

RSAC[®]Conference2020

San Francisco | February 24 – 28 | Moscone Center

HUMAN
ELEMENT

SESSION ID: TECH-F02

Prioritizing the Top 20 on a Shoestring



William Bailey

VP Information Security

Police & Fire FCU

@dalanshark

#RSAC

Achieving the Goal

- Need to Protect Systems
 - Regulations
 - Contractual
- Budget is Limited
 - Or, Non-existent
- Want to Adopt Best Practices
 - Read about CIS 20 Critical Controls
- No Strategy Already Exists... Where to Start?



Start → Move Up → Mature



V7.1

Basic

- 1 Inventory and Control of Hardware Assets
- 2 Inventory and Control of Software Assets
- 3 Continuous Vulnerability Management
- 4 Controlled Use of Administrative Privileges
- 5 Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
- 6 Maintenance, Monitoring and Analysis of Audit Logs

Foundational

- 7 Email and Web Browser Protections
- 8 Malware Defenses
- 9 Limitation and Control of Network Ports, Protocols and Services
- 10 Data Recovery Capabilities
- 11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
- 12 Boundary Defense
- 13 Data Protection
- 14 Controlled Access Based on the Need to Know
- 15 Wireless Access Control
- 16 Account Monitoring and Control

Organizational

- 17 Implement a Security Awareness and Training Program
- 18 Application Software Security
- 19 Incident Response and Management
- 20 Penetration Tests and Red Team Exercises

Just the Top Five – 85% of 2017 DBIR Breaches

| | NIST CSF | ISO |
|---|--------------------|--------------------|
| Inventory & Control of Hardware Assets | ID.AM-1 ID.AM-3 | A.7.1.1 |
| Inventory & Control of Software Assets | ID.AM-2 ID.AM-6 | A.12.5.1 |
| Continuous Vulnerability Management | ID.RA-1 ID.RA-2 | A.12.6.1 |
| Controlled Use of Administrative Privileges | PR.AC-4 | A9.1.1 |
| Secure Configuration of HW & SW | PR.IP-1 | A14.2.4 A14.2.8 |

Building Blocks

- Policies
- Know What You Have
- Don't Use Defaults
- Create Standards
- Protection – 100%?
- Follow Procedures
- “Social Networking”
- Learn

The **programmer** got stuck in the shower
because the instructions on the
shampoo bottle said,

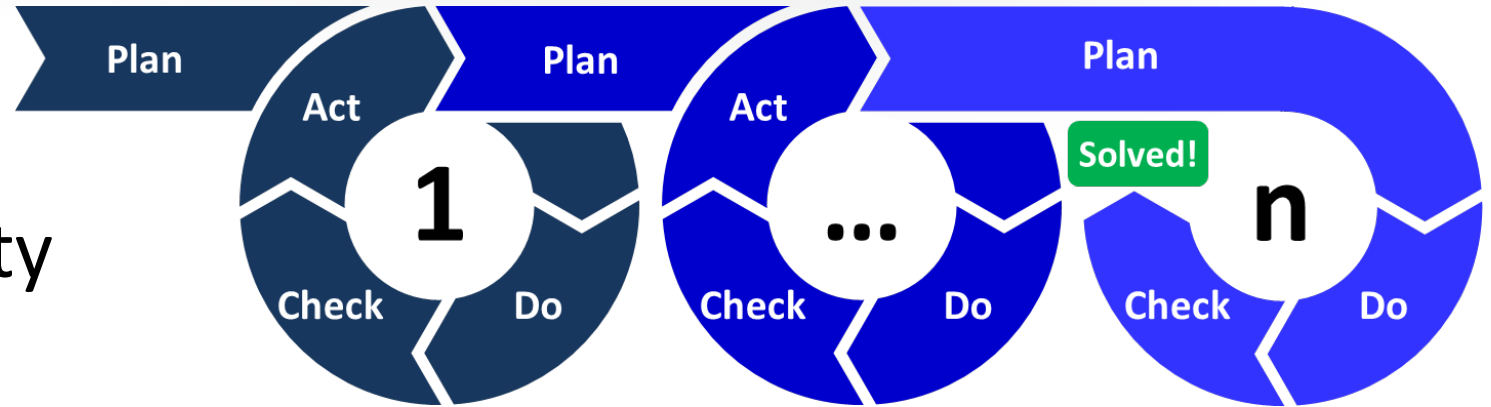
Lather, Rinse, Repeat.



