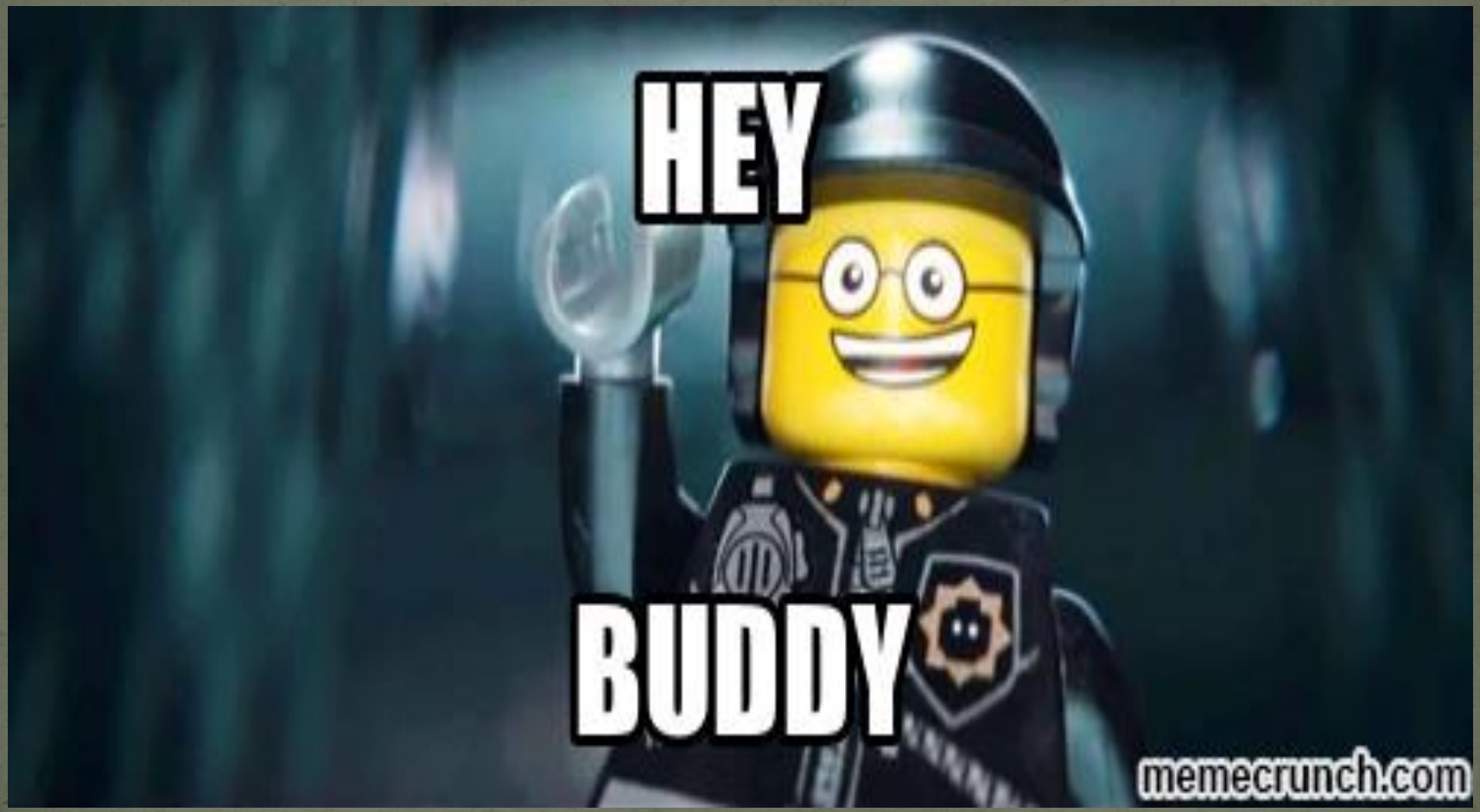
Circles & Boxes

Drawing SecArch into your program while avoiding the Tyranny of the Ivory Tower

Introduction



How do you define a guy that doesn't *DO* anything?

