

Protecting Critical Infrastructure from Our Bad Habits

Jerry L. Bowman, RCDD, RTPM, NTS, CISSP,
CPP, CDCDP
Square Mile Systems - US
Bethel, Ohio, USA

David Cuthbertson, MBCS, MIOD
Square Mile Systems - UK
Cirencester, Gloucestershire, United Kingdom



2017 BICSI *Fall*
CONFERENCE & EXHIBITION
SEPTEMBER 24-28 | LAS VEGAS, NV

- 1998 - Presidential Decision Directive 63 (PDD-63)
- 16 critical infrastructure sectors that compose the assets, systems, and networks, whether physical or virtual
- Vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety
- All rely on IT systems!

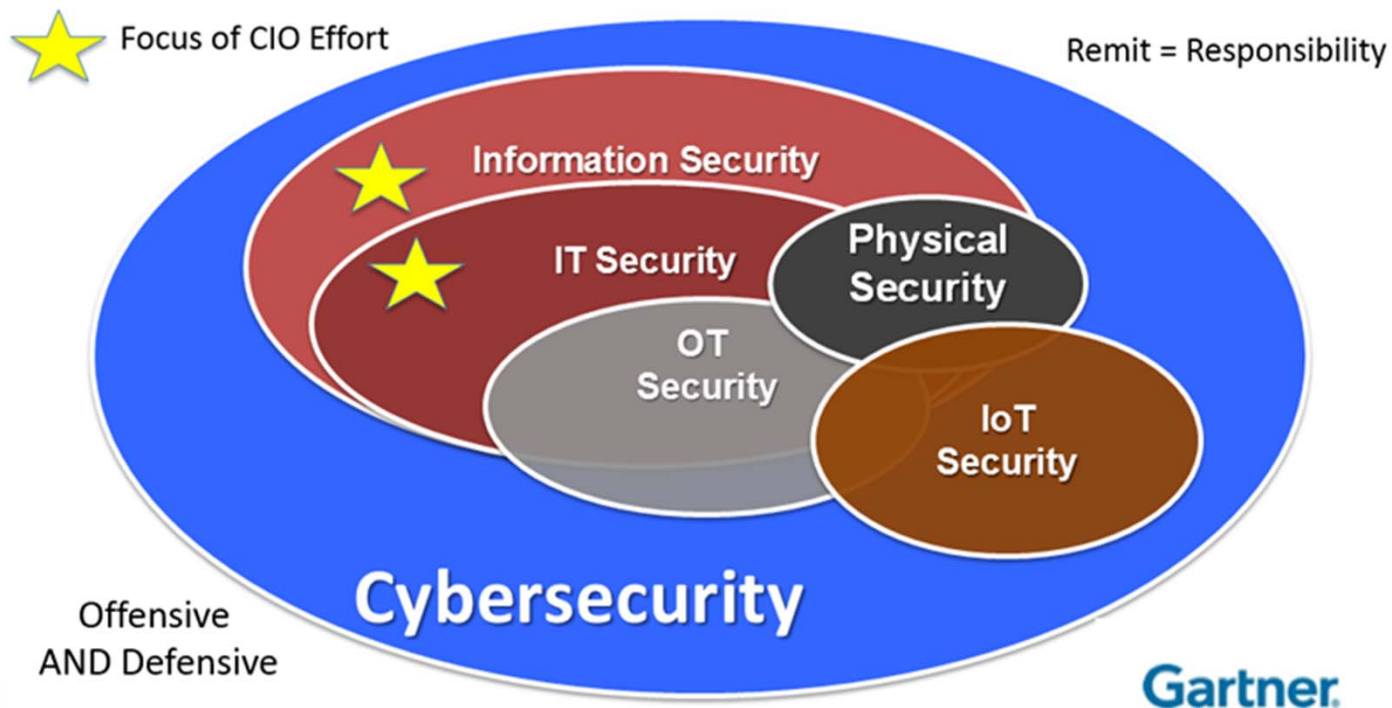
CRITICAL INFRASTRUCTURE SECTORS

	Agriculture and Food		Banking and Finance		Chemical
	Commercial Facilities		Communications		Critical Manufacturing
	Dams		Defense Industrial Base		Emergency Services
	Energy		Government Facilities		Healthcare and Public Health
	Information Technology		National Monuments and Icons		Nuclear Reactors, Materials and Waste
	Postal and Shipping		Transportation Systems		Water

Source: http://www.dhs.gov/files/programs/gc_1189168948944.shtm

Disruptive Security Evolution

Definition: The Expanding Remit of Security



Source: Top Security Trends and Takeaways for 2014, C. Byrnes, Gartner

Bad Habit #1: Poor Situational Awareness

- Knowing what's going on around you
- What do I have?
- Where is it?
- How much of it do I have?
- What would happen if I changed it or it stopped working?
- First and core principle for recent standards
 - NIST Cyber Framework – “IDENTIFY”
 - CCS Critical Security Controls – “INVENTORY”
 - National Governors Association – “ALLOCATE”



Protecting Against Deliberate or Random Acts?

