CYBERSECURITY

THE FINAL CHAPTER

Presenter: Louis C. King, AIG for Financial and IT Audits, DOT OIG

TABLE OF CONTENTS

- **Top Cybersecurity Issues**
- **Federal Cybersecurity Status**
- **Supply Chain Threat**
- **Insider Threat**
- **Artificial Intelligence**
- **Cloud Computing**
- **Epilogue**

TOP CYBERSECURITY ISSUES

Group A

- Supply Chain Threat
- Insider Threat
- Artificial Intelligence
- Cloud Computing

Group B

- Lack of Cybersecurity Talent
- Ransomware
- Malware
- Phishing
- Passwords
- Cyber hygiene

Group C

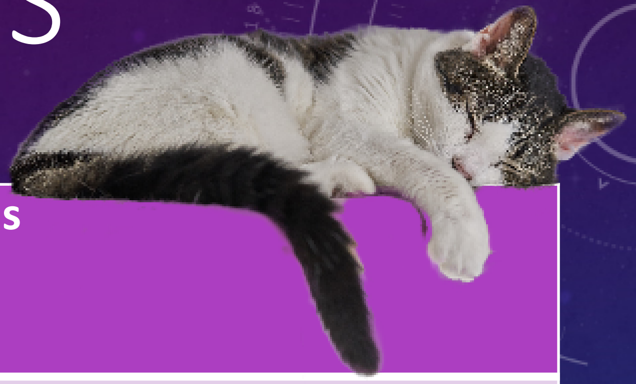
Cyber Hygiene

FEDERAL CYBERSECURITY STATUS

- IG Ratings of 23 CFO Act Civilian Agencies' Effectiveness (2018)
  - 19 Ineffective
  - 4 effective
    - Energy
    - Homeland Security
    - National Science Foundation
    - Nuclear Regulatory Commission

- IG Ratings of 24 CFO Act Agency By Maturity Level and Cybersecurity Domain (2018)

FEDERAL CYBERSECURITY STATUS



Cybersecurity Domain	Average of 76 Agency Assessments Performed in 2017	Domain Definitions
Identify	Level 3—Consistently Implemented	Understanding business context, critical functions, and related cybersecurity risks. Includes asset management (identifying hardware and software owned), risk management, and governance.
Protect	Level 3—Consistently Implemented	Configuration Management, Identity Management, Access Management, Data Protection and Privacy Management, Security Training Management
Detect	Level 2--Defined	Continuous Monitoring of Networks and Systems
Respond	Level 3—Consistently Implemented	Responding or addressing computer security incidents (theft of computers, viruses, etc.)
Recovery	Level 3—Consistently Implemented	Contingency planning and restoring systems after disruptions.

FEDERAL CYBERSECURITY STATUS

IG Ratings of CFO Act Agencies By Maturity Level & Cybersecurity Domain for 2018

	Ad Hoc	Defined	Implemented	Managed & Measureable	Optimized
Identify	2	8	**9**	4	1
Protect	1	8	**10**	5	0
Detect	2	**10**	8	4	0
Respond	0	9	5	**10**	0
Recover	2	8	**13**	1	0

SUPPLY CHAIN THREAT

- What if my computer or software comes with a “bug?” Problems can occur with, amongst other things:
  - Vendors
  - Transportation of products
  - Storage of products on route
  - Downloads
- Examples
  - A computer that is delivered to you with pre-installed malware
  - Counterfeit hardware that may not perform as expected

SUPPLY CHAIN THREAT

- Tight controls over component purchases (inspections, x-rays, prior to acceptance.)

Case Study: Kaspersky

- Russia stole documents detailing how the US attacks foreign computers and defends domestic ones.
- Russian hackers targeted NSA contractor’s home computer.
- Hackers used Kaspersky Anti-Virus software, which was used by contractor to protect his computer.
- Hackers used the anti-virus software as a “search engine” to find terms like “top secret.”
- Hackers located and retrieved documents without being detected.
- Foreign spies detected the hack.

