Reliability Engineering in Information Security: A Novel Approach to Risk Assessment

Chris Woods, CISSP
Mount Holyoke College

Disclaimer

This talk is:

- Speculative
- Additive
- Not intended to replace the advice of a competent information security professional that understands your infrastructure and needs.

Securing the Infrastructure

But how?

- Vulnerability Management
- Threat Hunting
- Intel Sharing
- Machine Learning and AI
- OS Hardening
- Identity Management
- Patching and Updating
- Etc

Risk Assessment and Management

NIST SP 800-30 Rev.1

There are no specific requirements with regard to:

- (i) the formality, rigor, or level of detail that characterizes any particular risk assessment;
- (ii) the methodologies, tools, and techniques used to conduct such risk assessments; or
- (iii) the format and content of assessment results and any associated reporting mechanisms.

Organizations have maximum flexibility on how risk assessments are conducted and are encouraged to apply the guidance in this document so that the various needs of organizations can be addressed and the risk assessment activities can be integrated into broader organizational risk management processes.

Annualized Loss Expectancy (ALE)

$$\text{ALE} = V * F$$

where *V* is the value of the incident expressed in monetary units and *F* is the expected frequency at which the loss realized.

ALE Calculation for Low Frequency/High Impact Event

$$ALE = \$1,000,000 * .01 = \$10,000$$

ALE Calculation for High Frequency/Low Impact Event

ALE = $100 * 100 = $10,000

Common Dilemmas

Standard risk analysis identifies assets requiring protection and this, in turn, defines how organizations :

- deploy resources
- procure infrastructure
- task personnel

Resource-constrained organizations often cannot effectively secure all assets within their infrastructure.

Limitations to Predicting the Frequency of Loss Events (or Anything Really)

- Humans are subject to an array of biases (e.g. Dunning-Kruger) and so are bad at this.
- Humans are subject to an array of biases (e.g. Gambler’s Fallacy) and so are bad at this.
- Humans are subject to an array of biases (e.g. Bandwagon Effect) and so are bad at this.
- Etc.

RCM methodology can help organizations make appropriate decisions to extend adequate and effective levels of security to all assets even when resources and information are constrained.

Benefits of RCM

- Eliminate unnecessary controls without compromising confidentiality, integrity, or availability.
- Identify applicable and effective controls to maintain confidentiality, integrity, or availability.
- Establish framework for asymmetric decision-making for selection of controls.