- Random
 - Viruses, ransomware
 - Consequential
- Deliberate
 - Organized teams – nation states, criminal, terrorist
 - Power infrastructure USA, Ukraine, UK, Ireland, Israel
 - Sweden - Air traffic control, driver licensing (IBM outsource)
- Grudge
 - Customers, staff, suppliers, personal

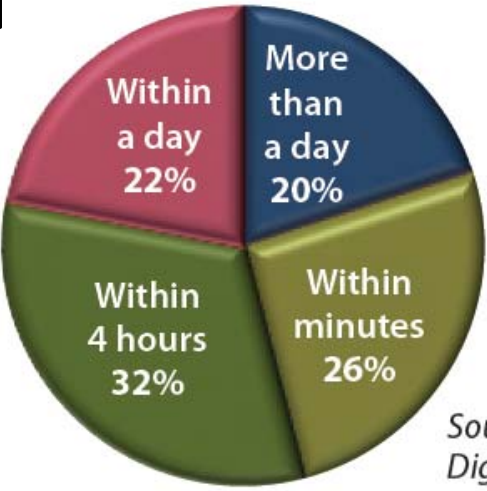
Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
PR	Protect	PR.AC	Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

Sub- Cat Unique Identifier	Sub-Category
ID.AM-1	Physical Inventory
ID.AM-2	Software Inventory
ID.AM-3	Communication and Data Flows
ID.AM-4	External Information Systems
ID.AM-5	Priority Resource and Classification
ID.AM-6	Roles and Responsibilities

The NIST Cybersecurity Framework

Helping with Situational Awareness

What is the Cost of Finding a Down Server?