INSIDER THREAT

- INSIDER: A current or former employee, contractor, or business partner who has or had authorized access to the organization's network, systems, or data.
- INSIDER THREAT: When an insider intentionally or unintentionally (knowingly or unknowingly) misuses access to negatively affect the confidentiality, integrity, or availability of the organization's critical information or systems.
- 25% of all incidents.
- ROOT CAUSE: People.
  - IT skills range from beginner to expert.
  - Motivations range from "didn't know better" to criminal.

INSIDER THREAT—WHAT CAN WE DO?

- Of course, there is TRAINING.
  - You can be an unwilling victim.
  - Crime and Punishment.
  - Report incidents.
- Technology—use it!
  - Patch and configure systems properly and monitor activity.
  - DEPLOY YOUR PIV CARDS CORRECTLY.
- Deter negative behaviors
  - Avoid fostering destructive work environments.
  - Employees or other insiders who feel mistreated, abused, or otherwise unfairly treated can become "disgruntled." You need to be prepared to diffuse these situations.
  - In the event an insider is disgruntled, access to the computer represents a concern.

INSIDER THREAT—CASE STUDY

- COMPANY X sends a team on a mining expedition.
- The COMPANY decides to use the expedition to for a second purpose—to collect a sample of a rare species.
- Only one team member is informed of the second objective.
- The captain is well trained in leadership, but not computers.
- The second in command is weak in soft skills, but has computer skills.
- The species is collected, but exposes the team to significant risks.
- Questions?
  - Is this a high risk scenario in terms of potential insider threat?
  - Who poses the greater risk of insider threat? The captain or the second in command?

Captain accesses main computer, an artificial intelligence, for assistance, but cannot obtain any useful information. He does not master the computer and has to manage as is.

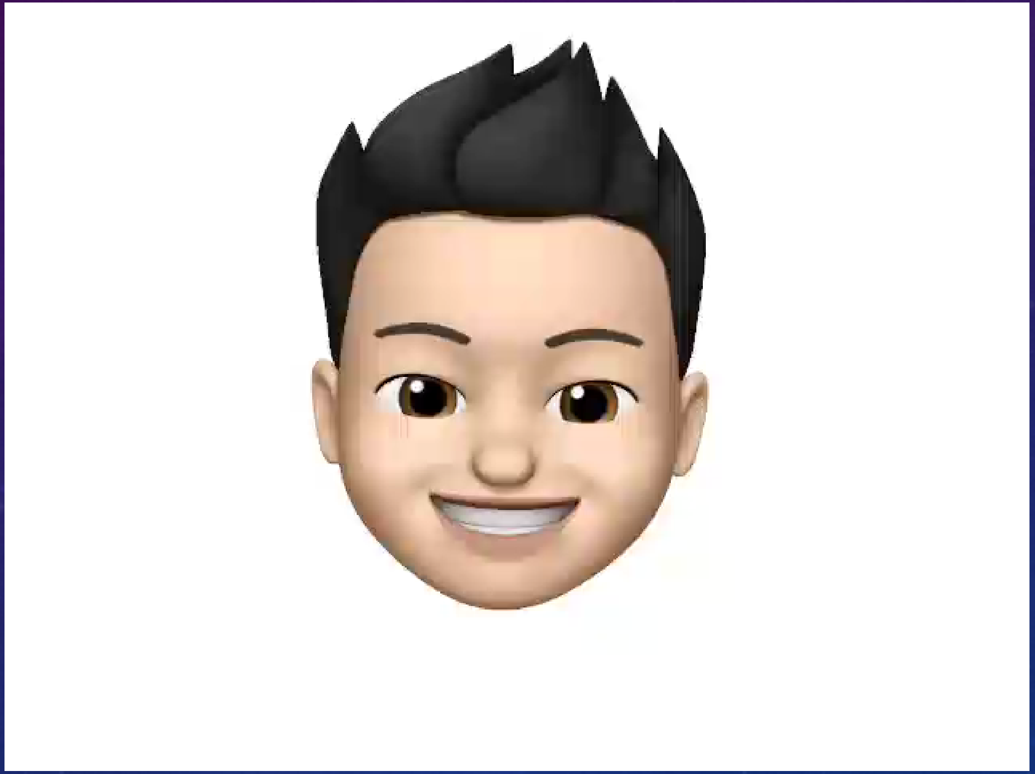
Captain passes away.