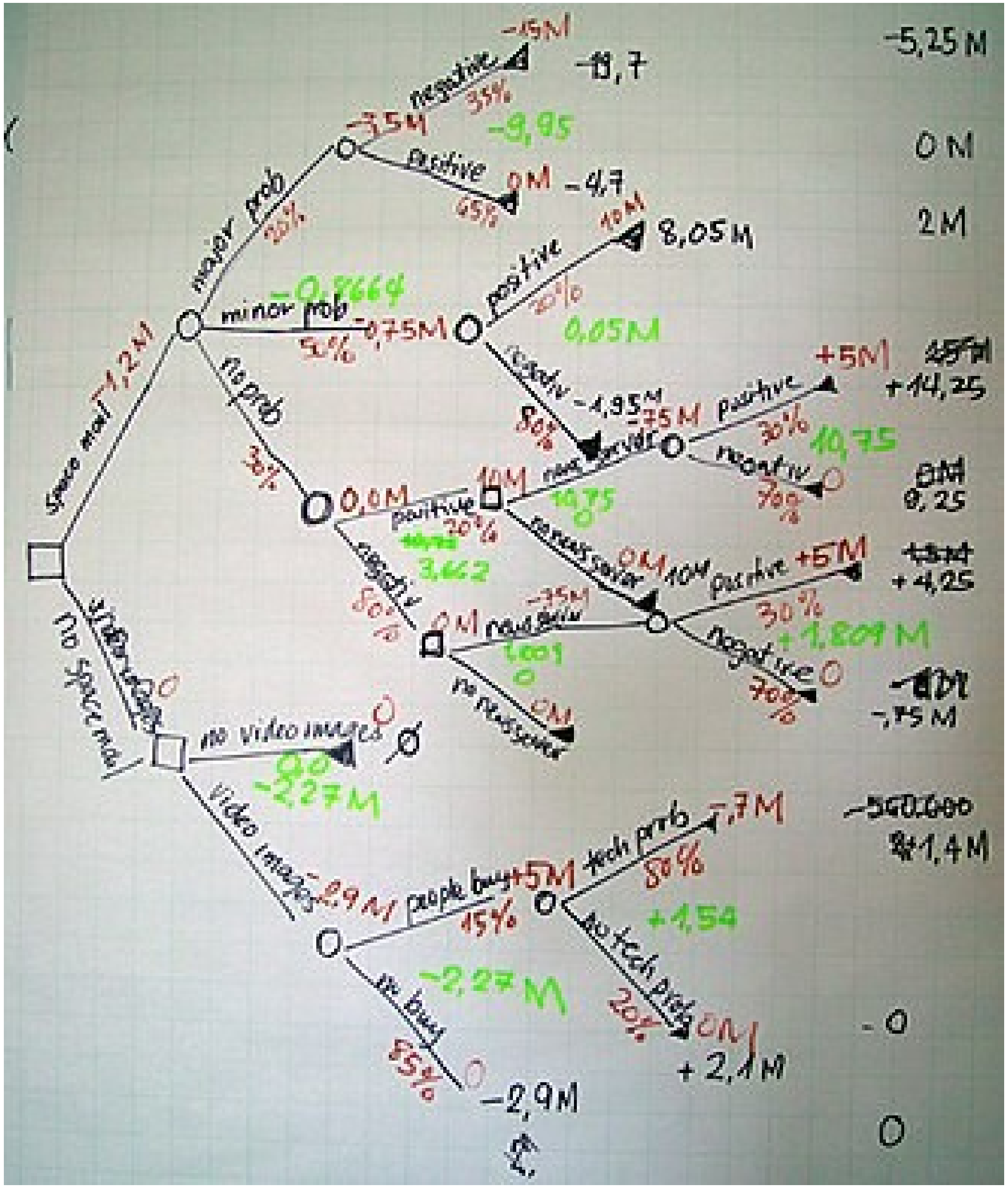
Origins of Reliability Engineering

- In the 50s and 60s wide-spread belief that reliability decreased with age.
- This belief was re-examined as jet transport came into common use.
- Aviation hardware showed typical failure curve with failure clustered at start-of-service (infant mortality) followed by a long period of stable performance for the duration of a part's life.

Origins of Reliability Engineering

- In the 1960’s commercial aviation was adapting to the operational requirements of jet-propelled aircraft.
- Failures (crashes) were common.
- Airlines applied decision tree logic to identify maintenance tasks.
- Boeing based the initial maintenance of the 747 on decision-tree methodology.
- This was making jet flight commercially infeasible.

Source: *Reliability-Centered Maintenance Handbook NAVSEA.*



https://commons.wikimedia.org/wiki/File:Manual_decision_tree.jpg

Origins of Reliability Engineering

- F. Stanley Nowlan, United Airlines
- Howard Heap, United Airlines
- Authored 1978 report: *Reliability-Centered Maintenance*.

Reliability refers to the expectation that a given system will continue to perform its function(s).

RCM asks:

What proof is there that an action taken prevents a given failure?*

* (and is that failure worth preventing?)

http://www.nationalgalleries.org/collection/simple-search/R/6240/artist_name/Allan%20Ramsay/record_id/22933

An Information Technologist (Mis)Uses Humean Causation

- Nature may cease to be regular at some point
- Past uniformity is no proof of future uniformity

How RCM Handles Uncertainty

- Understand systems in terms of functions
- Understand failures as loss of functions
- Understand effects of lost functions
- Utilizes maintenance tasks to prevent and redundancy to mitigate.

