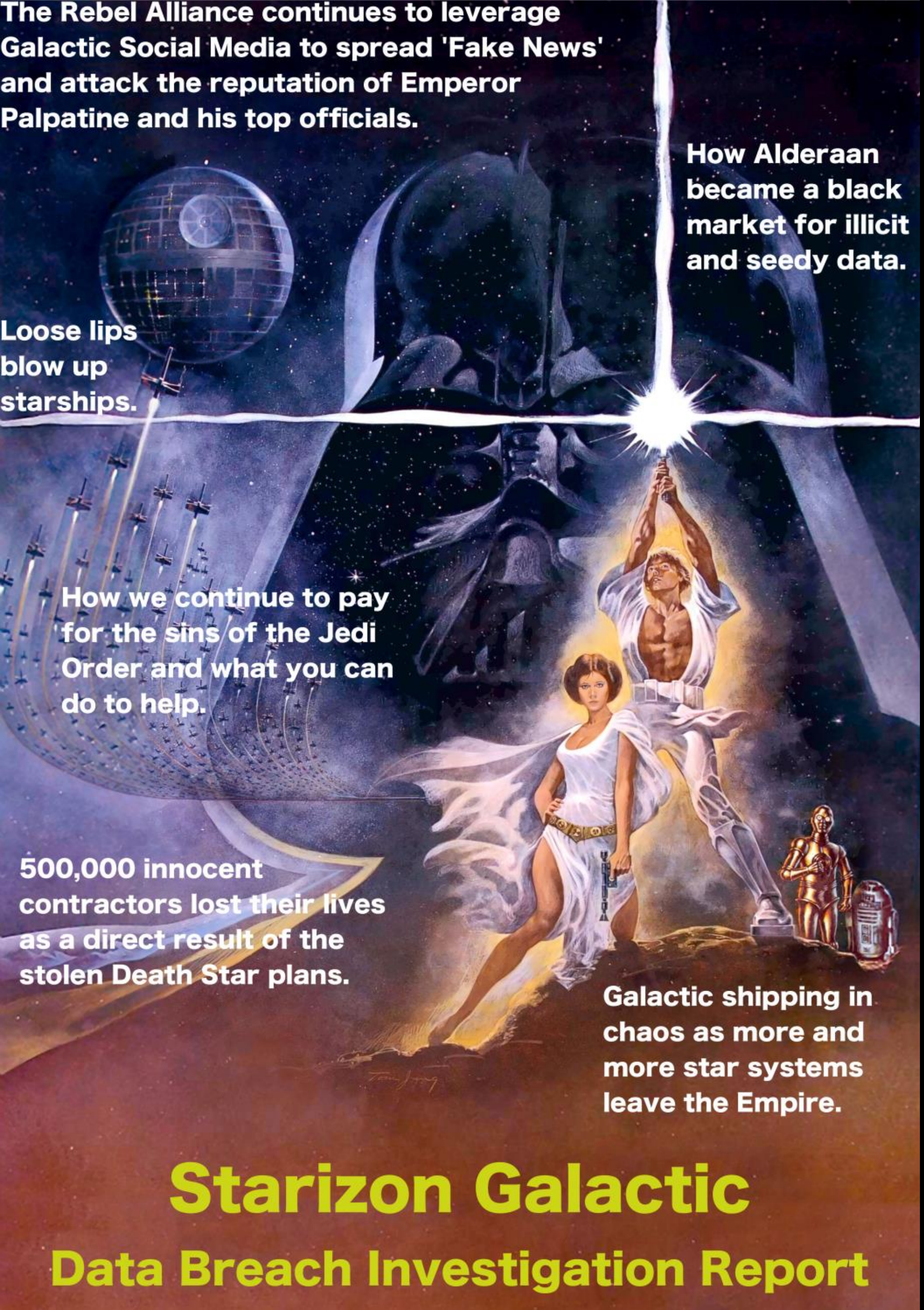


The Rebel Alliance continues to leverage Galactic Social Media to spread 'Fake News' and attack the reputation of Emperor Palpatine and his top officials.

How Alderaan became a black market for illicit and seedy data.

Loose lips blow up starships.

How we continue to pay for the sins of the Jedi Order and what you can do to help.