With the captain gone and the situation headed into a crisis, the new captain gains access to the main computer. She is already showing classic signs of insider threat potential--unhappiness, yelling at coworkers, etc. She gains access to the main computer. Using her expertise, she escalates her access until the computer reveals the true mission.

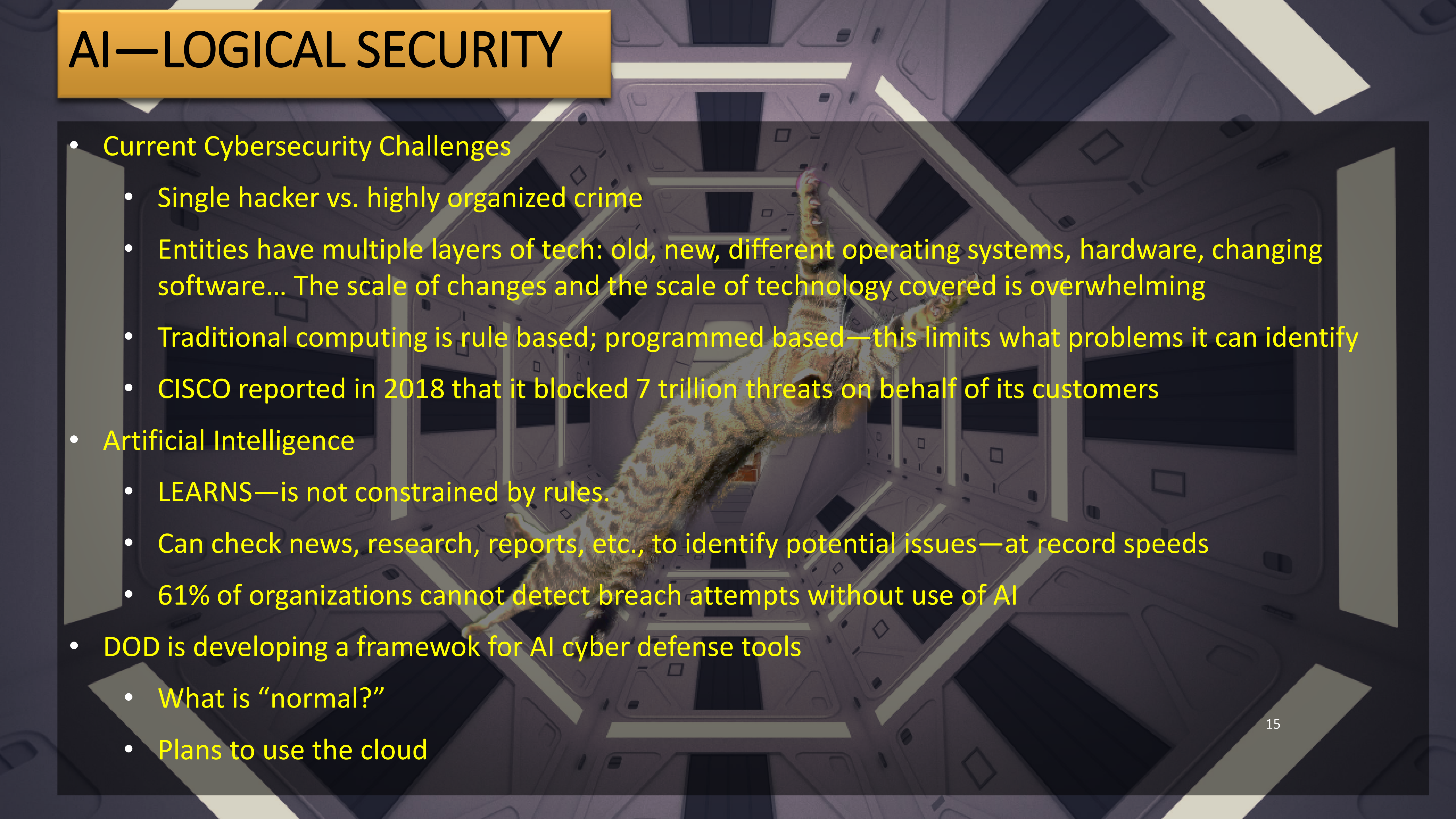
Discovering the company only wants the species, the new captain becomes disgruntled and destructive—ultimately setting off a self destruct mechanism which destroys the entire mining vessel, at a cost of billions to the company. Insider threat has, alas, claimed another victim (the COMPANY).