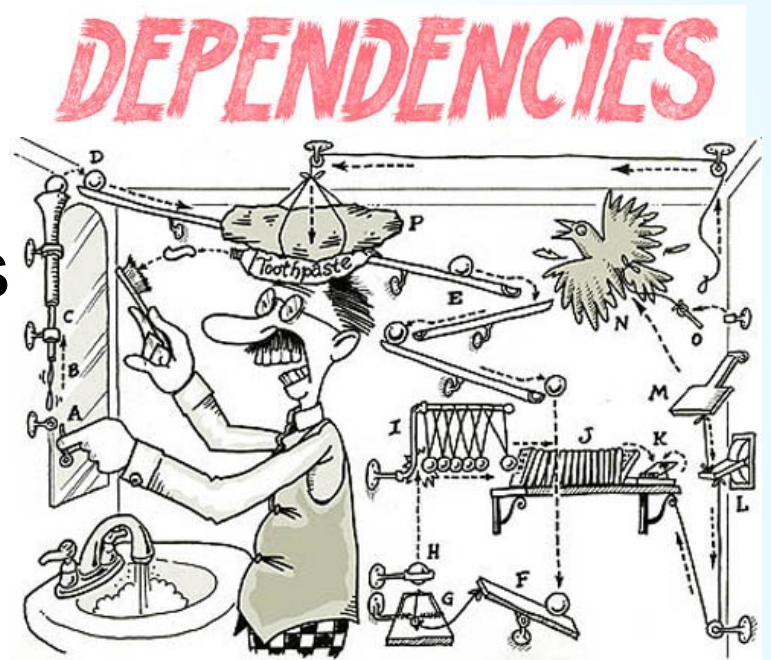
Source: Digital Realty Trust

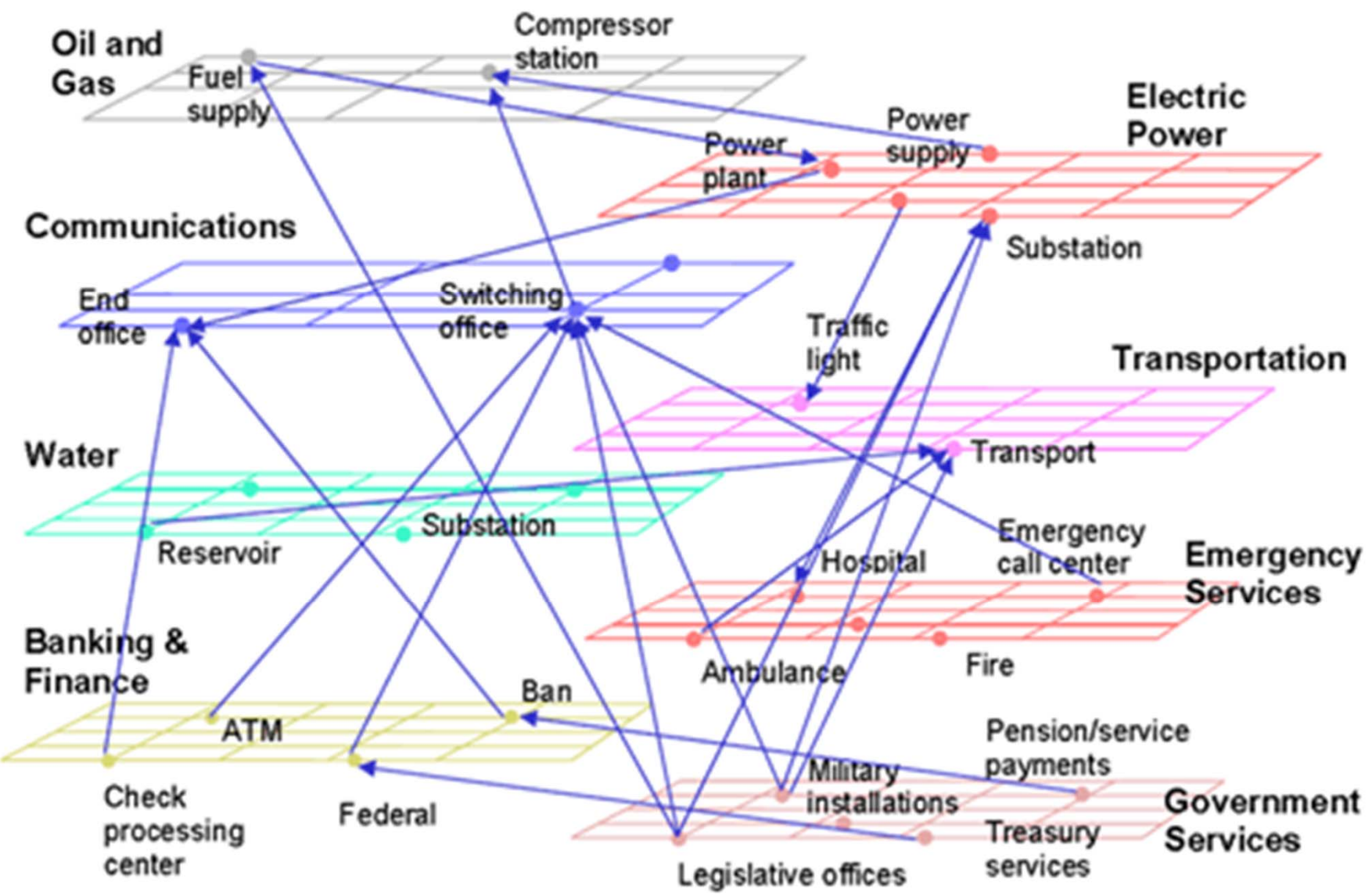
Source: Rand Group

	Minutes	4 Hours	A Day	> A Day
Low	\$50,000	\$400,000	\$2.4M	\$\$\$\$
Mid	\$150,000	\$1.2M	\$7.2M	\$\$\$\$
High	\$1.5M	\$12M	\$72M	\$\$\$\$

Bad Habit #2: Unknown Dependencies

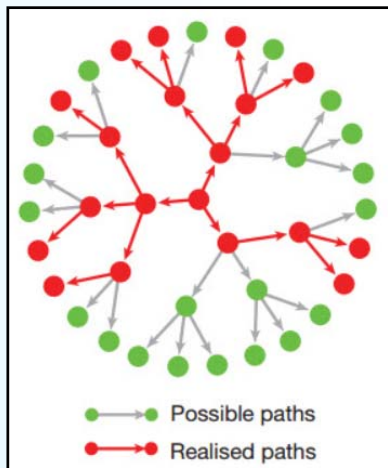
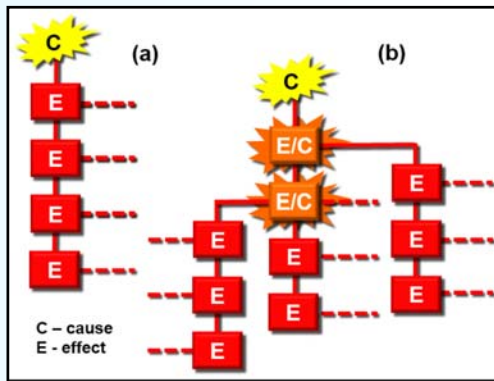
- If I unplug this cable will anyone scream?
- What departments or business services will be impacted if this cabinet was removed?
- Rube Goldberg Machine?
- Cascading events?