- Christopher Robinson aka CRob
- Sr. Program Manager for Product Security at Red Hat, Inc. (say that fast 5 times)
- President of Cleveland ISC2 Chapter
- 18 years Enterprise Engineering/Operations Management and Strategic Planning experience
- Worked for several Fortune 500 companies
- Leader, artist, mentor, writer, strategerist, game-designer, brewer, Pirate, Dungeon Master, teacher, vintner, father, Buckeye, consultant, Boy Scout, teacher, Ambassador, gamer, Security-ologist, bacon-enthusist

Topics of Discussion

- Circles!
- Boxes!
- Lines Connecting Circles and Boxes!
- Lines Connecting Boxes to Circles!
- Circles inside of Circles!
- L33T P0W3RP0int1NG! (ZOMG!)
- Ivory Towers
- Unicorns and Pirates
- Security Architecture & InfoSec Programs

All told mostly in pictures

So, I'm an architect.....

(please hold you boos, tomatoes, torches & pitchforks until the end of the presentation)

Our problem (or What do you do?)

- Building excellent, quality, or cost-efficient products requires complex solutions.
- As complexity grows, using whiteboards and bar napkins quickly fails to be effective as engineering methods.

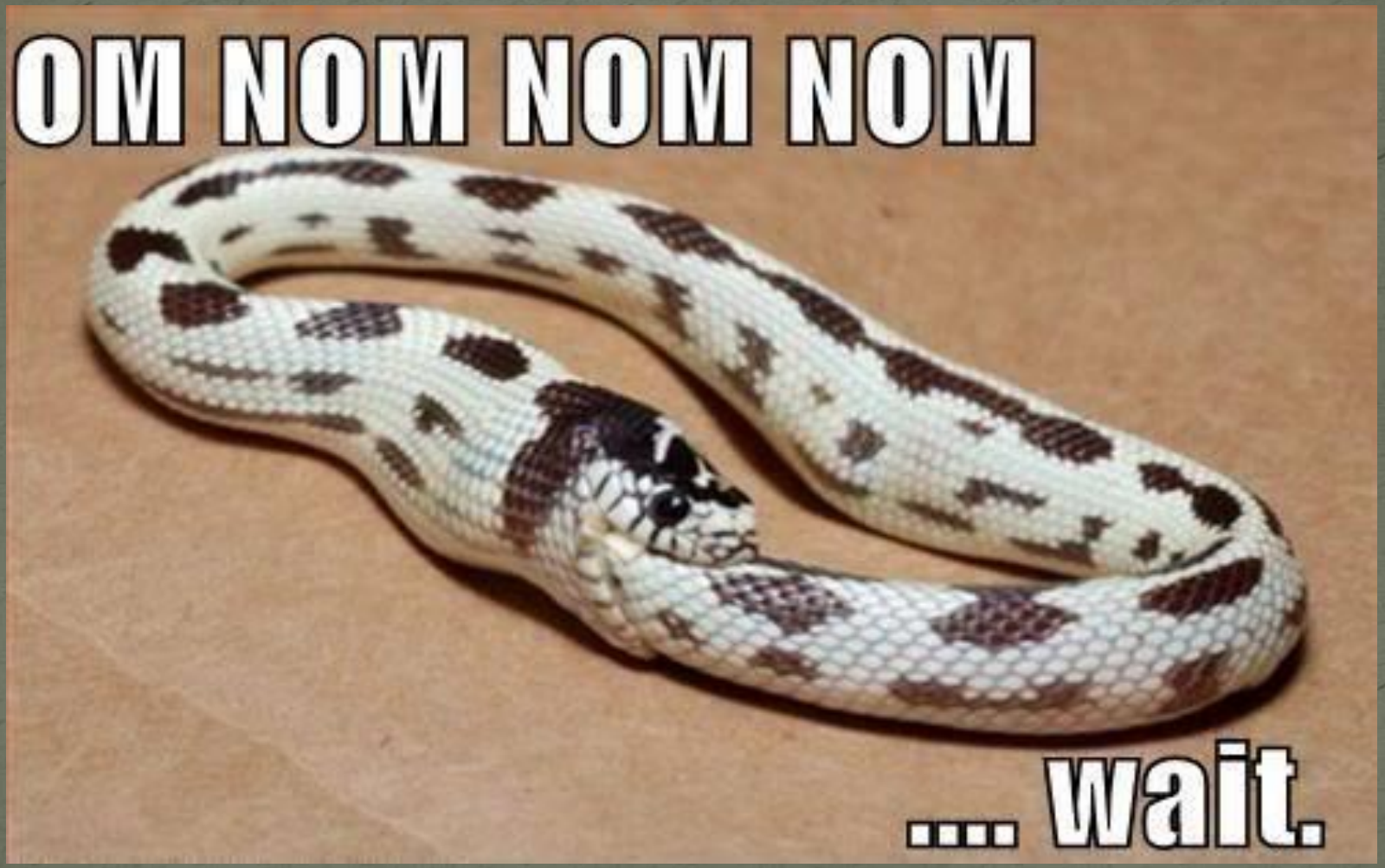
I play with models

Circles and Boxes

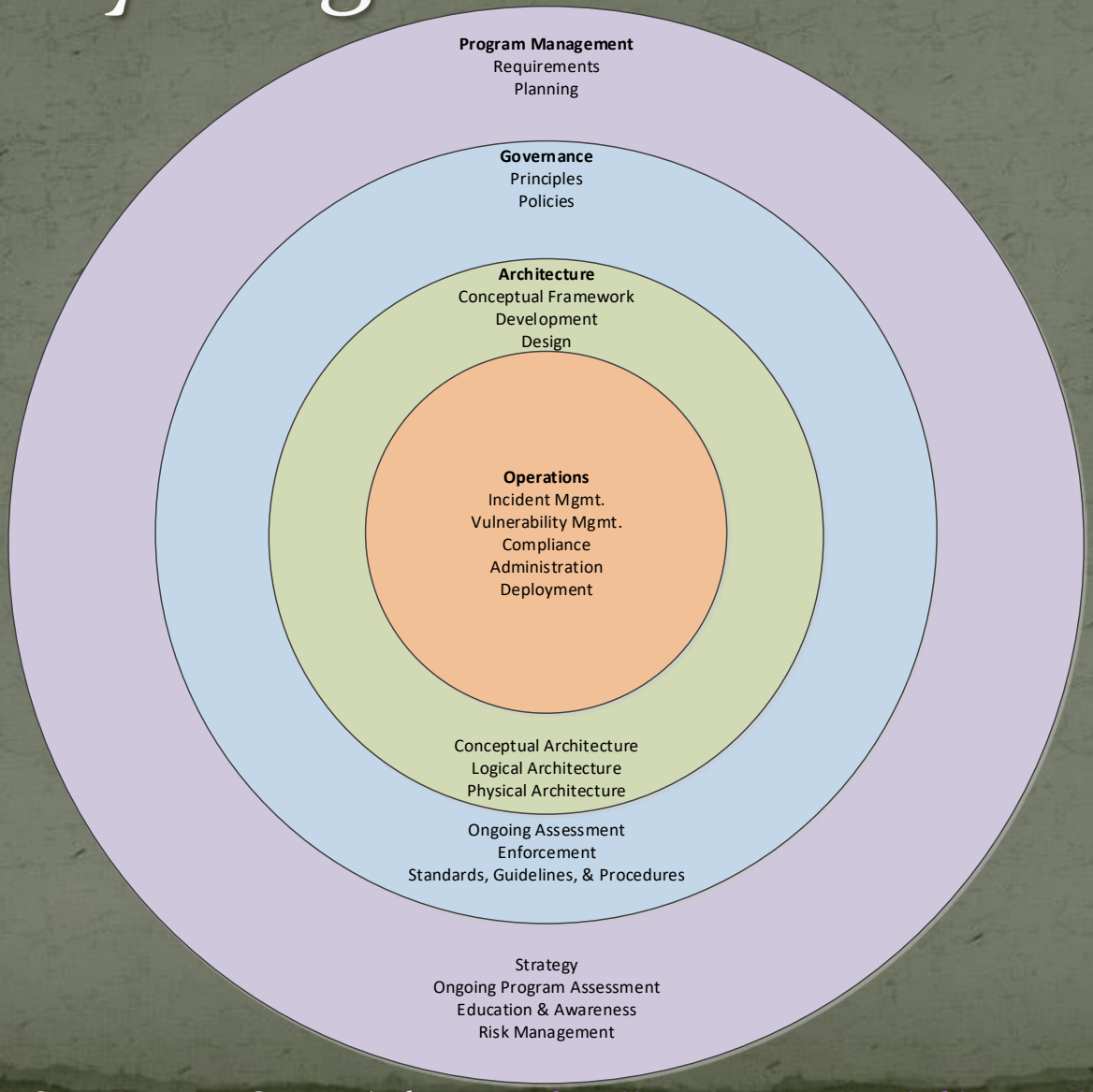
(...and Diamonds and Rectangles, Oh My!)