AI—HAS IT FULFILLED ITS PROMISE?

- As a security tool?
  - Physical
  - Logical

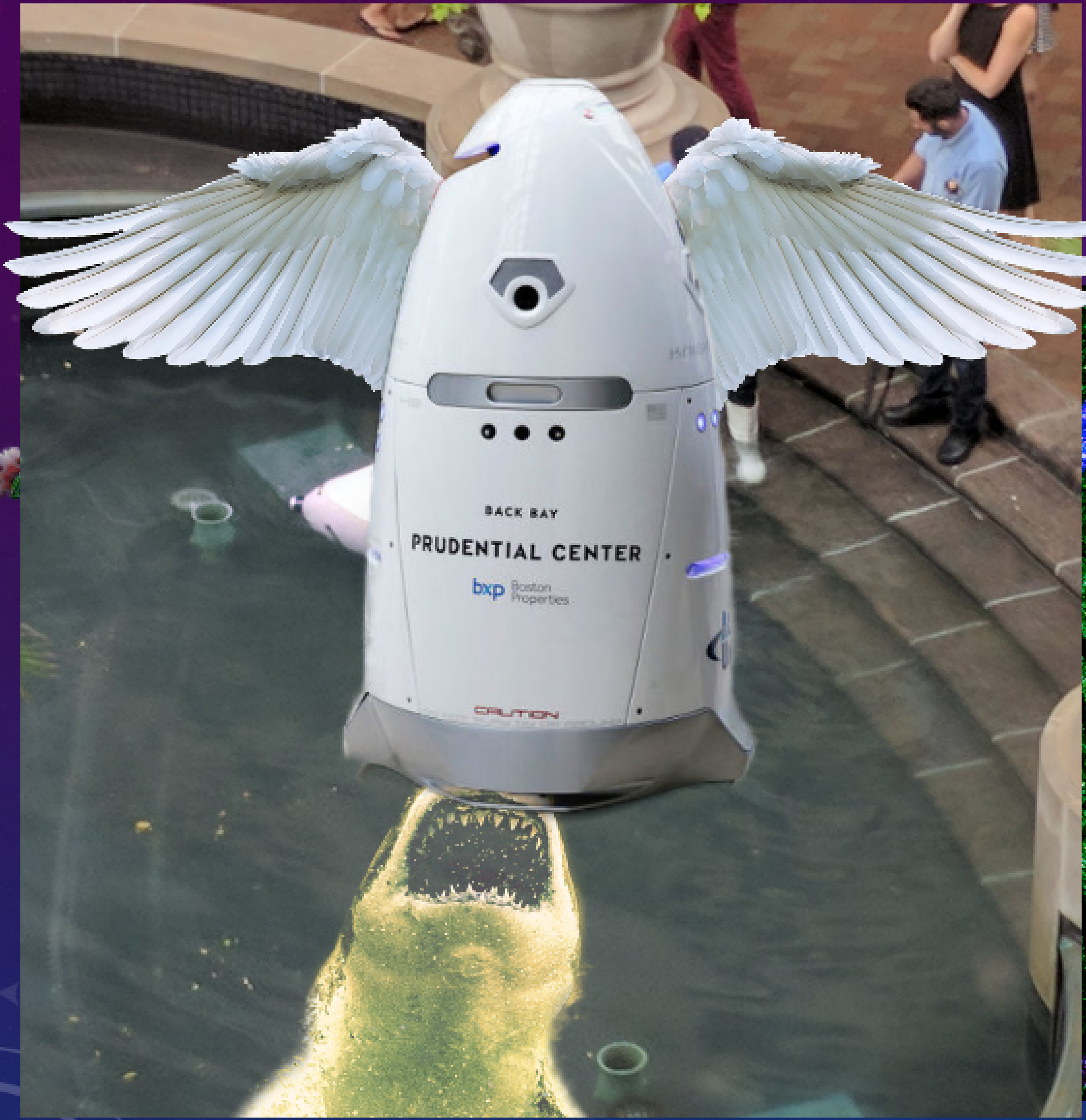


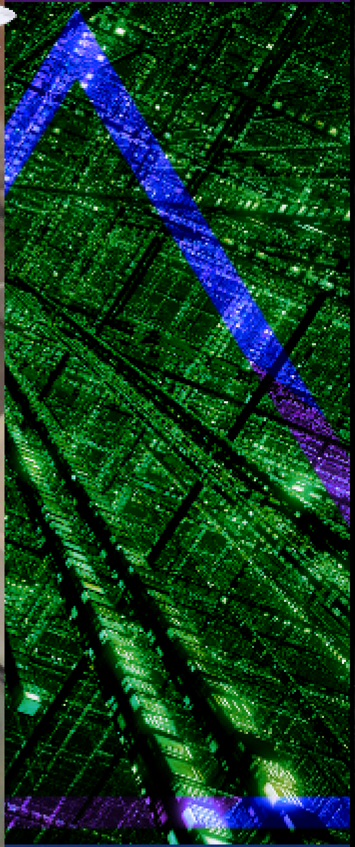
AI—LOGICAL SECURITY



- Current Cybersecurity Challenges
  - Single hacker vs. highly organized crime
  - Entities have multiple layers of tech: old, new, different operating systems, hardware, changing software… The scale of changes and the scale of technology covered is overwhelming
  - Traditional computing is rule based; programmed based—this limits what problems it can identify
  - CISCO reported in 2018 that it blocked 7 trillion threats on behalf of its customers
- Artificial Intelligence
  - LEARNS—is not constrained by rules.
  - Can check news, research, reports, etc., to identify potential issues—at record speeds
  - 61% of organizations cannot detect breach attempts without use of AI
- DOD is developing a framewok for AI cyber defense tools
  - What is “normal?”
  - Plans to use the cloud

