Vulnerable software affects risk directly.

Patching affects risk indirectly by correcting vulnerable conditions in software.

Patching’s efficacy is dependent on many other controls.
NIST-CSF to FAIR-CAM

FAIR-CAM Control Function Names

Loss Event Control Model

Variance Management Control Model

Decision Support Control Model

Volume of mappings by control function
In summary:

- FAIR-CAM is a published standard through the FAIR Institute
- FAIR-CAM defines “controls physiology”:
  - The specific ways in which controls affect risk, both directly and indirectly
  - The complex relationships and interdependencies between controls
  - Units of measurement for control functions
- FAIR-CAM is being mapped to existing control frameworks
- When controls are mapped to the FAIR-CAM functions they support, their efficacy and risk reduction value can be forecasted and empirically measured.
- This supports sensitivity analyses and other methods of determining optimized risk management strategies.
- It also enables the ingestion of controls telemetry and data to refine and/or automate risk analysis.
Questions?