500,000 innocent contractors lost their lives as a direct result of the stolen Death Star plans.

Galactic shipping in chaos as more and more star systems leave the Empire.

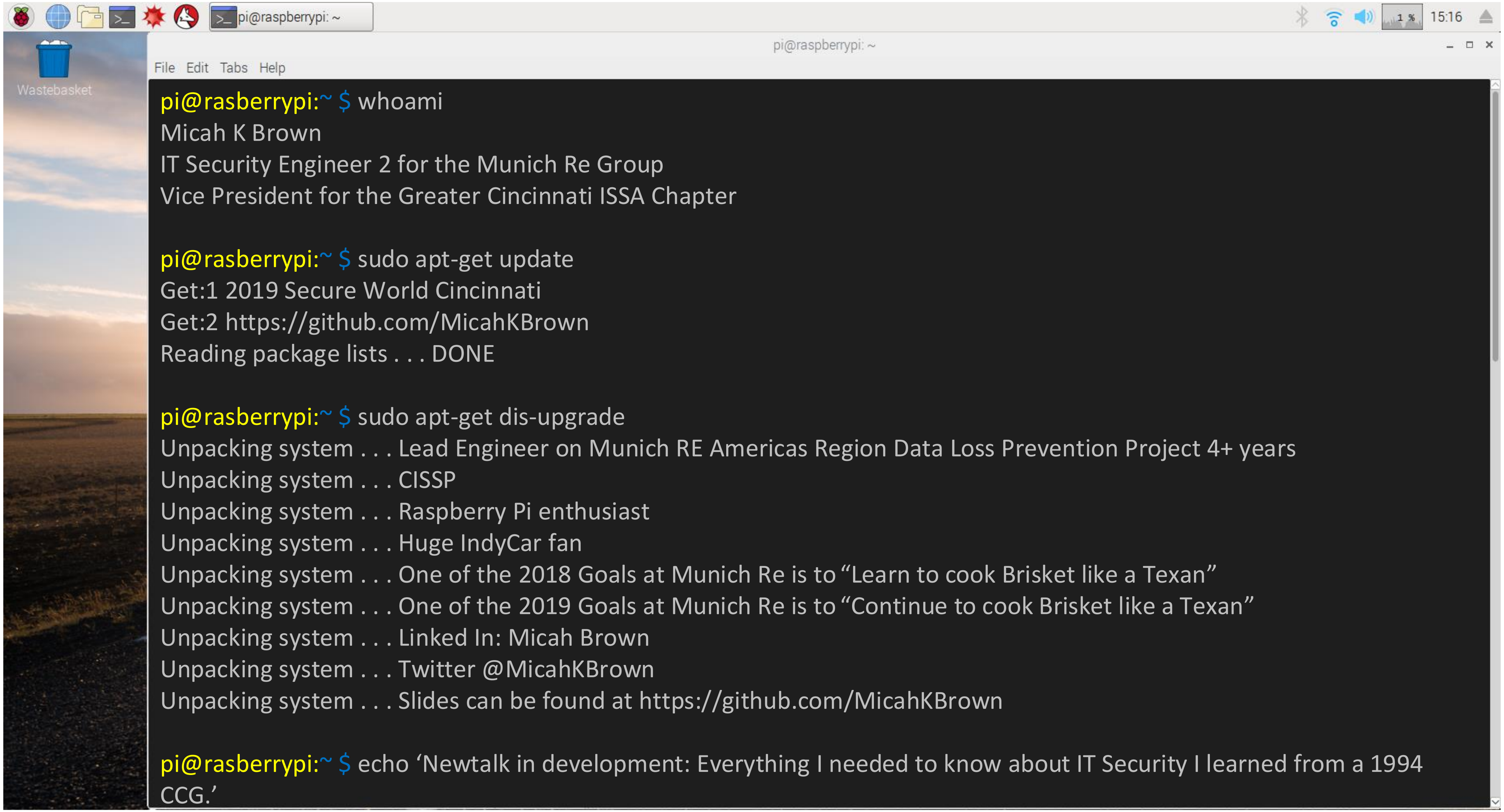
Starizon Galactic

Data Breach Investigation Report

STAR WARS

How an ineffective Data Governance Program destroyed the Galactic Empire

Presented by Micah K Brown, Greater Cincinnati ISSA v011



```
pi@rasberrypi:~ $ whoami
Micah K Brown
IT Security Engineer 2 for the Munich Re Group
Vice President for the Greater Cincinnati ISSA Chapter

pi@rasberrypi:~ $ sudo apt-get update
Get:1 2019 Secure World Cincinnati
Get:2 https://github.com/MicahKBrown
Reading package lists . . . DONE

pi@rasberrypi:~ $ sudo apt-get dis-upgrade
Unpacking system . . . Lead Engineer on Munich RE Americas Region Data Loss Prevention Project 4+ years
Unpacking system . . . CISSP
Unpacking system . . . Raspberry Pi enthusiast
Unpacking system . . . Huge IndyCar fan
Unpacking system . . . One of the 2018 Goals at Munich Re is to “Learn to cook Brisket like a Texan”
Unpacking system . . . One of the 2019 Goals at Munich Re is to “Continue to cook Brisket like a Texan”
Unpacking system . . . Linked In: Micah Brown
Unpacking system . . . Twitter @MicahKBrown
Unpacking system . . . Slides can be found at https://github.com/MicahKBrown

pi@rasberrypi:~ $ echo ‘Newtalk in development: Everything I needed to know about IT Security I learned from a 1994
CCG.’
```

