INFRAGARD MAINE PEOPLE AND THREATS

Improving your outcomes

Barb Armstrong VP Maine

Frank Appunn P Maine

Outline

1. Your Speakers and InfraGard
2. The cyber pieces represented in this session
3. Threats – where there is too much guessing
4. Human impacts: Our Adversaries and Clients
5. People remain our biggest exposure – Solutions?
6. Q&A

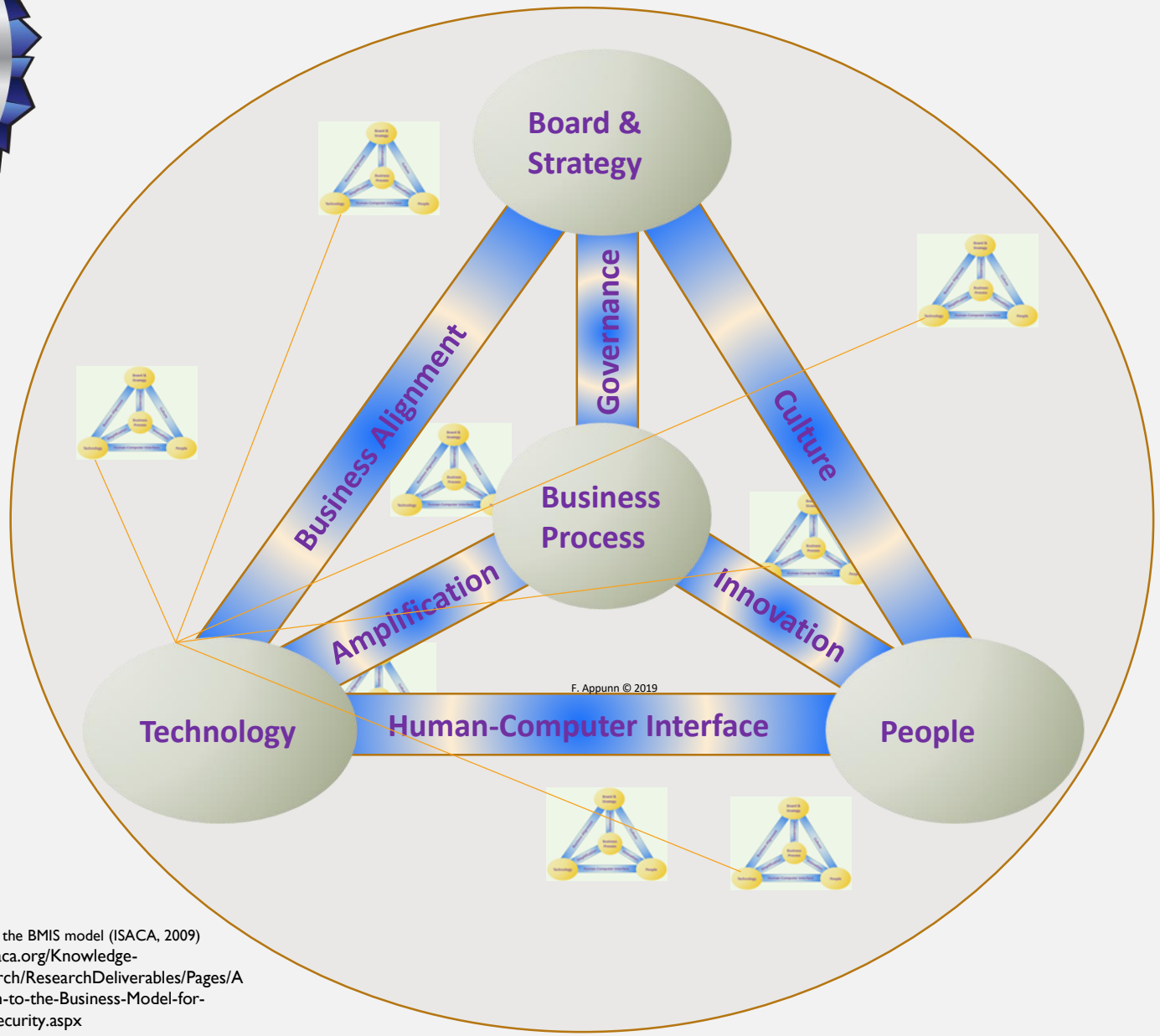
1. Your Speakers and InfraGard

- Barb Armstrong
- Frank Appunn

- InfraGard National
- InfraGard Maine
- Industry Collaboration
- Updates and Bulletins
- InfraGard Training
- Patriots Circle

2. The Cyber Pieces Represented in this Session

- Organizations — Where does technology fit?
- Risks — Parts of risk
- Risks: — Plan and operate



An extension of the BMIS model (ISACA, 2009)
http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/An-Introduction-to-the-Business-Model-for-Information-Security.aspx