Whiteboard WAT – a brief tangent

So……Circles



Security Program Model

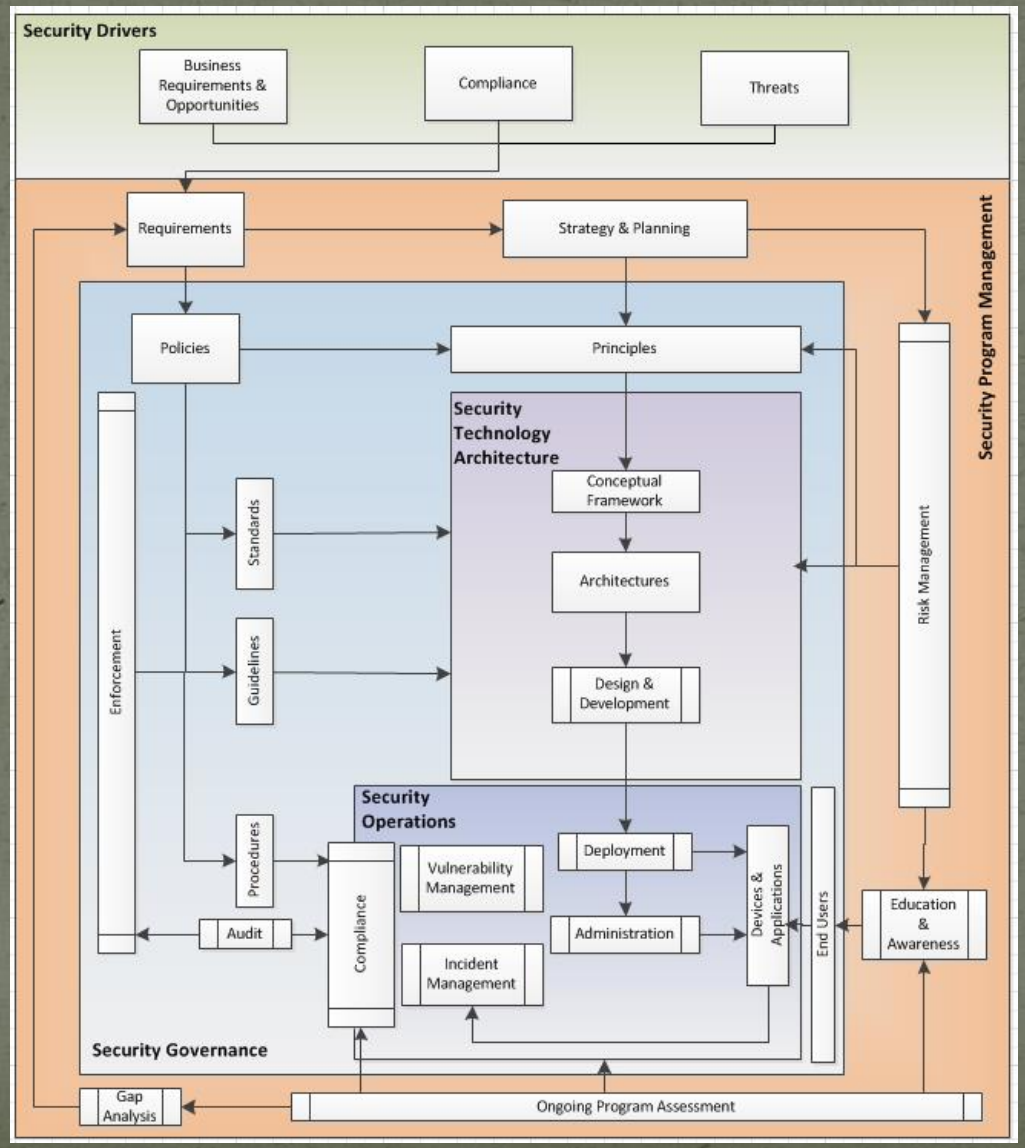


ZOMG! It's full of SIRKURLZ!

Based on OESA – Open Enterprise Security Architecture – http://www.opengroup.org/subjectareas/security/architecture

Boxes!

So many boxes….



SABSA-cadabra!

SABSA SERVICE MANAGEMENT MATRIX (Aligned with ITIL v3)

	ASSETS (What)	MOTIVATION (Why)	PROCESS (How)	PEOPLE (Who)	LOCATION (Where)	TIME (When)
	Service Delivery Management	Operational Risk Management	Process Delivery Management	Personnel Management	Management of Environment	Time & Performance Management
	The row above is a repeat of Layer 6 of the main SABSA Matrix. The five rows below are an exploded overlay of how this Layer 6 relates to each of these other Layers					
CONTEXTUAL ARCHITECURE	Business Driver Development	Business Risk Assessment	Service Management	Relationship Management	Point-of-Supply Management	Performance Management
	Business Benchmarking & Identification of Business Drivers	Analysis of Internal & External Risk Factors	Managing Service Capabilities for Providing Value to Customers	Managing Service Providers & Service Customers; Contract Man'ment	Demand Man'ment; Service Supply, Deployment & Consumption	Defining Business-Driven Performance Targets
CONCEPTUAL ARCHITECTURE	Proxy Asset Development	Developing ORM Objectives	Service Delivery Planning	Service Management Roles	Service Portfolio	Service Level Definition
	Defining Business Attributes Profile with Performance Criteria, KPIs & KRIs	Risk Analysis on Business Attributes Proxy Assets	SLA Planning; BCP; Financial Planning & ROI; Transition Planning	Defining Roles, Responsibilities, Liabilities & Cultural Values	Planning & Maintaining the Service Catalogue	Managing Service Performance Criteria and Targets