E GLITCH



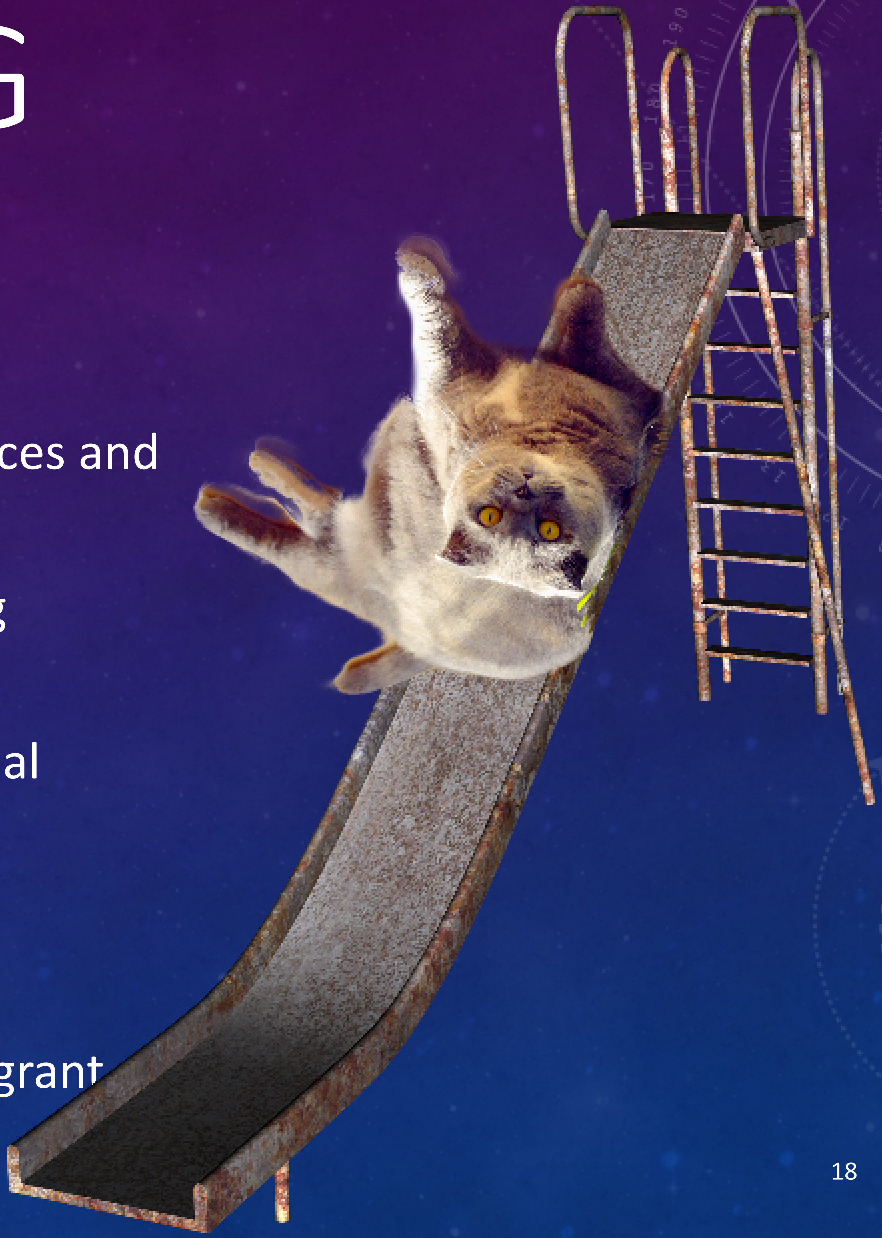


CLOUD COMPUTING

- Why is it call a cloud?
- FISMA Audit Questions:
  - To what extent does the organization maintain a comprehensive and accurate inventory of its information systems (including cloud systems)? (Identify/Risk Management/Q1)
  - To what extent does the organization ensure that specific contracting language (such as appropriate information security and privacy requirements and material disclosures, FAR clauses, and clauses on protection, detection, and reporting of information) and SLAs are included in appropriate contracts to mitigate and monitor the risks related to contractor systems and services? (Identify/Risk Management/Q11)
  - To what extent has the organization adopted the Trusted Internet Connection (TIC) program to assist in protecting its network? (Protect/Configuration Management/Q20)
  - To what extent has the organization defined and implemented its information system contingency planning program through policies, procedures, and strategies, as appropriate? (Recover/Contingency Planning/Q61)

CLOUD COMPUTING

- FEDRAMP (Federal Risk and Authorization Management Program)
  - Provides for initial authorization for cloud services and reuse of authorization packages
  - To start, Vendor submits security package using FEDRAMP requirements.
  - Either FEDRAMP or an agency grant a provisional authorization to operate (ATO) or agency ATO, respectively.
  - Vendor is placed on FEDRAMP Marketplace.
  - Other agencies can use existing ATO, but must grant ATOs for usage at their respective agencies.



The "Final Insult" from this auditor's perspective

- **Final**
- **Insult**
- **To**
- **Audits &**
- **Risk**
- **Analysis/Acceptance**

- Federal IT Acquisition Reform Act (FITARA)
- Biannual FITARA Scorecard includes a score for Cybersecurity, based on both CIO and OIG input.
- Case Study:
  - OIG found poor agency cybersecurity control implementation and over reliance on risk acceptance (i.e., continually accepting risks when controls failed).
  - OIG noted that components were postponing fixes until central CIO office addressed the matter.
  - CIO Assessment neutralized OIG Assessment.
  - As a result, the agency scored a "C" in cybersecurity.
  - Overall FITARA score of C+ remained unchanged.

EPILOGUE

Questions?

Thank You!

It’s been a pleasure!