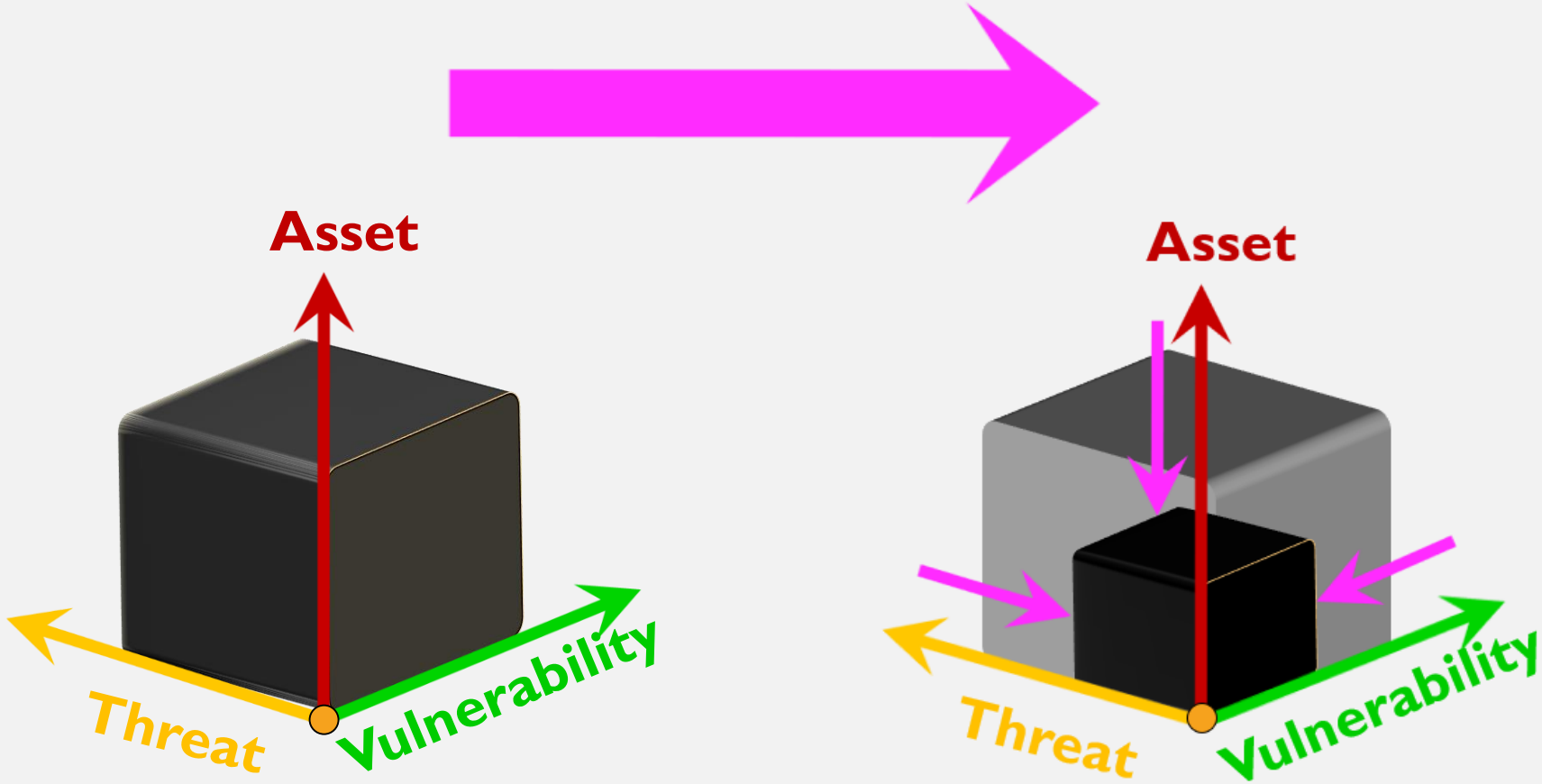
2. The Cyber Pieces Represented in this Session:

Technology and the Organization

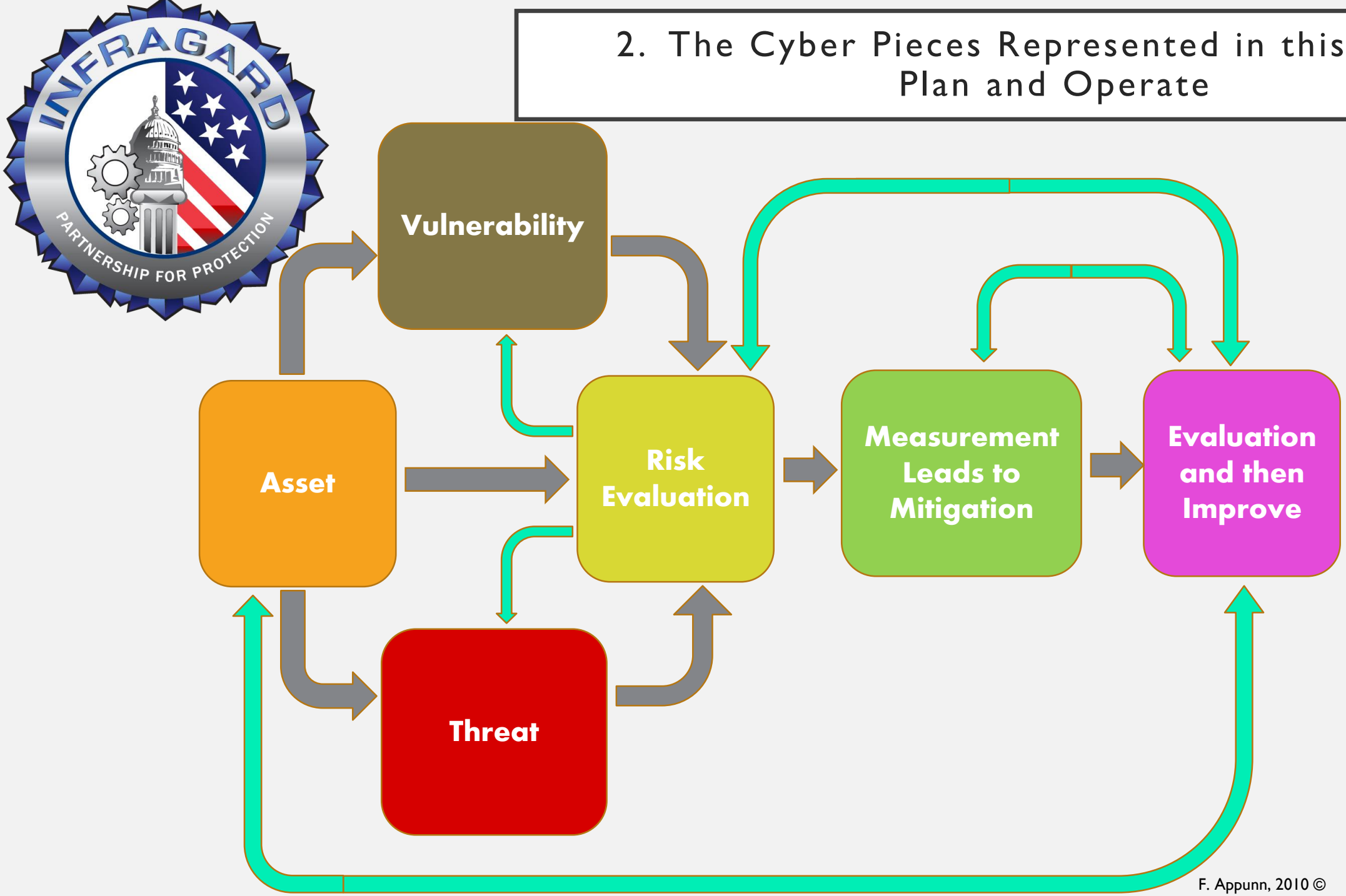
If we cannot explain it, we will not get resources to fix it