DBWebSolutions.com

Policies

- Going Forward...
- Match Your Capability
- Measurable
- Incremental Changes, Reviewed Annually
- Exceptions Possible, Exceptions Reviewed
- Just enough specifics
 - Standards, baselines, procedures, guidelines



Know What You Have

Assets

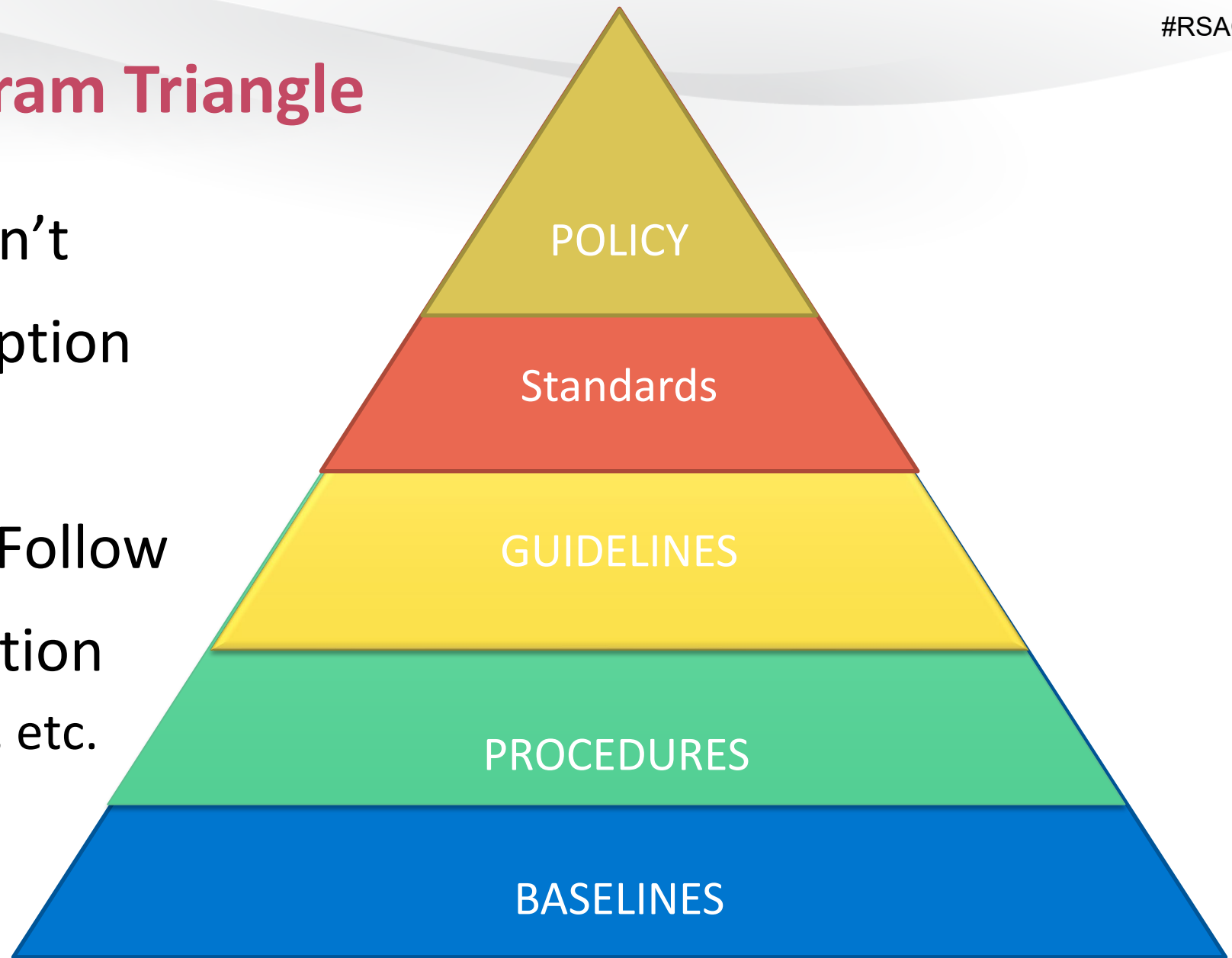
- Hardware
- Software
- Information
- Vendors

Tools (examples)

- Nmap / ZenMap
- BRO / Zeek
- Spreadsheets (ugh)
- Fun with Scripts
- Learn the Business
- Talk with Accounting / Contracting

Cybersecurity Program Triangle

- High-Level Do or Don't
- Must Use XYZ Encryption
- "Least Privilege"
- Recipe Anyone Can Follow
- Allow for Customization
 - Windows 1903, 2003, etc.



