# Integrating Business Risk and IT Risk

**Bobbie Stempfley**

**Dec 6, 2016**

MITRE

# Established to Serve the Public Interest

established
**1958**

**not-for-profit**

**conflict-free**
environment

science **&**
technology

**Part of the ecosystem of federal research centers**



Approved for Public Release; Distribution Unlimited. Case Number 16-0634

MITRE

# The New Frontier of Cyber Risk

**Convergence goes far beyond TV and telephone**

- Billions of smart connected devices

**By 2020, 26 Billion (Gartner) or 212 Billion (IDC) devices internet connected**

**Security concerns:** scale, pervasiveness, and persistence of threats against much larger attack surface

**Lack of built-in security can result in:**

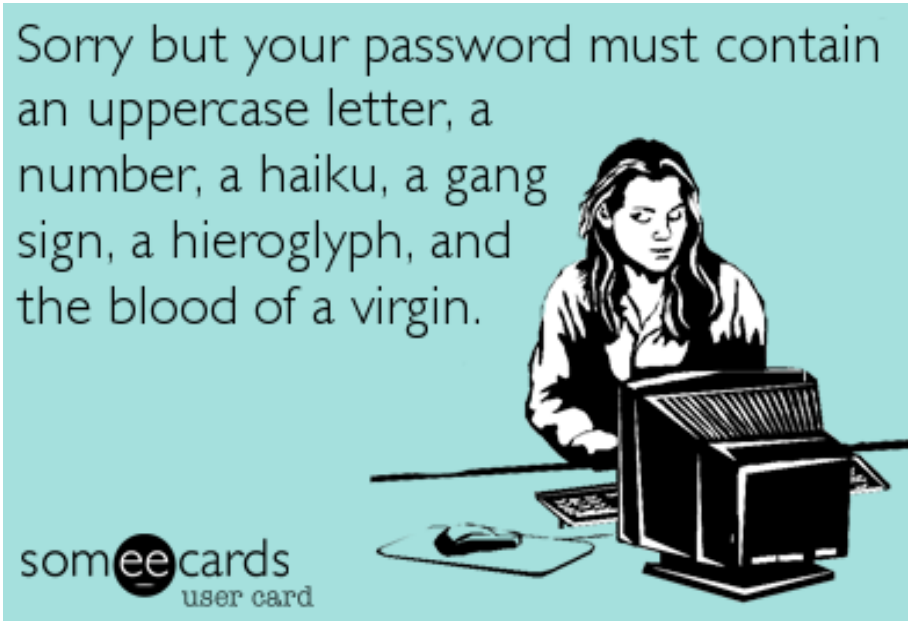
- Unauthorized access to services and data
- Exposure of privacy data
- Modification or deletion of data
- Denial or disruption of access to services
- Installation of backdoors and malware
- Loss or damage of critical infrastructures