**C
O
M
M
U
N
I
C
A
T
I
O
N
S**

2001 Baltimore Train Crash

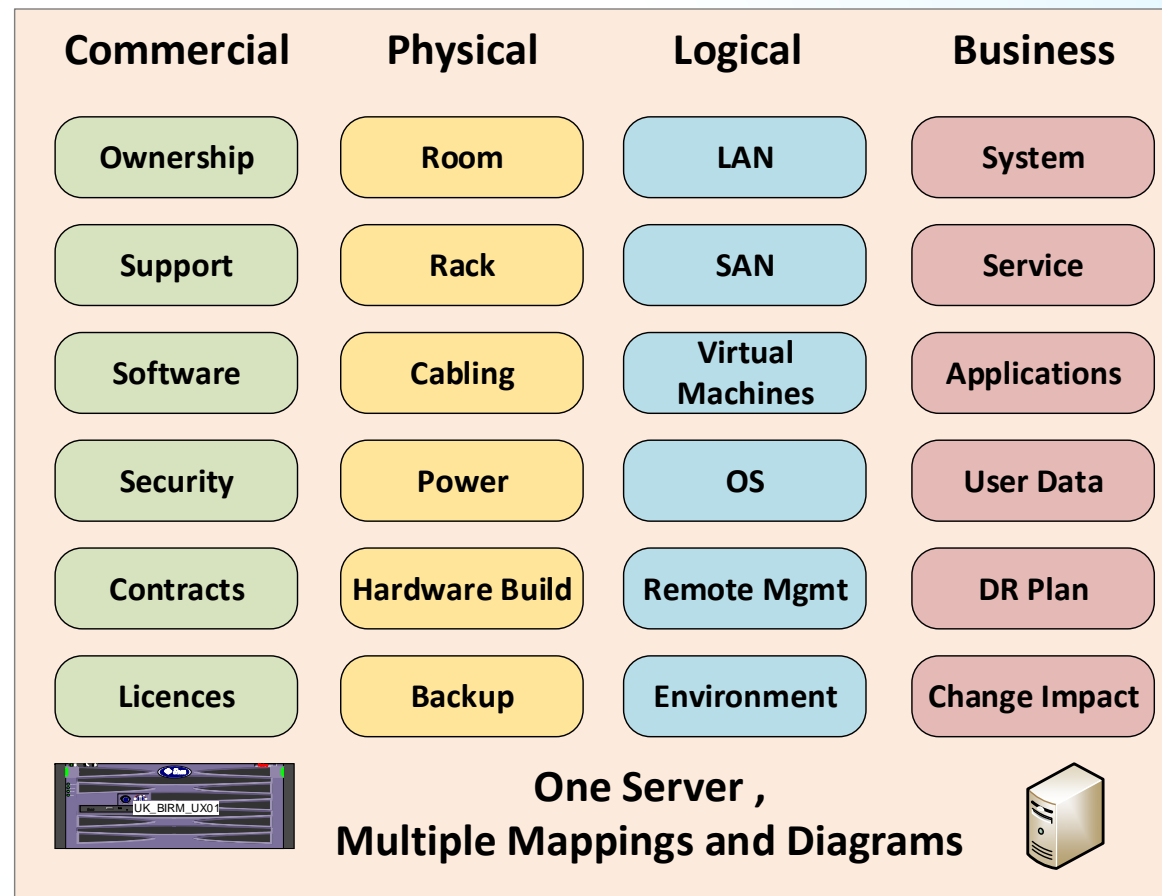


- A train 3 – locomotives/60 cars derailed in Baltimore tunnel
- Ruptured a tanker railcar full of liquid tripropylene
- Not considered hazardous to human health or the environment... but it does burn
- The flames interacted with hydrochloric acid in a different tank car.
- Created black toxic smoke spread across the Baltimore downtown area, forcing the authorities to evacuate for 2 days
- A burst water main flooded local streets and freight traffic was heavily affected for more than five days.
- The joint effect of water, fire and wreckage compromised three major fiber optic lines that lay in the tunnel, generating severe disruption of Internet services in the northeast United States