LOGICAL ARCHITECTURE	Asset Management	Policy Management	Service Delivery Management	Service Customer Support	Service Catalogue Management	Evaluation Management
	Knowledge Management; Release & Deployment Management; Test & Validation Management	Policy Development; Policy Compliance Auditing	SLA Management; Supplier Management; BCM; Cost Management; Transition Management	Access Management; User Privileges, Account Administration & Provisioning	Configuration Management; Capacity Planning; Availability Management	Monitoring & Reporting Performance against KPIs and KRIs
PHYSICAL ARCHITECTURE	Asset Security & Protection	Operational Risk Data Collection	Operations Management	User Support	Service Resources Protection	Service Performance Data Collection
	Change Management; Software & Data Integrity Protection	Operational Risk Management Architecture	Job Scheduling; Incident & Event Management; Disaster Recovery	Service Desk; Problem Man'ment; Request Man'ment	Physical & Environmental Security Management	Systems and Service Monitoring Architecture
COMPONENT ARCHITECTURE	Tool Protection	ORM Tools	Tool Deployment	Personnel Deployment	Security Management Tools	Service Monitoring Tools
	Product & Tool Security & Integrity; Product & Tool Maintenance	ORM Analysis, Monitoring and Reporting Tools & Display Systems	Product & Tool Selection and Procurement; Project Management	Recruitment Process Disciplinary Process Training & Awareness Tools	Products & Tools for Managing Physical & Logical Security of Installations	Service Analysis, Monitoring and Reporting Tools & Display Systems

Bring me more Boxes!