Greater Cincinnati IT Security groups

ISSA

http://www.cincy-issa.org/

SMBA

https://sites.google.com/view/cincysmba

CiNPA

Cincinnati Networking Professionals Association

Security Special Interest Group

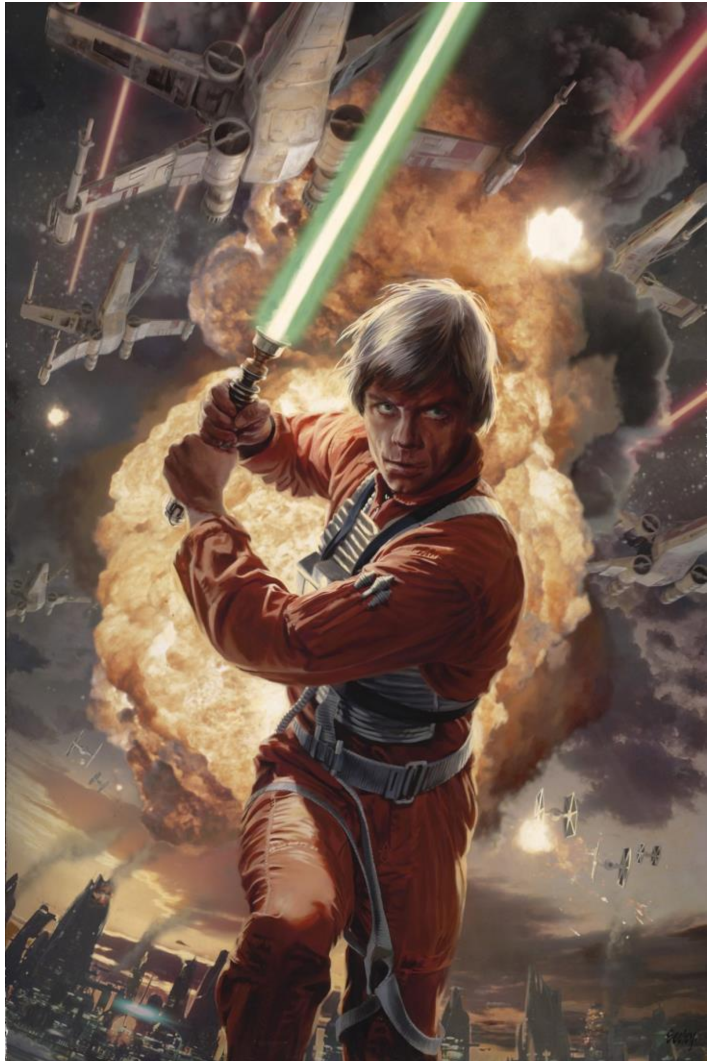
SECURITY SIG

https://www.meetup.com/TechLife-Cincinnati/events/

(ISC)^{2}®

https://www.infoseccincy.org/

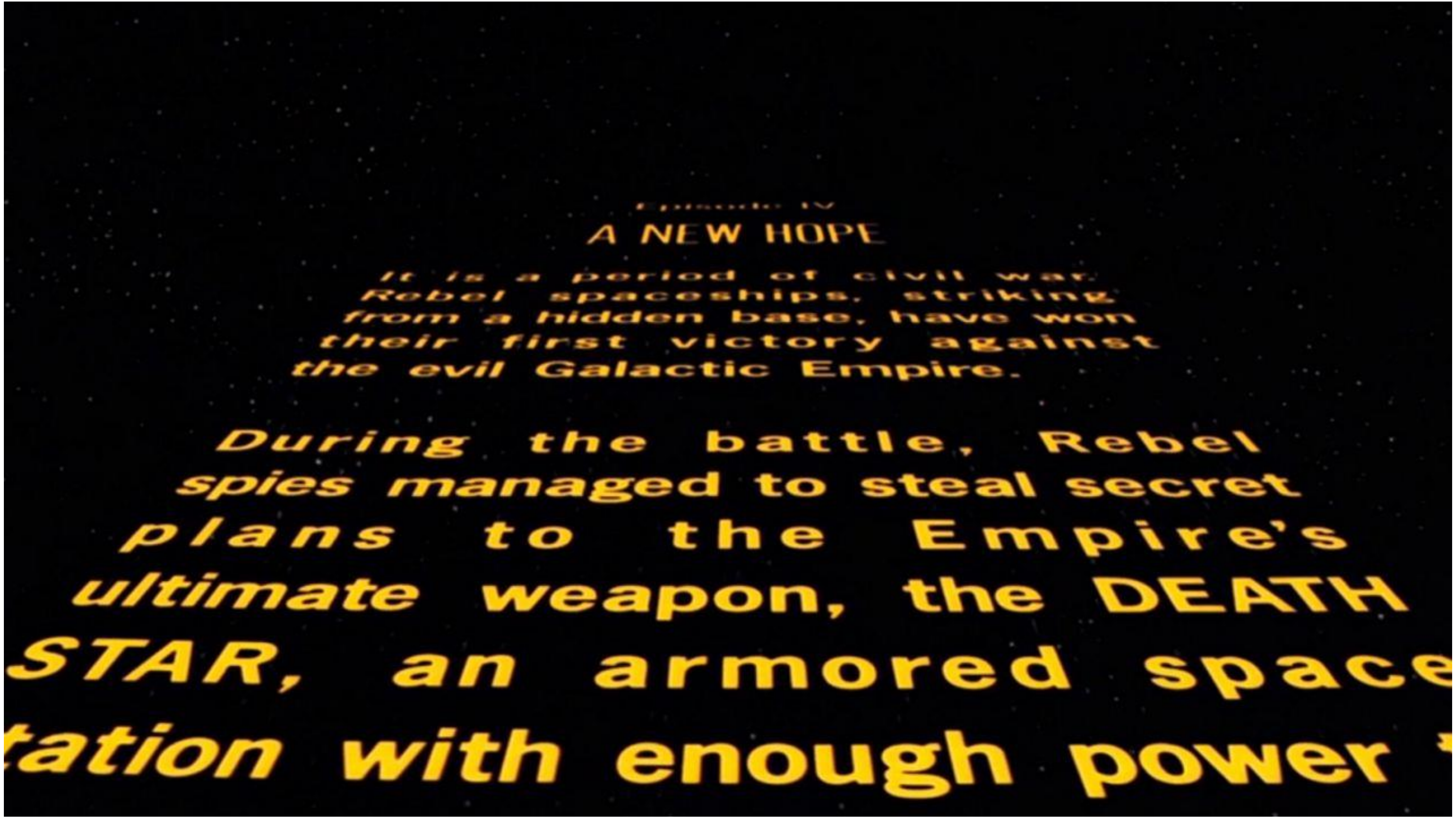
THIS IS NOT THE HERO YOU ARE LOOKING FOR:



- **While his actions might be heroic, without the access to the STOLEN Death Star Plan the Rebels would have never known of the superweapons weakness. I assert that the Rebel Alliance would have been destroyed in the Battle of Yavin IV.**
- **Chewbacca also deserved a medal**

Star Wars: Luke Skywalker and the Shadow of Mindor cover art by Dave Seeley
https://starwars.fandom.com/wiki/Luke_Skywalker_and_the_Shadows_of_Mindor

MY PROOF?