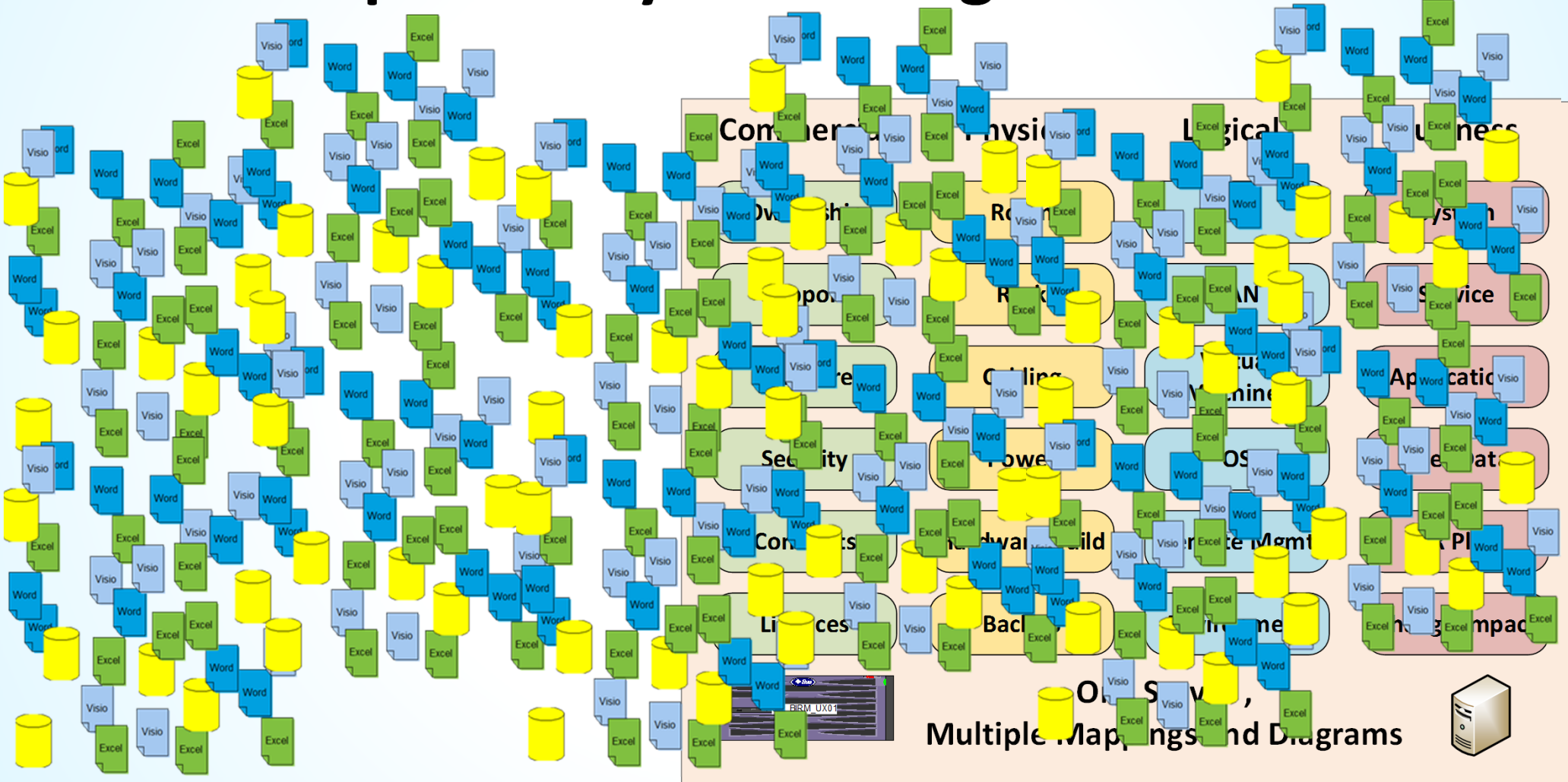
Source FEMA Training Manual

Dependency Knowledge Is Vital