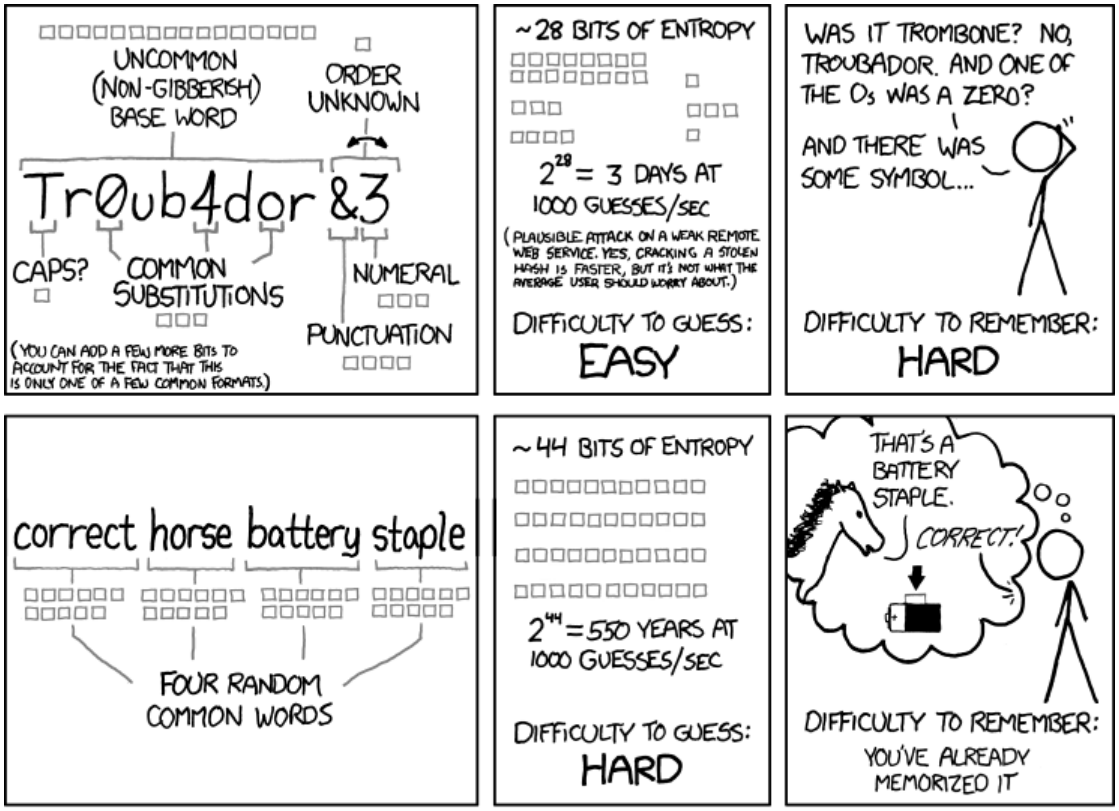

**Security engineering workforce can't keep up**

**Need for affordable, scalable cyber defense**

**The password must:**

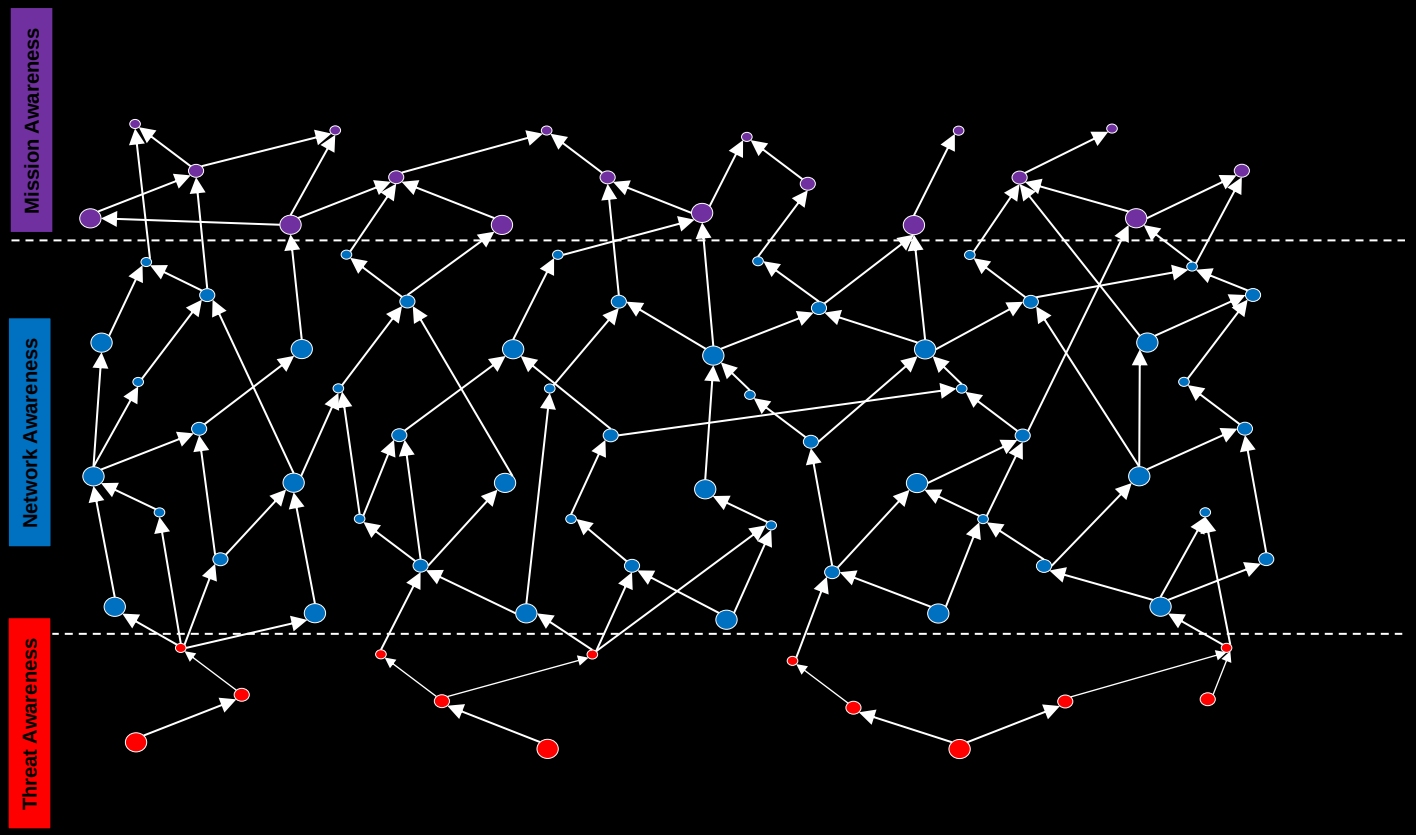
- **have at least 12 characters**
- **have at least 1 non-alphanumeric characters**
- **have at least 1 letters**
- **have at least 1 digits**
- **not contain a dictionary word (e.g. xyzw1o2r3d)**
- **not be the profile ID or name**
- **not be the profile ID or name backwards**
- **not contain the profile ID or name**
- **not contain the profile ID or name backwards**
- **not contain your user name or any part of your full name**
- **contain elements from three of the four following types of characters:**
  - English upper case letters
  - English lower case letters
  - Westernized Arabic numerals
  - non-alphanumeric character
- **contain only characters available on a standard English (US) keyboard.**
- **not have 5 occurrences of the same character**
- **not be an old password**
- **allow old passwords after 730 days**






THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

# Reality is Complex




## Enterprise Architecture

ARCON
ISO 19439 Ent Modeling
TOGAF (Open Group)
DNDAF (CAN)
DoDAF (US DoD))
MODAF (UK)
NAF (NATO)
FEAF (US Fed)
NIST EA Model
TEAF (US Treasury)
Zachman
etc.

???

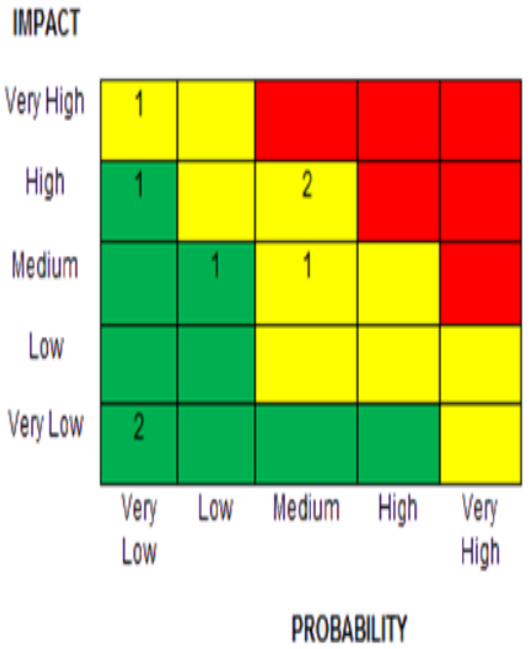
**"Out of intense complexities intense simplicities emerge”**

**-Winston Churchill**

- Business Need Validation
- Attach Findings to Approval
- Bottom Line Up Front (BLUF)

| | |
|---|---|
| Details Overview | Deadline and Driver |
| Business Justification | Issue(s) |
| Risk Evaluation | Other Observations |