Episode IV

A NEW HOPE

It is a period of civil war. Rebel spaceships, striking from a hidden base, have won their first victory against the evil Galactic Empire.

During the battle, Rebel spies managed to steal secret plans to the Empire's ultimate weapon, the DEATH STAR, an armored space tation with enough power

MY PROOF?

It is a period of civil war.
Rebel spaceships, striking
from a hidden base, have won
their first victory against
the evil Galactic Empire.

During the battle, Rebel
spies managed to steal secret
plans to the Empire's
ultimate weapon, the DEATH
STAR, an armored space
station with enough power to
destroy an entire planet.

Pursued by the Empire's
sinister agents, Princess
Leia races home aboard her
starship, custodian of the
stolen plans that can save
her people and restore
freedom to the galaxy.....

Star Wars: A New Hope opening crawl 1997

ANCIENT ALIENS ASTRONAUT THEORISTS MIGHT BELIEVE

Giorgio A. Tsoukalos
The History Channel's
Ancient Aliens

TRUE HERO OF THE REBELLION:

- A common every day IT Security Practitioner / Data Analyst that struggles to find a work / life balance.
- Struggles to get the correct tools / resources / visibility to do their job and protect the Galactic Empire.
- Has daily challenges separating the signal from the ~~noise~~ jam.
- Is responsible to articulate deeply technical issues such as the Bleeps, the Sweeps, and the Creeps to others.
- Has challenges communicating gaps / concerns to Imperial Officers / SR management.
- This guy also deserves a medal.

Mel Book's Spaceballs 1987

WHAT IS DATA GOVERNANCE ANYWAY?

OVERVIEW

EVENT, ALERT, INCIDENT?

- **Event:** *any detectable or discernible occurrence that has significance for the management of the IT Infrastructure or the delivery of IT service and evaluation of the impact a deviation might cause to the services. Events are typically notifications created by an IT service, Configuration Item (CI) or monitoring tool.* (ITIL Service Operation Book)
- **Alert:** *a notification that a particular event (or series of events) has occurred, which is sent to responsible parties for the purpose of spawning action*
- **Incident:** *An event which is not part of the standard operation of a service and which causes or may cause disruption to or a reduction in the quality of services and Customer productivity."* In ITIL v3 it is defined as *"An unplanned interruption to an IT Service or a reduction in the Quality of an IT Service. Failure of a Configuration Item that has not yet impacted Service is also an Incident. For example, Failure of one disk from a mirror set (ITILv2)*