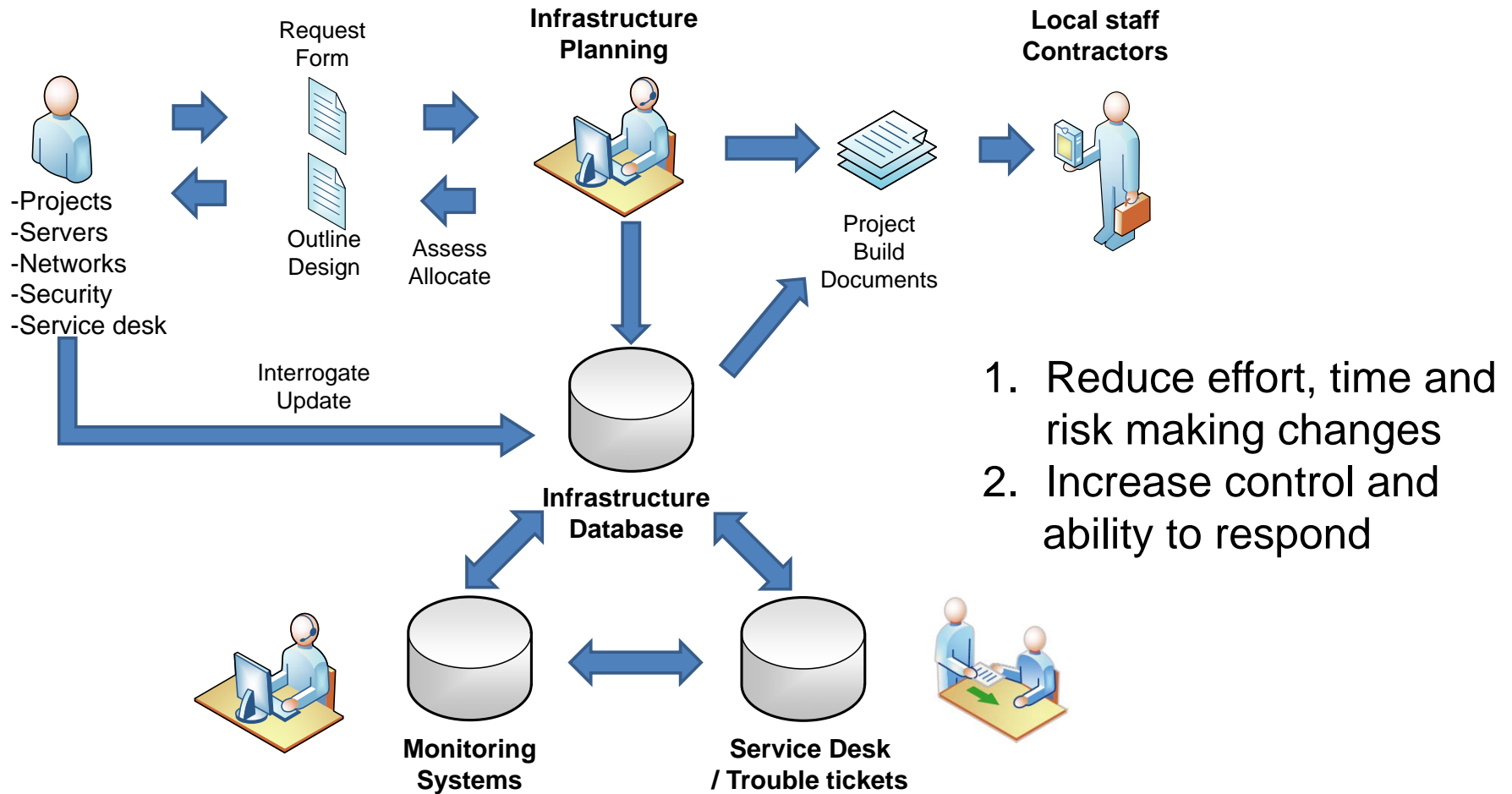
- Day to day changes
- Major projects
- Change impact
- Situational awareness