- Heat Map Visualization



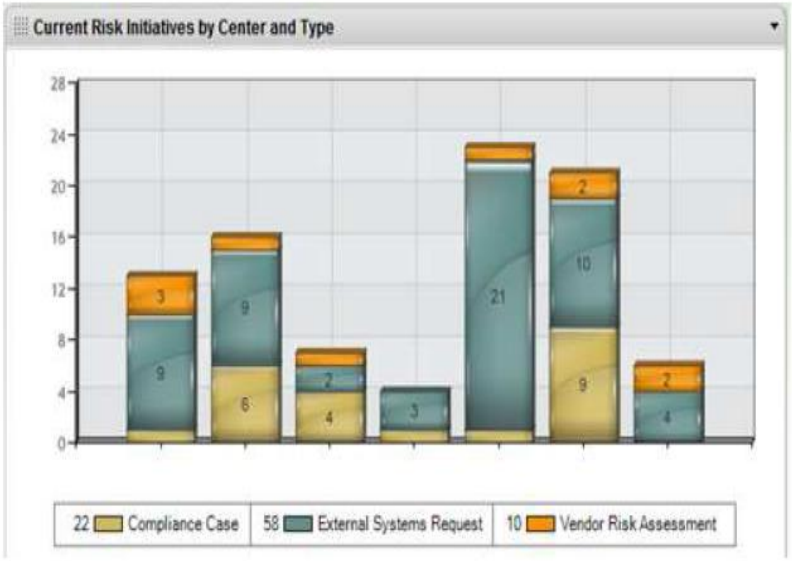
- What is current risk posture?
- What do we have deployed?
- What did we previously think?
- Something like this already?