"The driving element in all maintenance decisions is not the failure of a given item, but the consequences of that failure for the equipment as a whole." (Nowlan & Heap, p.29)

What is a Failure?

An unsatisfactory condition.

What is a Failure?

In information security terms it is a loss of:

- Confidentiality.
- Integrity.
- Availability.

Evaluation of a given control starts with identification of the functional failure and consequence (severity) it is intended to prevent.

Define Failures as Loss of Function

Functions can be provided at any layer of the stack:

- Broken wire leads to loss of availability.
- Misconfigured switch leads to loss of confidentiality.
- Incorrect application settings leads to loss of integrity.

Applying RCM Methodology to Information Security

Four basic questions asked by RCM modified for application to information security:

- What does a system do?
- What failures can occur?
- What are the consequences/impact of a given failure?
- What can be done to prevent/mitigate the failure?

Defining a Functional Failure

- Identify the functions a given system provides
- Use ‘fails to...’ construction (e.g. System fails to log all user sessions.)
- Failure effects are roughly analogous to loss of one or more of the CIA triad.
- Generally, it is more useful to think in terms of layers or systems than of a single entity.

Should Failures be Prevented?

- Only when feasible.
- All other failures are mitigated or accepted according to risk analysis.
- Failures that cannot be prevented or mitigated must be accepted.
- Abandon the activity if failure cannot be prevented/mitigated and is unacceptable.

Failure Modes

- Simple systems have a few evident failure modes (cables break, power fails, etc).
- Complex systems have multiple failure modes that often have no evident effect but usually have a dominant failure mode (backups fails because disk is full of logs).
- When you hear hoofbeats think horses not zebras.

Risk Asessment with RCM

Evaluate the consequences of failure and classify according to severity of the consequences: (e.g. critical data is unavailable...)

- High severity rankings (greatest concern): Legal/Regulatory, Health and Safety, Major Economic/Reputational (existential risk to org).
- Medium severity rankings (less concern): Economic/Reputational - cost can be born by organization or transferred.
- Low severity rankings (least concern): Economic/Reputational - cost can be born by operations budget or transferred.

Risk Assessment with RCM

Risk can be:

- Mitigated with appropriate controls
- Accepted (if severity is least concern)
- Transferred (if cost-effective).
- If risk/failure severity is low and cost of preventing failure exceeds consequence of failure: accept it.
- If risk/failure cannot be mitigated by controls, transferred, or accepted: don't do it.

Cost of failure includes cost of the loss of the service. Losing a service mid-summer may not be a big deal. Losing it during acceptance notification could be existential risk. Assign the correct severity based on the maximum expected loss.