Dependency Knowledge Is Vital

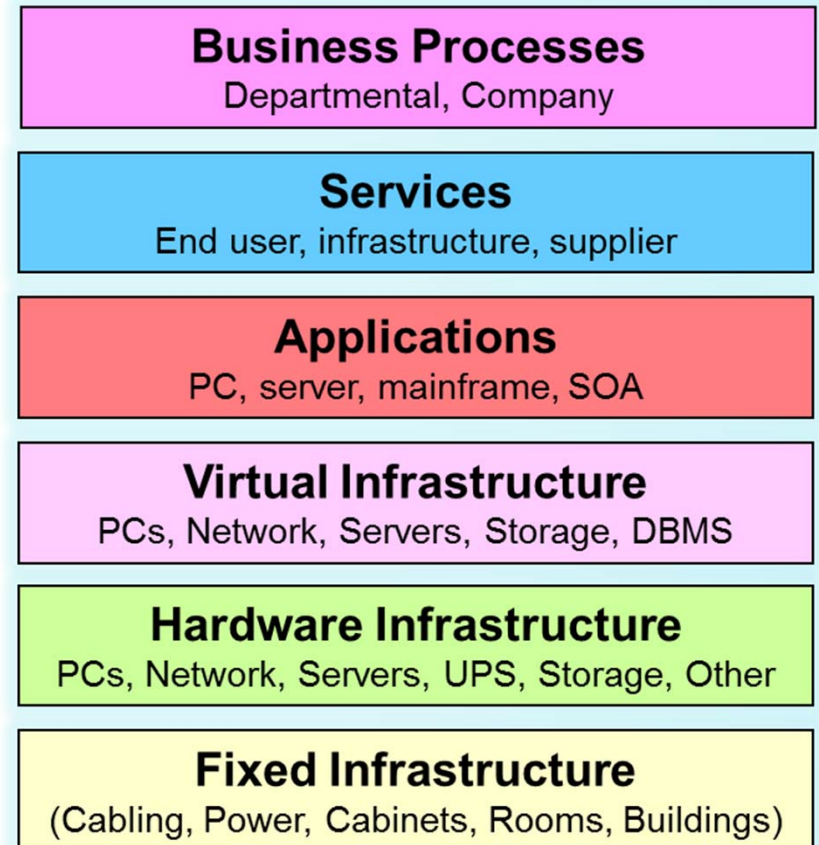


Integrated Change Management



Bad Habit #3: Play Career Roulette

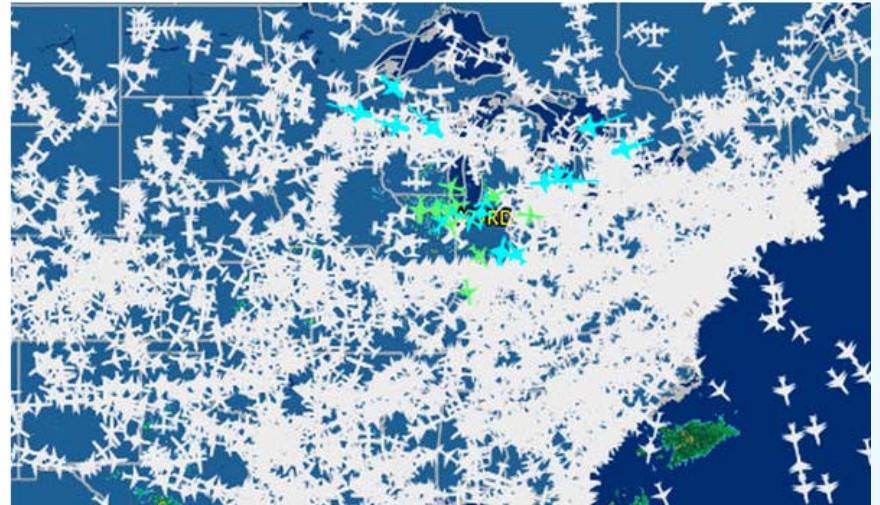
- Do we have enough trusted information to make informed real-time decisions?
- What do I do when I see non-conformance or bad practice?
- Who will take the lead to develop processes that cross technology boundaries?



Buildings can't be built on sand.....

Chicago FAA Arson/Suicide

- Chicago air traffic control center
- Disgruntled contract employee sets fires and attempts suicide during morning rush hour
- All Chicago air traffic rerouted or grounded for 5 hours
- 20 of 29 server racks destroyed
- 2,000 flights cancelled in/out of Chicago airports
- The contractor was authorized to be at the site
- 1 Week Later operations back to 80% - only 180 flights cancelled
- FAA has ordered a review of the security plans and contingency plans
- Estimated to be weeks until air traffic returns to normal



Informed, Real-Time Decisions

- CIO needs to implement VoIP across enterprise
- 92 Campuses in 60 countries, 282 data centers
- Managed services contract - ignored infrastructure documentation
- Required 20 Engineers/ 9 months / \$6M / 3.5 TB for audit and gap analysis before planning
- Led to strategy to capture ITAM data during ITSM process – centralized, updated Asset Mgmt. Database
- Reduced visits to closets from 5 per closet per year down to 2 per closet, per year



Bad Habit #4: Trusting Blinking Lights

- Activity is not performance
- Green indicators are not always the truth
- People and process issues can not be solved by “more technology”
- IT Service Management helps predict and avert issues;
 - Capacity
 - Incident
 - Event
 - Request
 - Availability
 - Security
 - Change
 - Trouble

What Should Be **RED**, **AMBER** or **GREEN** ?