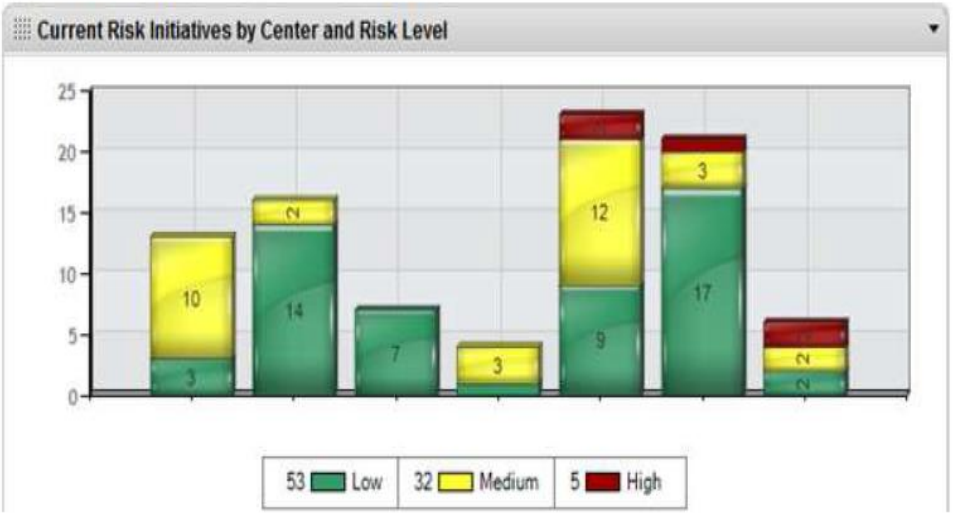
Pato

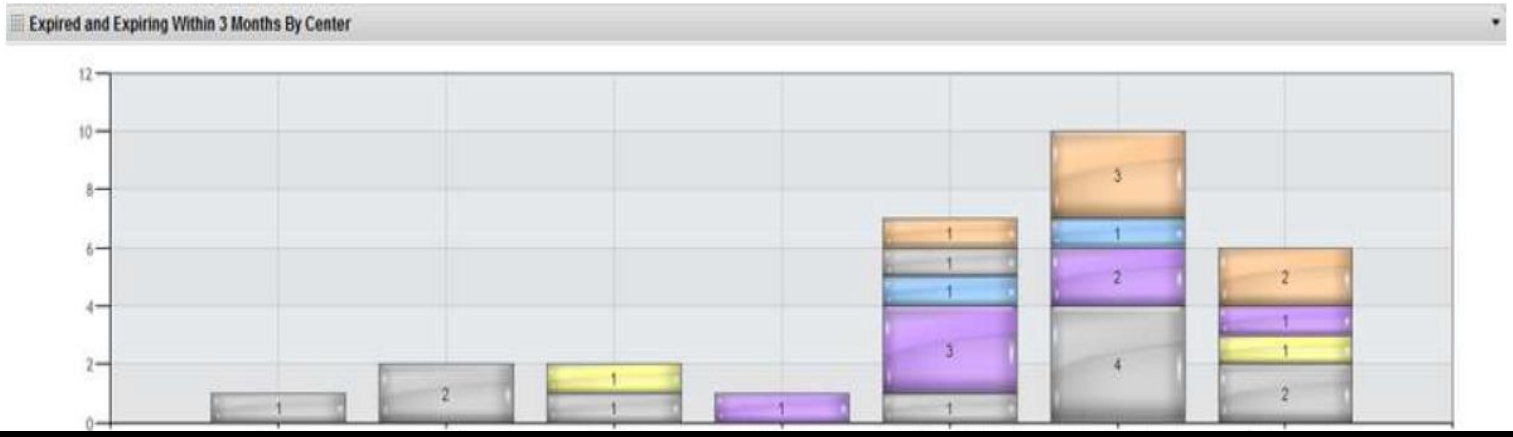
## Impact and Probability References

| | |
|---|---|
| Very High | • Highly Sensitive Data, PII, HIPAA |
| High | • Sensitive Data |
| Medium | • Bulk Internal Data Loss |
| Low | • Limited Internal Data Loss |
| Very Low | • Loss of Public or Test Data |