2. The Cyber Pieces Represented in this Session

Security Objectives

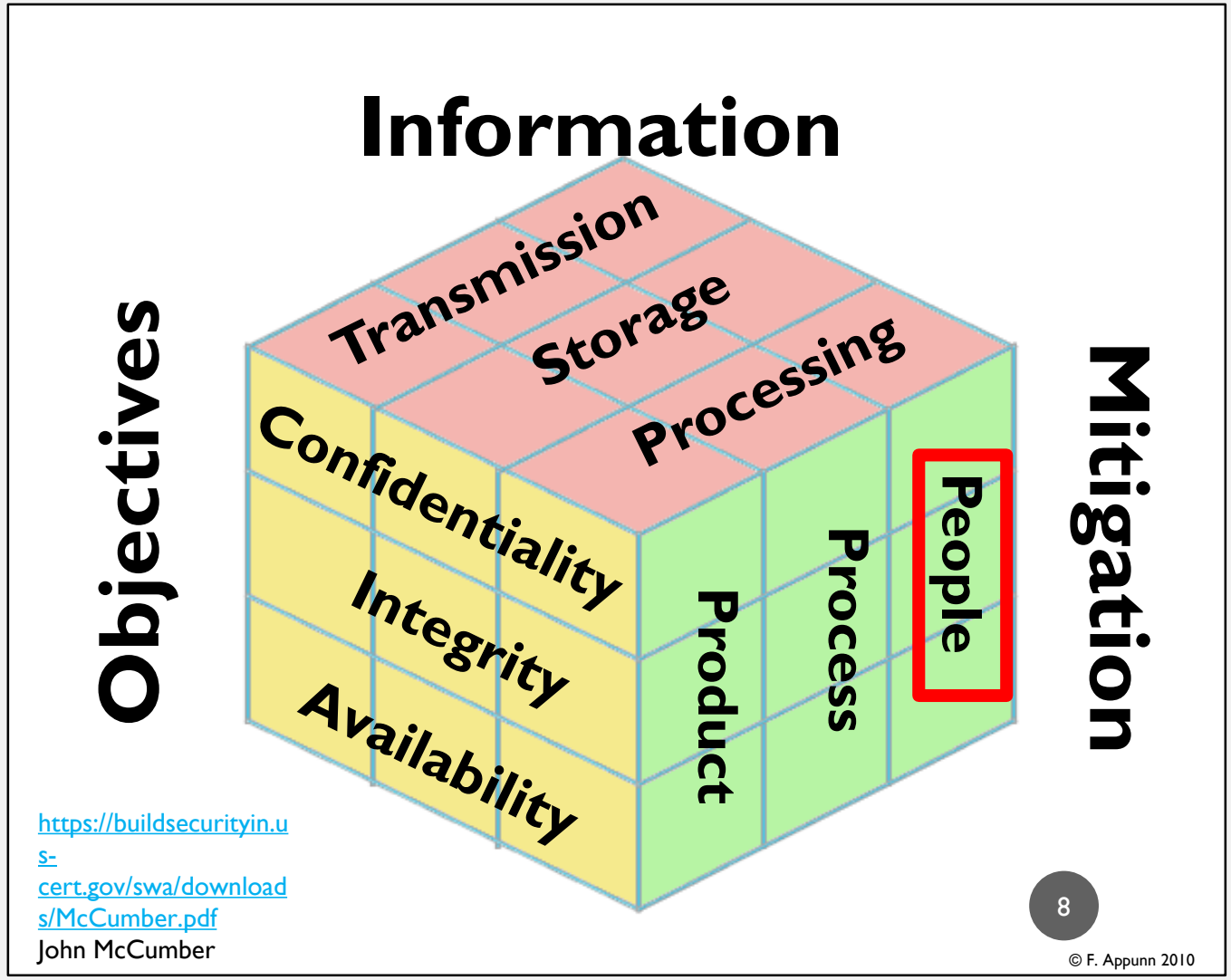


2. The Cyber Pieces Represented in this Session Plan and Operate



3. Threats – There is Too Much Guessing

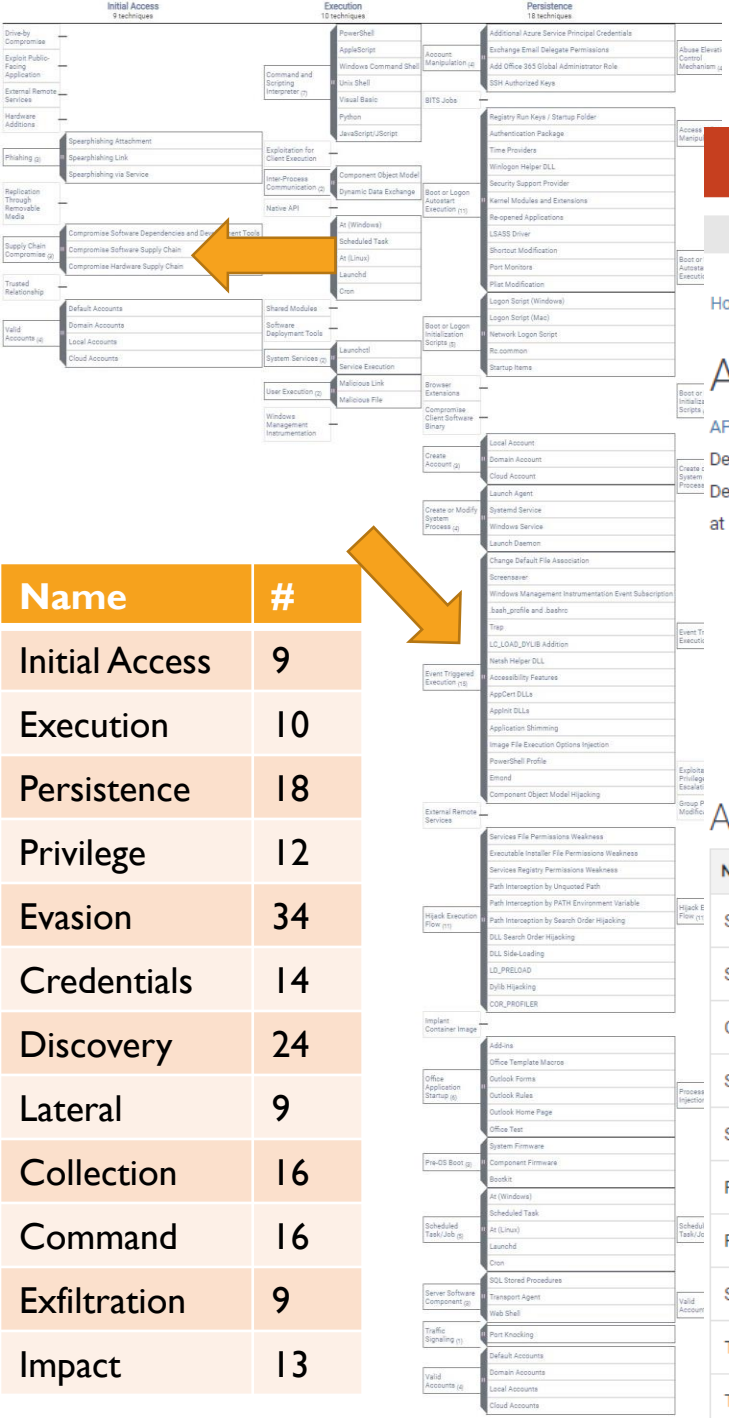
- What threats are there?
- The McCumber Cube
- Internal / External
- Known / Unknown
- Mistakes
- Foreign
- People



https://buildsecurityin.us-cert.gov/swa/downloads/McCumber.pdf
John McCumber

3. Threats – Where There is Too Much Guessing

- Our Tax Dollars
- Rand Corporation (rand.org) [Long term future]
- National Institute of Standards and Technology NIST (nist.org)
- MITRE (mitre.org)
  - ATT&CK: What attacks are out there? How do they work? What can I do?
  - Tactics, threats, procedures TTPs
  - An Ecosystem
  - SHIELD: How can I protect myself
- DHS and CISA



Name	#
Initial Access	9
Execution	10
Persistence	18
Privilege	12
Evasion	34
Credentials	14
Discovery	24
Lateral	9
Collection	16
Command	16
Exfiltration	9
Impact	13

Event Triggered Execution

Sub-techniques (15)

ID: T1546

Matrices Tactics Techniques Mitigations Groups Software Resources Blog Contribute Search