Don't Use Defaults - RTFM

- Built-in Accounts
- Password(s)
- Port(s)
- Logging options



Create Standards

Why?

- Assist Troubleshooting
- Consistency of Experience
- Easier to Secure
- Less “Whack a Mole”
- Don’t Have to Support Everything

How?

- Gold Images
- Hardware Platforms
- Software Platforms
- Process to Introduce New Technologies

Protection – How Much?

- Anti-malware – managed
- Backups – encrypted
- Encryption – in motion, at rest
- Limit Sessions
- Passwords
- Remember “Best of Breed” vs. What You Need
- Updates – Install them



Don't Have What You Don't Need

- Privileges – Remove Admin, Ability to Install Software
- User Accounts - Set Expiration Dates Before, Not Later
- Software – Remove Bloatware, Components
- Data – Move from endpoint to server, and dispose at end of life
- Extra Features = Extra Bugs!



Follow Procedures

- Can't document everything on the first day,
- But you can require better documentation for any new:
 - Hardware implementation
 - Software deployment
 - Vendor selection

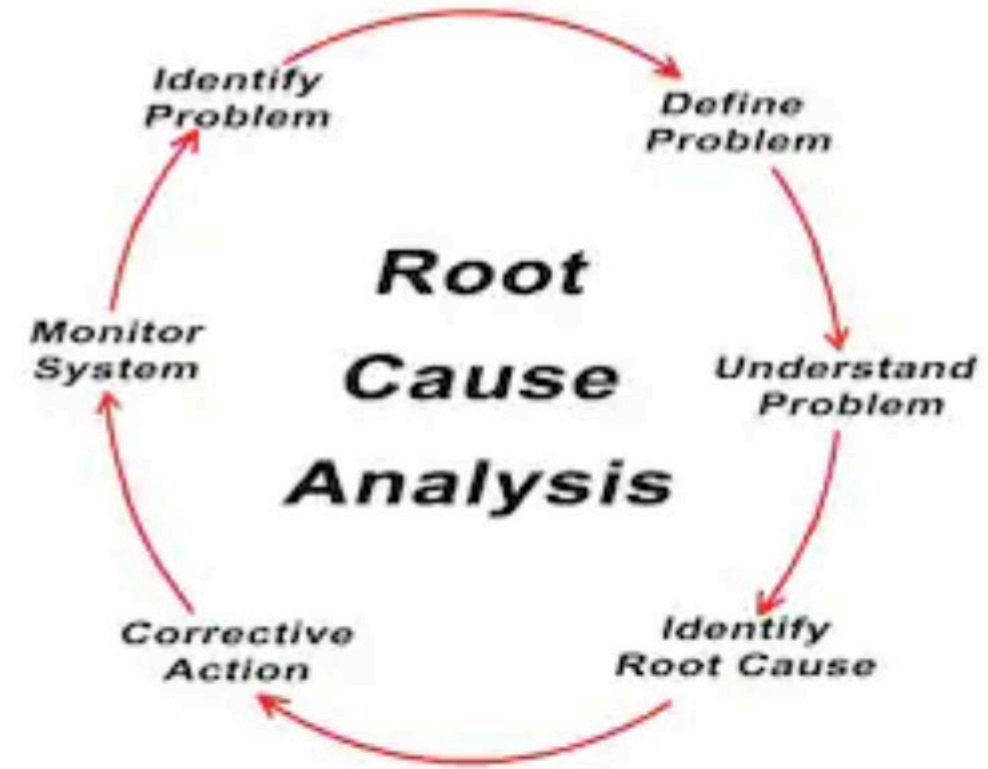
“Social Networking”

- Discussions
 - These may be informal
- Interviews
- Survey(s)
- Walkthrough(s)
- Industry