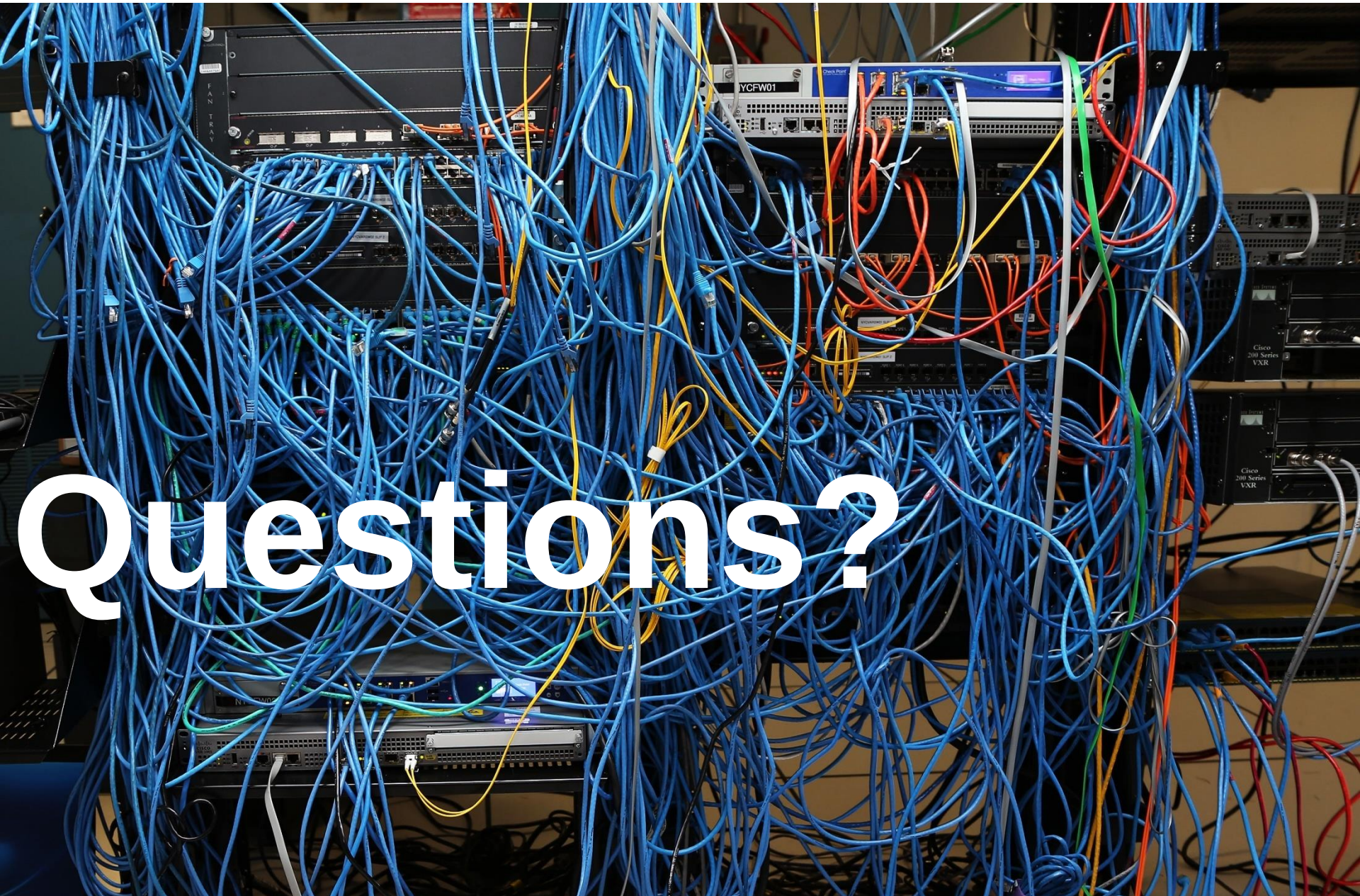
# Reporting and Dashboards



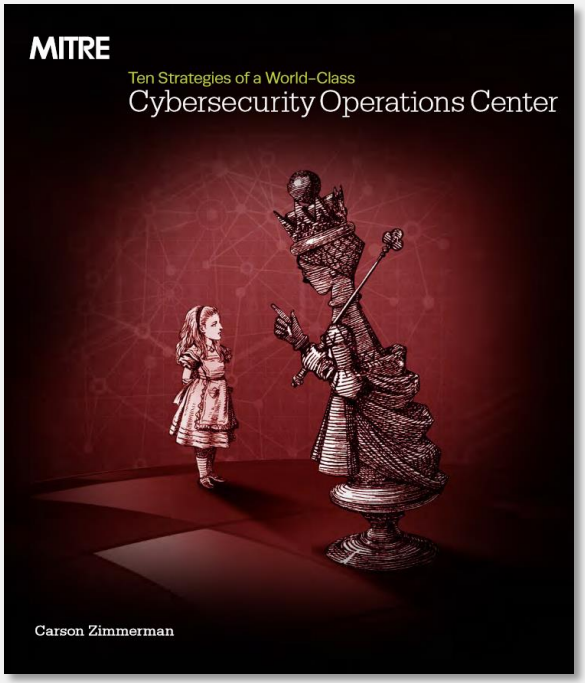

2. The Situation
4. Lead Up
The Event
The Context
1. The Person of the Meta-Leader
The Problem
The Culture
5. Lead Connectivity
3. Lead the Silo




# Questions?

# Some Resources Available for You

## Ten Strategies of a World-Class Cybersecurity Operations Center

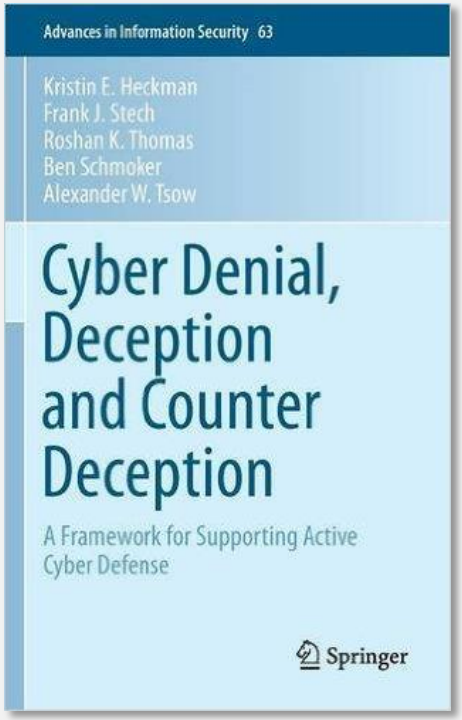



**Carson Zimmerman**

Free download at:

www.mitre.org/sites/default/files/publications/pr-13-1028-mitre-10-strategies-cyber-ops-center.pdf

## Cyber Denial, Deception and Counter Deception




**Kristin Heckman, Frank Stech, Roshan Thomas, Ben Schmoker and Alex Tsow**

## ACSC Advanced Cyber Security Center

**Information Sharing and Analysis Centers (ISACs)**

## NIST National Institute of Standards and Technology U.S. Department of Commerce

- 1800-1 Securing Electronic Health Records on Mobile Devices
- Identity - Attribute Based Access Control
- Financial IT Asset Mgmt
- Mobile Device Security

**NIST 1800 Series Practice Guides**



Approved for Public Release; Distribution Unlimited. Case Number 16-0634

MITRE