Register to stream the next session of ATT&CKcon Power Hour November 12

Home > Groups > APT28

APT28

APT28 is a threat group that has been attributed to Russia's Main Intelligence Directorate of the Russian Gener
Department of Justice indictment. This group reportedly compromised the Hillary Clinton campaign, the Demo
Democratic Congressional Campaign Committee in 2016 in an attempt to interfere with the U.S. presidential el
at least 2004.[1] [2] [3] [4] [5] [6] [7] [8] [9] [10] [11]

Swallowtail, Group 74,
STRONTIUM, Tsar Team,

y Ratliff, IBM; Richard

Associated Group Descriptions

Name	Description
SNAKEMACKEREL	[15]
Swallowtail	[10]
Group 74	[18]
Sednit	This designation has been used in reporting both to refer to the threat group
Sofacy	This designation has been used in reporting both to refer to the threat group
Pawn Storm	[5] [27]
Fancy Bear	[3] [37] [27] [2][18][10][24]
STRONTIUM	[37] [27] [30]
Tsar Team	[27][18][18]
Threat Group-4127	[5]

Group targets:
Banks: 8 specific groups
Healthcare: 8 specific groups

Group sources:
China 36
Russia 17

Examples:
Anthem – DeepPanda
Banks: North Korea (Lazarus)
$121 million story

THE PRIVACY FRAMEWORK

Function	
IDENTIFY (ID)	
PROTECT (PR)	Identity
	Inf
DETECT (DE)	
RESPOND (RS)	
RECOVER (RC)	

	NIST Privacy Framework Core	
	Function	Category
Identify - Privacy	**IDENTIFY-P (ID-P):** Develop the organizational understanding to manage privacy risk for individuals arising from data processing.	**Inventory and Mapping (ID.IM-P):** **Business Environment (ID.BE-P):** **Risk Assessment (ID.RA-P):** **Data Processing Ecosystem Risk Management (ID.DE-**
Govern - Privacy	**GOVERN-P (GV-P):** Develop and implement the organizational governance structure to enable an ongoing understanding of the organization's risk management priorities that are informed by privacy risk.	**Governance Policies, Processes, and Procedures** **Risk Management Strategy (GV.RM-P):** **Awareness and Training (GV.AT-P):** **Monitoring and Review (GV.MT-P):**
Control - Privacy	**CONTROL-P (CT-P):** Develop and implement appropriate activities to enable organizations or individuals to manage data with sufficient granularity to manage privacy risks.	**Data Processing Policies, Processes, and Procedures** **Data Processing Management (CT.DM-P):** **Disassociated Processing (CT.DP-P):**
Communicate - Privacy	**COMMUNICATE-P (CM-P):** Develop and implement appropriate activities to enable organizations and individuals to have a reliable understanding and engage in a dialogue about how data are processed and associated privacy risks.	**Communication Policies, Processes, and Procedures (CM.PO-P):** **Data Processing Awareness (CM.AW-P):**
Protect - Privacy	**PROTECT-P (PR-P):** Develop and implement appropriate data processing safeguards.	**Data Protection Policies, Processes, and Procedures** **Identity Management, Authentication, and Access** **Data Security (PR.DS-P):** **Maintenance (PR.MA-P):** **Protective Technology (PR.PT-P):**