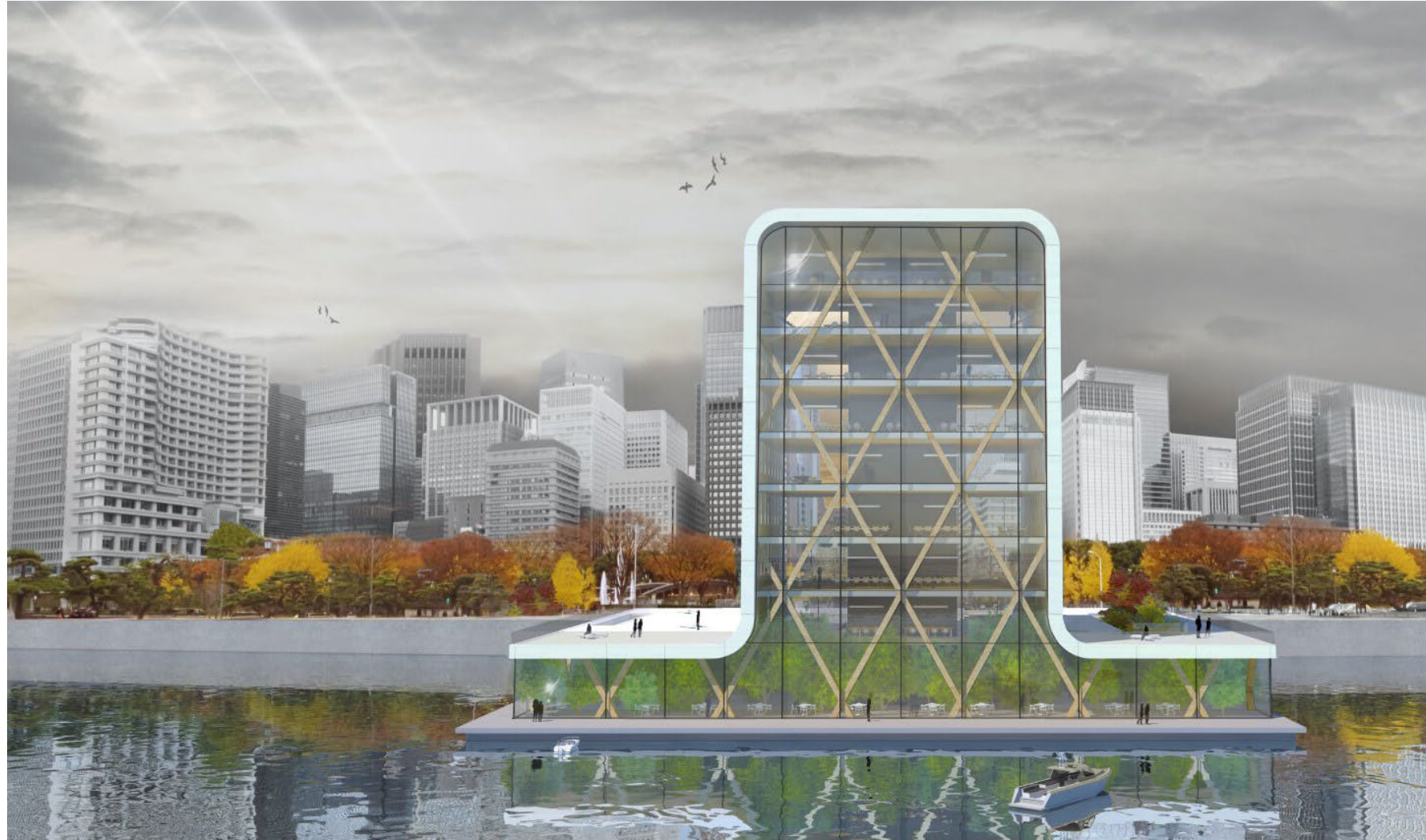
Learn

- Perform Root Cause Analysis
- Look at Threat Intelligence – use low-cost resources
 - Information Sharing (ISACs) – e.g. FS-ISAC, H-ISAC, MS-ISAC
 - Volunteer at the event = Reduced Admission
 - Mailing List(s)
 - Vendor(s)
- Vendor Training
- What or Who is on the News?



Summary

- Policies Drive the Effort
- Small Elements Bring Great Benefits
- Remember that “Rome Wasn’t Built in a Day”



Apply

- Request the CIS 20 Controls Document(s)
 - <https://www.cisecurity.org/controls/cis-controls-list/>
- Dust off your organization's policies
- Look around at your organization. Learn at first
- Look at peers
- Draft *incremental* project plans / business plans by year

RSA[®]Conference2020

San Francisco | February 24 – 28 | Moscone Center

HUMAN
ELEMENT

SESSION ID:



#RSAC

“Apply” Slide

- Bullet point here (see slides 5 – 8 for instructions)
- Bullet point here
- Bullet point here

RSA[®]Conference2020

RSA[®]Conference2020

RSA[®]Conference2020