Meta-Metrics:

Building a Scorecard for the Evaluation of Security Management and Control Frameworks

Michael Smith

Metricon 5.0 08/10/2010

Laws, Sausages, and Frameworks?

- Top-down: regulation->policy->procedures ->technical
- Organic growth: tech->architecture->policy
- Throw in the kitchen sink, built a checklist, rinse, repeat
- Lessons learned: Company X got pwned so you have to pay for their crimes
- Years of analysis: extended PhD thesis
- The Gray-Hair approach, I know better than you

The Part Where Mike Gets Meta

- "The nature of all security frameworks is to devolve into a checklist" --Rybolov
- All frameworks suck, the one you're using sucks the worst
- Management by inclusion v/s exclusion
- Build a rational way to judge frameworks

Framework Scorecard

$$$$$ Small, Medium, Large Organizations	

Framework Scorecard

$$$$$ Small, Medium, Large Organizations	Efficacy Tactical/Technical Patch and Vulnerability

Framework Scorecard

$$$$$ Small, Medium, Large Organizations	Efficacy Tactical/Technical Patch and Vulnerability
Completeness Sustainable Program	

Framework Scorecard

$$$$$ Small, Medium, Large Organizations	Efficacy Tactical/Technical Patch and Vulnerability
Completeness Sustainable Program	?Robustness? Shelfware-Resistance Low-Maintenance Atomicity v/s Dependence

SWAG Reactions: ISO 27002

$$ Reasonably large	Some Guidelines
Reasonably Complete	OK Robust, some audit burden and rework

SWAG Reactions: PCI-DSS

Relatively Small	Mostly Tactical
Bollocks for Sustainable Has “Policy”	Robustness as a function of small size

SWAG Reactions: NIST RMF

Much Cost	Prescribed but not the focus due to abstraction
The Whole Hawg of Completeness	Horribly fragile, this adds significantly to the cost

Uses

- Conscious design of security, compliance, regulation, risk, etc frameworks
- Prioritization of effort
- Split-horizon assessment/audit
- Maturity models
- Ending “Legislation Amateur Hour”

OMG What Have I done?

- Have I built a better GRC and should I be hanged from the neck until I am dead?
- Is an abstract of an abstract leading to a divide-by-zero error that will end the world?
- Have I lost my bloody mind?

Questions, Comments, or War Stories?

http://www.guerilla-ciso.com/

rybolov(a)ryzhe.ath.cx