Detect	**DE.AE** Anomalies and Events	
	DE.CM Security Continuous Monitoring	

4. HUMAN IMPACTS: OUR ADVERSARIES

Threat actors are increasingly focused on the people that use the systems -

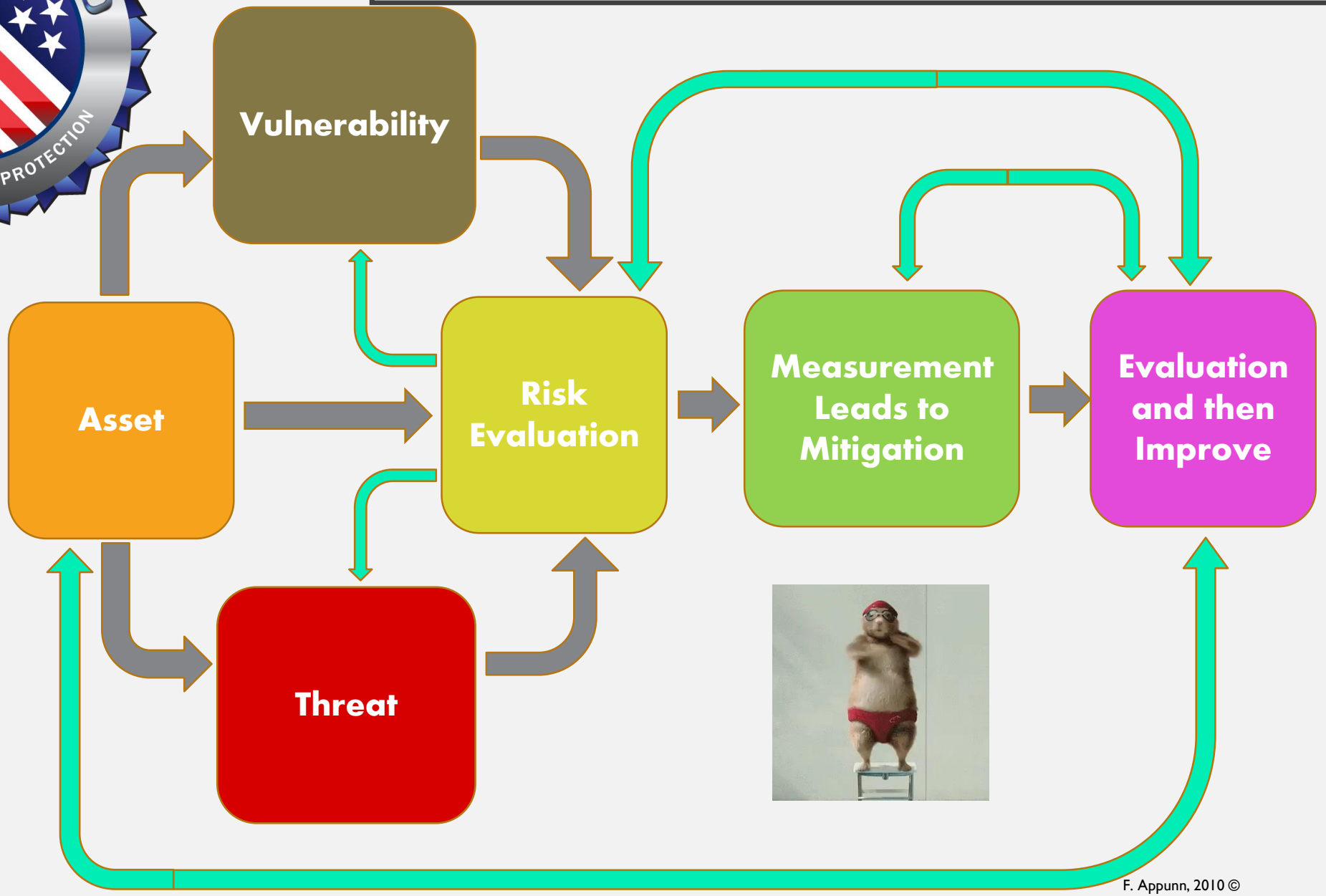
- Attackers are evolving their techniques and are doing more of this:
  - Studying **human behavior**
  - Watching the (global and local) **news**
  - Monitoring **social** trends
  - Using **spelling and grammar** checkers
  - Understanding **organizational dynamics and structures**
  - Understanding **supply chain** connections (and values)
  - **Assessing potential targets** and identifying current – and future weaknesses – not just for the 'big ones' anymore
  - **Multi-threat, multi-impact** attacks now (for greater payback)

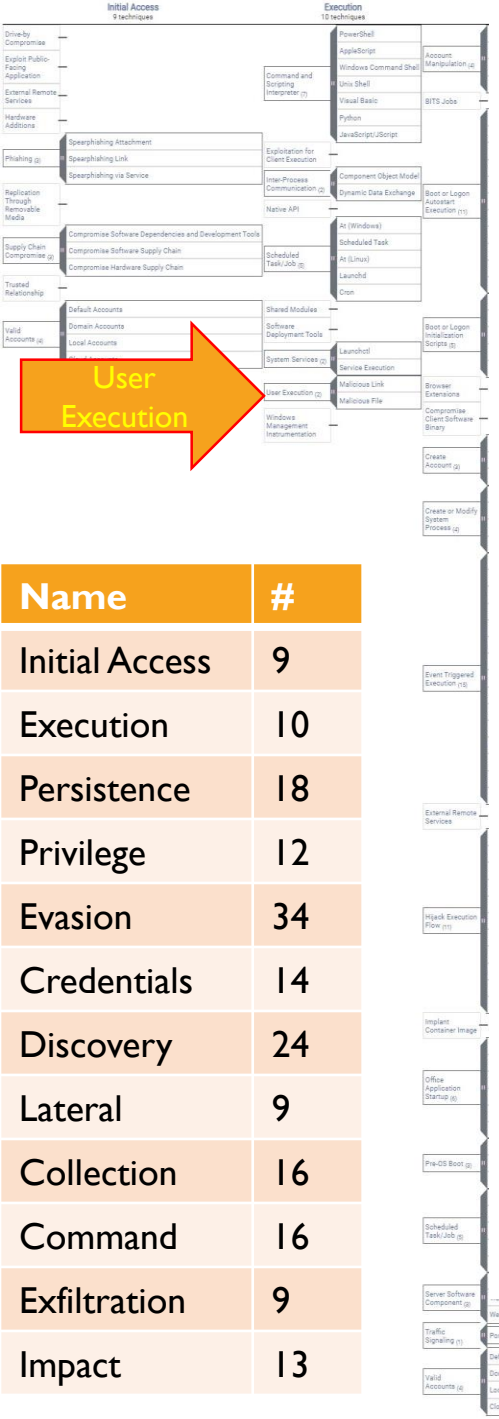
HUMAN IMPACTS: OUR CLIENTS

Business and Individual Users are Also Changing – Creating Exposures/Risks:

- **Connectivity 24X7**
- **Multiple devices** – increasingly mobile and technology fluid
- '**Walls**' between work and non work **blurred** – esp. now!
- Continued trend of reduced knowledge about how things work (or get compromised) – residing more at the graphical interface layer (**click culture**)
- Greater trust in **social norms** vs. policies or procedures
- (misguided) **Sense of optimism** – 'it won't happen to me', 'I am protected'….
- **Situational (un)awareness**
- **Fragmented** work streams / accepted culture of interruption