BOXES
BOXES EVERYWHERE
quickmeme.com

NIST Cybersecurity Framework (meh)

Function	Function Definition	Category	Definition
IDENTIFY	Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.	Asset Management	The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.
		Business Environment	The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.
		Governance	The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.
		Information Security Risk Assessment	The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.
		Information Security Risk Management Strategy	The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.
PROTECT	Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.	Access Control	Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.
		Awareness & Training	The organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.
		Data Security	Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.
		Information Protection Processes & Procedures	Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.
		Maintenance	Maintenance and repairs of industrial control and information system components is performed consistent with policies and procedures.
		Protective Technology	Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.
DETECT	Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.	Anomalies & Events	Anomalous activity is detected in a timely manner and the potential impact of events is understood
		Security Continuous Monitoring	The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.
		Detection Processes	Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events.
RESPOND	Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.	Response Planning	Response processes and procedures are executed and maintained, to ensure timely response to detected cybersecurity events.
		Communications	Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies.
		Analysis	Analysis is conducted to ensure adequate response and support recovery activities.
		Mitigation	Activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident.
RECOVER	Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.	Recovery Planning	Recovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity events.
		Improvements	Recovery planning and processes are improved by incorporating lessons learned into future activities.
		Communications	Restoration activities are coordinated with internal and external parties, such as coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors.

http://www.nist.gov/cyberframework/

NIST-to-Real Controls

Function	Category	Sub-Category/Capability/Service
IDENTIFY	Asset Management	CMDB
		BCP App List
		Database Data List
		System Secure Baselines
		Data Flow & Dependency Documentation
		System Connection & Dependencies Documentation
		Asset Lifecylce Management Process
	Business Environment	Business Strategy/Planning Engagement
		M&A Activities Engagement
		Business Leadership Informs (ITLT, ISOC, ERM Committee, etc)
		Legal-Regulatory Environment Awareness
		Business Impact Analysis
	Governance	Information Security Policies
		Waiver administration
		Access Audits
		Audit Liason
		SSDLC
		InfoSec Program Reporting/Dashboard
	Risk Assessment	Risk Assessments
		Vendor Security Reviews
		Security Reviews/Posture Assessments
		Internal & External penetration tests
		Gold Tier System Management Review
	Risk Management Strategy	Information Security Strategy
		Audit Responses

NIST-to-Business Capabilities

Function	Function Definition	Category	Definition	Technology Capability
IDENTIFY	Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.	Asset Management	The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	Information Security Program Governance
		Business Environment	The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	
		Governance	The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	Risk & Threat Analysis
		Information Security Risk Assessment	The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	Information Protection Processes & Procedures
		Information Security Risk Management Strategy	The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	
PROTECT	Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.	Access Control	Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.	Identity & Access Management
		Awareness & Training	The organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.	
		Data Security	Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	
		Information Protection Processes & Procedures	Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	Perimeter Protections
		Maintenance	Maintenance and repairs of industrial control and information system components is performed consistent with policies and procedures.	Internal Protections
		Protective Technology	Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	
DETECT	Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.	Anomalies & Events	Anomalous activity is detected in a timely manner and the potential impact of events is understood	Security Event Detection, Monitoring, & Alerting
		Security Continuous Monitoring	The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.	
		Detection Processes	Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events.	
RESPOND	Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.	Response Planning	Response processes and procedures are executed and maintained, to ensure timely response to detected cybersecurity events.	Security Incident Management
		Communications	Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies.	
		Analysis	Analysis is conducted to ensure adequate response and support recovery activities.	Investigation & Discovery
		Mitigation	Activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident.	Disaster Recovery Planning
RECOVER	Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.	Recovery Planning	Recovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity events.	Business Continuity Planning
		Improvements	Recovery planning and processes are improved by incorporating lessons learned into future activities.	
		Communications	Restoration activities are coordinated with internal and external parties, such as coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors.	Incident Recovery