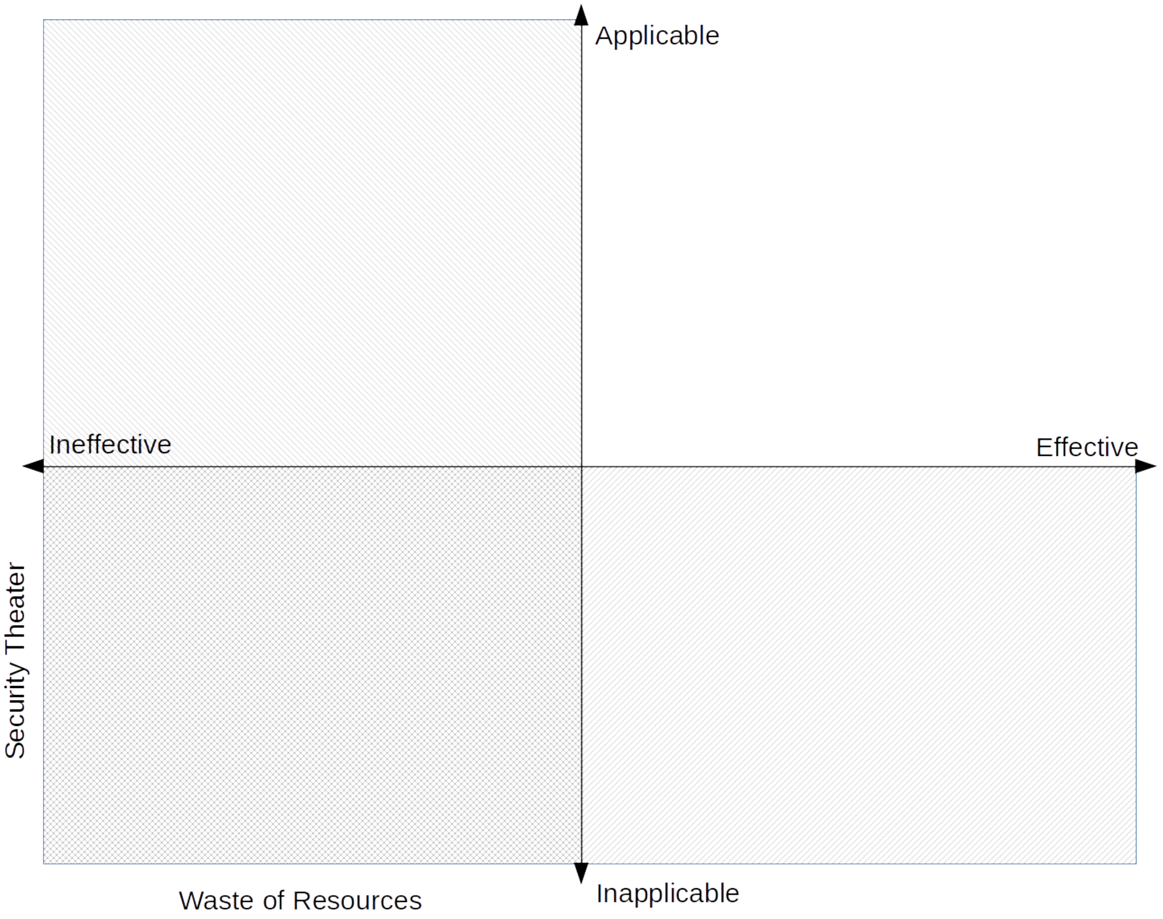
Applicability

Requires that each security control be implemented for an identifiable and explicit reason (e.g. hourly file backup to ensure availability of critical data).

Effectiveness

Requires that each security control implemented for an identifiable and explicit reason does so at a cost that is lower than the ALE (or suitable metric) of the event it is intended to prevent or mitigate.

Conjoined Parallelograms of Risk Assessment Wizardry™



Control Selection

Select controls to prevent or mitigate failure. Controls might be:

- Setting or modes within an application
- Rules or policies governing system use
- Physical security
- Network routing and firewall rules
- Etc

If a given control cannot reduce the risk of a failure to an acceptable level, a new control must be implemented or the system redesigned to reduce its severity.

"Control means the ability to keep the state of a system within some preferred subset of all its possible states"
(Quigley, et al. 2017, p. 50)

Giving Up

- Be mindful that the information you hold implies the a certain type of infrastructure to protect that asset.
- It is worth asking: is the information held worth the effort to secure it?
- Sometimes it is.
- If it isn’t then give up.

Further Reading

- **Reliability-centered Maintenance** - F. Stanley Nowlan, Howard F. Heap (http://www.dtic.mil/dtic/tr/fulltext/u2/a066579.pdf)
- **Guide for Conducting Risk Assessments** – NIST (https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final)
- **Too Critical to Fail** – Quigley, et al. (http://www.mqup.ca/too-critical-to-fail-products-9780773551619.php)
- **Modeling and Mitigation of Information Technology Risks** - Reiko Ann Miura-Ko (https://purl.stanford.edu/nm984rf7823)

Thanks!
Questions?