The Cyber Pieces Represented in this Session
Plan and Operate – FOR PEOPLE





Name	#
Initial Access	9
Execution	10
Persistence	18
Privilege	12
Evasion	34
Credentials	14
Discovery	24
Lateral	9
Collection	16
Command	16
Exfiltration	9
Impact	13

User Execution

User Execution: Malicious File

Other sub-techniques of User Execution (2)

An adversary may rely upon a user opening a malicious file in order to gain execution. Users may be subjected to social engineering to get them to open a file that will lead to code execution. This user action will typically be observed as follow-on behavior from Spearphishing Attachment. Adversaries may use several types of files that require a user to execute them, including .doc, .pdf, .xls, .rtf, .scr, .exe, .lnk, .pif, and .cpl.

Adversaries may employ various forms of Masquerading on the file to increase the likelihood that a user will open it.

While Malicious File frequently occurs shortly after Initial Access it may occur at other phases of an intrusion, such as when an adversary places a file in a shared directory or on a user's desktop hoping that a user will click on it. This activity may also be seen shortly after Internal Spearphishing.

ID: T1204.002

Sub-technique of: T1204

Tactic: Execution

Platforms: Linux, Windows, macOS

Permissions Required: User

Data Sources: Anti-virus, Process command-line parameters, Process monitoring

Version: 1.0

Created: 11 March 2020

Last Modified: 11 March 2020

Version Permalink

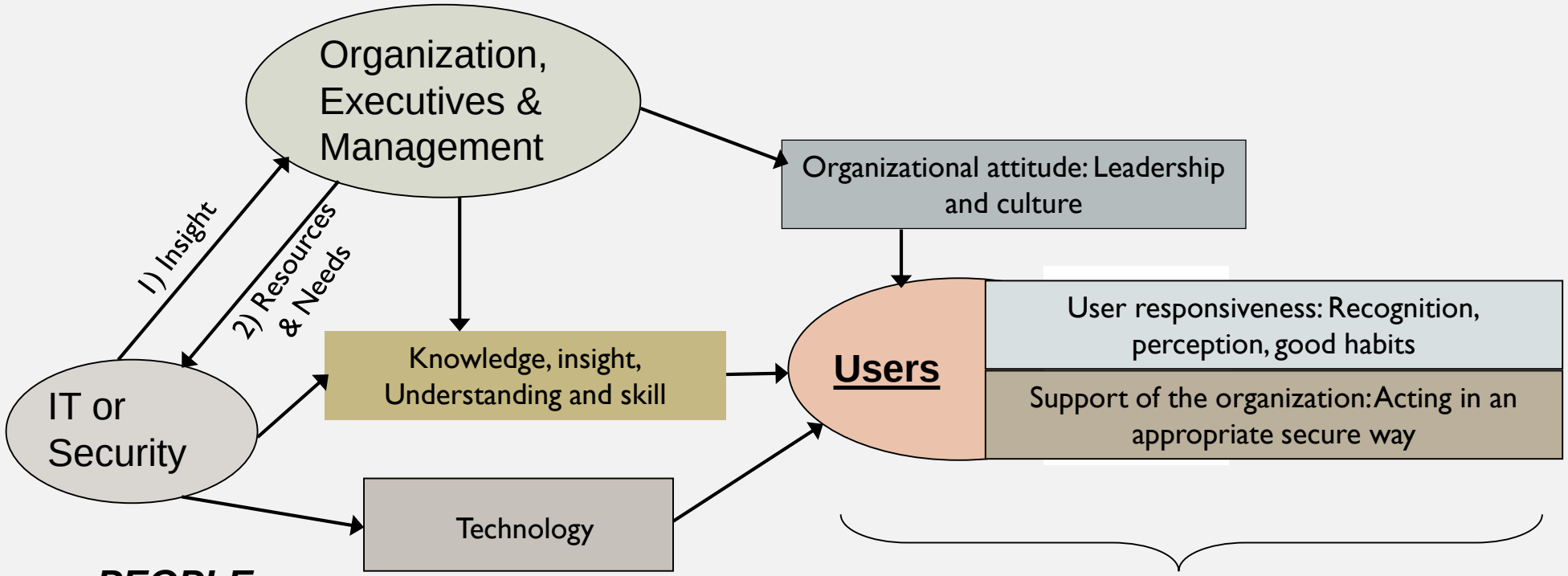
Procedure Examples

Name	Description
admin@338	admin@338 has attempted to get victims to launch malicious Microsoft Word attachments delivered via spearphishing emails.[90]
Agent Tesla	Agent Tesla has been executed through malicious e-mail attachments [15]
APT-C-36	APT-C-36 has prompted victims to accept macros in order to execute the subsequent payload.[94]
APT12	APT12 has attempted to get victims to open malicious Microsoft Word and PDF attachment sent via spearphishing.[88][89]
APT19	APT19 attempted to get users to launch malicious attachments delivered via spearphishing emails.[23]
APT28	APT28 attempted to get users to click on Microsoft Office attachments containing malicious macro scripts.[28][29]
APT29	APT29 has used various forms of spearphishing attempting to get a user to open links or attachments, including, but not limited to, malicious Microsoft Word documents, .pdf, and .lnk files. [32] [33]
APT32	APT32 has attempted to lure users to execute a malicious dropper delivered via a spearphishing attachment.[66][67][68][69]
APT33	APT33 has used malicious e-mail attachments to lure victims into executing malware.[111]
APT37	APT37 has sent spearphishing attachments attempting to get a user to open them.[26]
APT39	APT39 has sent spearphishing emails in an attempt to lure users to click on a malicious attachment. [72][73][74]
BlackTech	BlackTech has used e-mails with malicious documents to lure victims into installing malware.[13]

5. People: Remain Our Biggest Exposure

- How does it work?