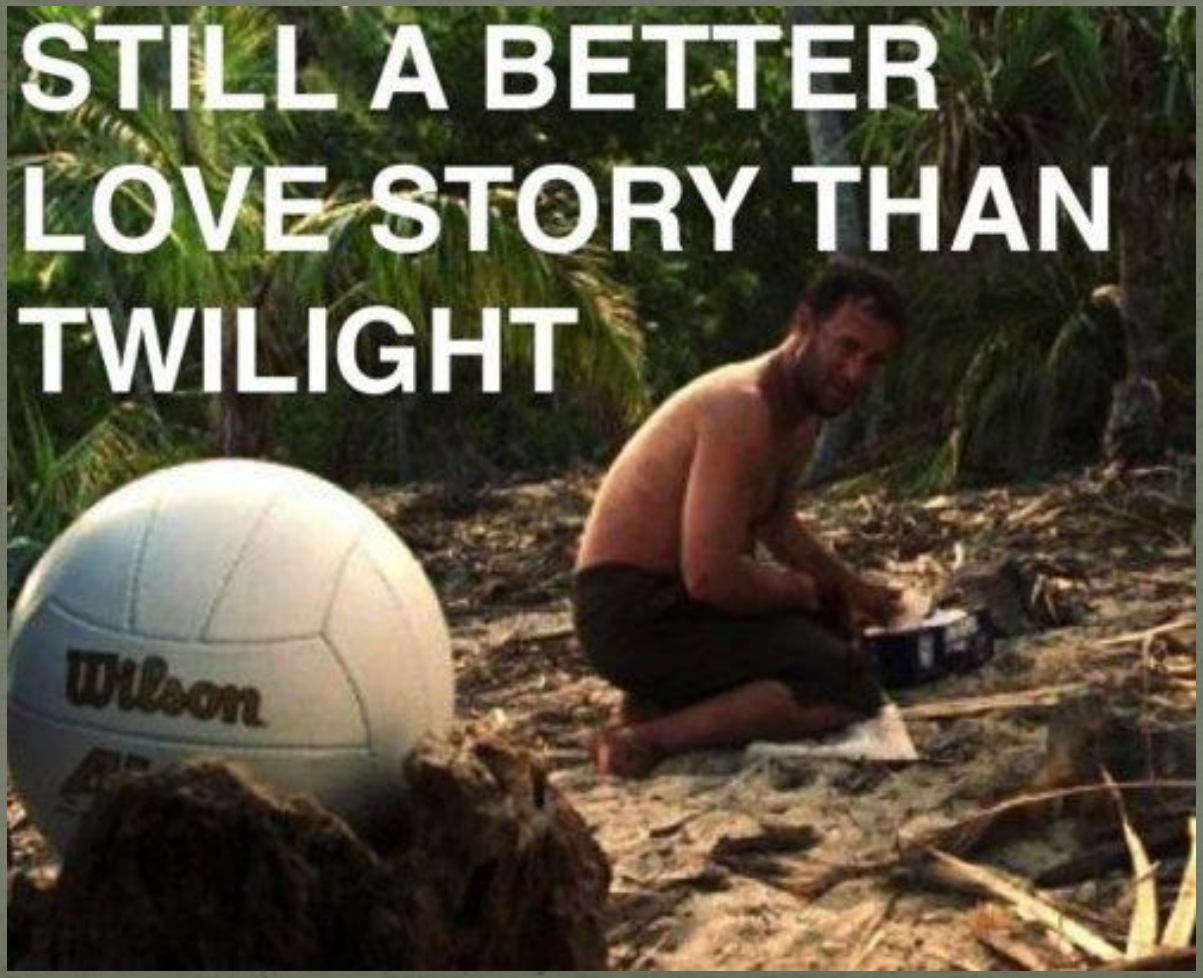

THIS FECES
IS NO LONGER
FIGURATIVE
memegenerator.net

So Why is this important?


BECAUSE
REASONS

No Man is an Island

Circle!! →




PARTY BALANCE
You've got to have at least one member of each of the four basic classes or you won't survive this dungeon crawl.

There is no “u” in team

In summary….


GROW UP,
BE A UNICORN,
STAB PEOPLE WITH YOUR HEAD.

PART MAN,
PART MACHINE,
PART UNICORN,
ALL COP.

Questions?

- Contact – CRob@RedHat.com
- Tweets - @RedHatCRob