The CCTV screens have gone blank



I need to install my 20 new servers



We have to rollback yesterdays s/w update



We're pulling out the old CAT 3 cable



This update will disable anti-virus s/w



We are updating the payroll system



We are doing a DC generator test



Need to change the firewall rules



My mobile calendar hasn't been updated



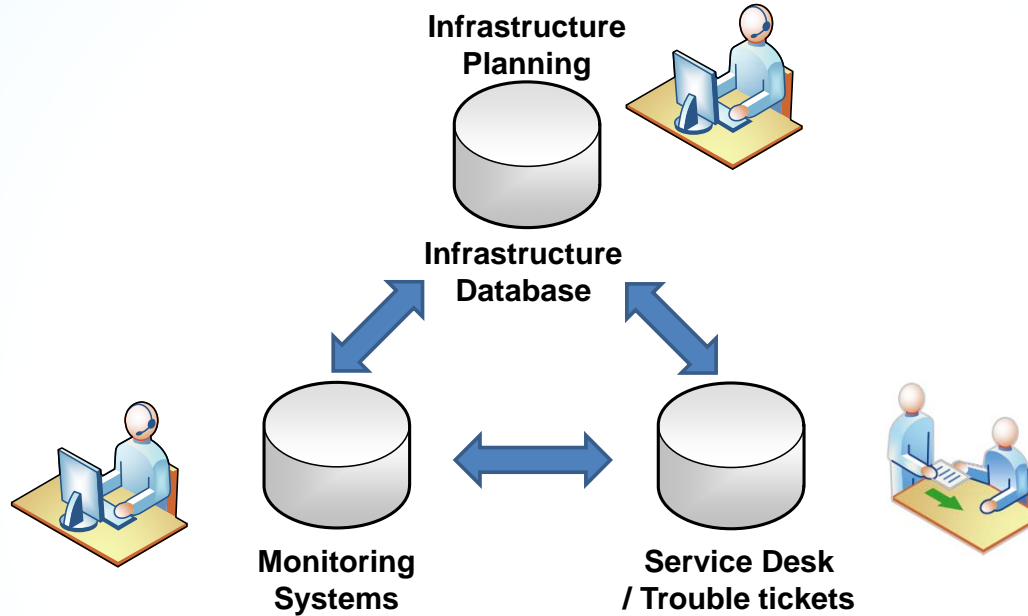
My PC is going slow or has it stopped?



I can't access the server



Urgent, bug fix for yesterdays website crash




Bad Habit #5: Capacity Mystery

1025

DATE _____

PAY TO THE ORDER OF _____ \$

_____ DOLLARS  Security Features
Included
Details on Back.

MEMO _____

⑆0000000000⑆ ⑆0000000000⑆ 1025

Bad Habit #5: Capacity Mystery

- If there are checks in the checkbook, do I have money in the bank?
- “If there is a power outlet – I have power.”
- If there’s an open outlet or data port do I have enough capacity?
- Real capacity is more than an open port – denial of service can be self inflicted
- All tickets require 2 trips to the remote site – 1 to check for capacity and the 2nd to do the work.
- Plus the other unnecessary trips to check, audit and document inventory and connections.



Underfloor Capacity?



Port Capacity?



Summary

- Our bad habits result in
 - Increased cost managing changes, projects and risks
 - Lack of confidence in the “team” and their level of control
 - Increased exposure to internal/external attack disruption
- Some simple steps
 - Understand what you have
 - Understand the dependencies
 - Develop processes to keep both up to date (and save money)



Additional Information

Jerry L. Bowman, RCDD, RTPM, NTS, CISSP, CPP, CDCDP
Square Mile Systems - US
Email: Jlbowman@squaremilesystems.us

David Cuthbertson, MBCS, MIOD
Square Mile Systems - UK
Email: David.cuthbertson@squaremilesystems.com

www.tiaonline.org

TIA 568 Family of Standards

www.bicsi.org

ICT Standards and Best Practices

www.squaremilesystems.com Visio Utilities | Videos | Downloads

www.assetgen.com

Infrastructure Management Software Suite



**Jerry L. Bowman, RCDD, RTPM, NTS, CISSP,
CPP, CDCDP
Square Mile Systems - US
Bethel, Ohio, USA**

**David Cuthbertson, MBCS, MIOD
Square Mile Systems - UK
Cirencester, Gloucestershire, United Kingdom**



**2017 BICSI *Fall*
CONFERENCE & EXHIBITION
SEPTEMBER 24-28 | LAS VEGAS, NV**