Computer Security and Users: In Organizations



PEOPLE
Procedures
Products

Transfers a major influence to ALL security outcomes

5. People: Remain Our Biggest Exposure

- Need to **change habits** – Like COVID protection
- **Strong authentication**
  - MFA? Token? Multiplatform?
  - ~~Passwords~~ Passphrases: Words you know and no one can guess, best if you can imagine a picture or phrase and wrap words around it.
  - Different - everywhere
  - Passphrases: Long, Never shared, repeated, in a readable file, or written down
  - Password manager?
- **DON'T click there**!
  - No trust, then verify
  - Verify and be suspicious - Check that link and email CAREFULLY
- **Mail service** protections may catch most, but not all

5. People: Remain Our Biggest Exposure

- **Home networks**
  - Should you worry about your remote worker's home Wi-Fi network security?

    or assume it is compromised and build end point protections based on that assumption
- **Home workspaces**
  - What is visible? What else is connected? Network Bandwidth – is it sufficient? Critical employees – during a time of crisis, can they connect safely?
- **Client Endpoints** – uses, protections, situational awareness
- **Data** storage - one vs. many (but strong backup controls)
- **Educate**, test/measure, communicate, adjust and repeat…
- Use **Social** strategies for greater adoption and **infusion** in the culture

InfrGard Survey Data	
Analysis of Responses	
Did not request support	573
Desiring information	584
Trusted information	199
Best practices	356
Webinar and education	313
Home and remote	229
Awareness	103
Supply chain and PPE	119
Help exchange	146
Faith	12
InfraGard, keep it up	2080
Total	4714

STATISTICS FOR COVID 19

CYBER THREATS & COVID-19

- Ransomware
  - An industry with multiple organizations
  - Specialists that trade
  - "Marketing" and "Distribution" are active
  - Payload changes anticipate

- TO DO
  - A new Awareness campaign
  - Air gap back up (not connected)
  - An extra complete backup, updated
    - Keep more versions
- At Home
  - Be suspicious, do not drop your guard

- Healthcare Industry
  - The industry is stressed
  - It will get much worse
  - Stress leads to weakness
  - Are you adding inexperienced people?

- TO DO
  - New personnel get a cyber chart and video
  - Check security for emergency processes
  - Do not drop identity and access controls
  - Double check if you are suspicious
  - Clinical network integration check

6. Q&A

- Next InfraGard meeting:
  - December 8
  - Online
  - AGM 4 vacancies on the Board
  - Critical Industry Leaders needed

THE END … RESOURCES

- InfraGard https://www.infragard.org/
- DarkReading https://www.darkreading.com/
- Darknet Diaries https://darknetdiaries.com/
- NIST https://csrc.nist.gov/publications/sp https://www.nist.gov/privacy-framework https://www.nist.gov/cyberframework
- CISA https://www.cisa.gov/cybersecurity
- MITRE: https://attack.mitre.org/ https://shield.mitre.org/matrix/ https://attack.mitre.org/groups/
- SBA https://www.sba.gov/business-guide/manage-your-business/stay-safe-cybersecurity-threats
- FCC https://www.fcc.gov/general/cybersecurity-small-business

5. Requests of Assistance: Opportunity

Investigative Tables
Further data analytics

- 4714 ideas shared
- 573 had no specific request, of which 168 were "n/a"

- 584 wanted "Information" in general of in specific areas
  - Some is provided at present, others are specific to industries,
  - A few were disappointed that they had seen it all before
- 199 wanted trusted data (like InfraGard data)
  - Others were for fast data access, pre-release, or privileged access

5. Requests of Assistance: Opportunity
Investigative Tables
Further data analytics

- Knowledge, Skill, and Experience
- This represents a range of different requests that represents a potential capability for InfraGard
  - 356 request for assistance wanted "best practices" proven techniques, specific suggestions for small organizations, specific segments, etc. Most of these might be a collection of practices for suggestions. One might crowd source these for significant benefit to these members. Options might be NIST of CISecurity.org
  - 313 would benefits from "webinars or education" plus smaller topics of interest to groups in a common area. Other hope to get unrestricted use of content. Sharing within the enterprise might fit. Experience with solutions – like conferencing for organizations.
  - 103 wanted Awareness solutions, 199 wanted supply chain suggestions

5. Requests of Assistance: Opportunity
Investigative Tables
Further data analytics

- Help Exchange
  - 27 offered help. A desire to access people or organizations in need.
  - 119 requested specific help that would need interaction: Not sure of the question, workshop an issue, want advice, or unusual requests.

- Faith
  - 12 comments related to faith. A small but unique set of data.

- Keep it up!
  - 2080 expressed satisfaction or appreciation for InfraGard's efforts.
  - ~ 50% of all comments