DATA GOVERNANCE HAS A LOT IF DIFFERENT DEFINITIONS? 1:2

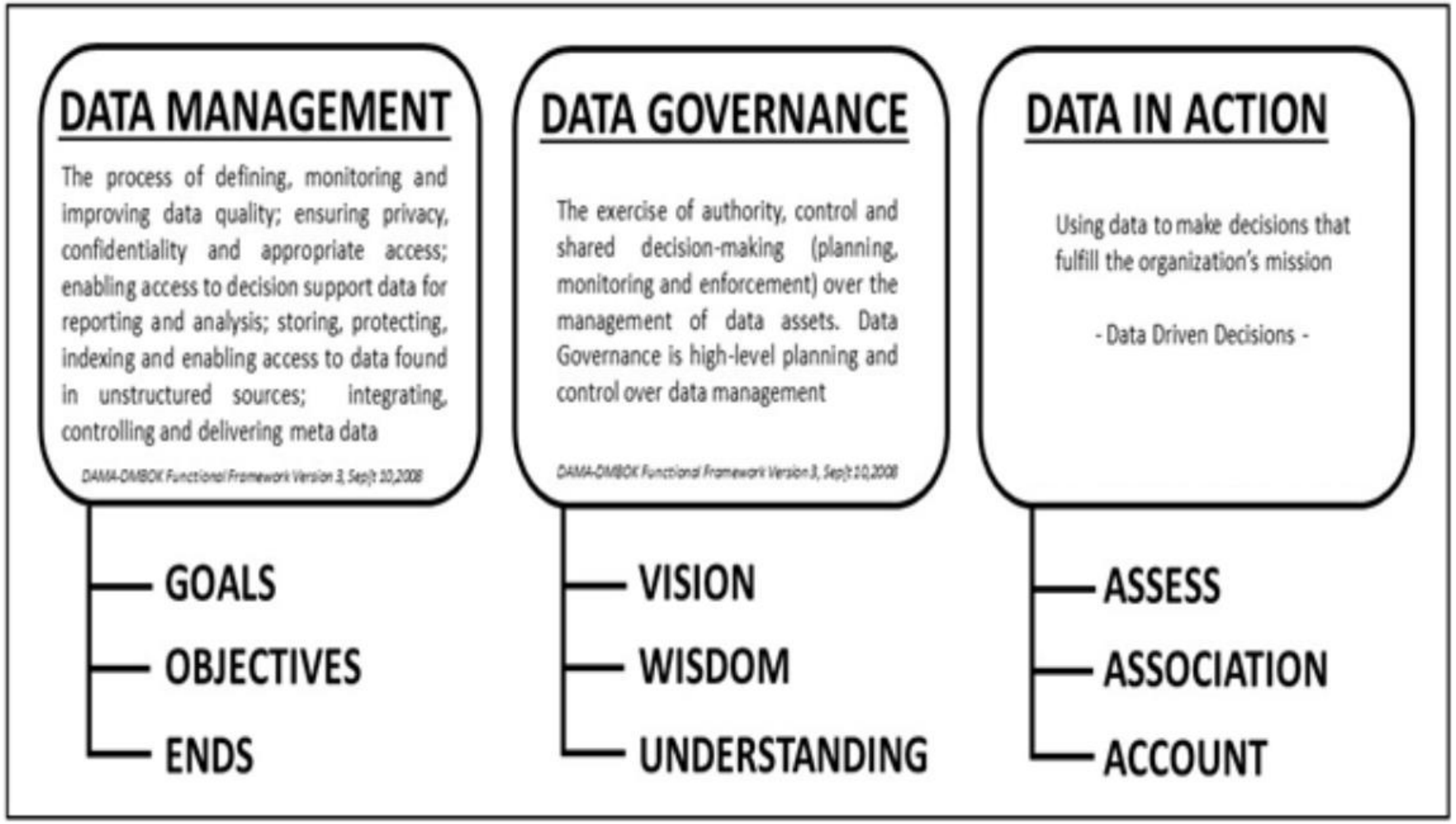
- **Data Governance:** Data governance encompasses the people, processes, and information technology required to create a consistent and proper handling of an organization's data across the business enterprise. It provides all data management practices with the necessary foundation, strategy, and structure needed to ensure that data is managed as an asset and transformed into meaningful information. https://en.wikipedia.org/wiki/Data_governance
- **Data Governance:** A discipline that provides clear-cut policies; procedures; standards; roles; responsibilities; and accountabilities to ensure that data is well-managed as an enterprise resource. https://dgpo.org/
- **Data governance:** is the orchestration of people, processes and technology to enable an organization to leverage data as an enterprise asset. It helps make data more usable, accessible, consistent and trustworthy. ftp://public.dhe.ibm.com/software/data/sw-library/ii/whitepaper/LIW14003USEN.pdf
- **Data governance:** effective [data] governance provides the framework in which stakeholders can collaborate and align intra-agency and government-wide objectives that move all agencies in a shared, common direction. www.nists.gov/TheDataCabinet The Federal Government Data Maturity Model

DATA GOVERNANCE HAS A LOT IF DIFFERENT DEFINITIONS? 2:2

- **Data Governance:**
  - Means different things to different people.
  - Allows the business to decide what data governance means for itself.
  - Involves people, process, and technology. (not necessarily in that order)
  - Allows the business to make strategic decision on how data is stored, processed, transmitted, and accessed in its environments.
  - Should optimize the Confidentiality, Integrity, and Availability of data to authorized users.

- **Data Governance:** is how we "decide how to decide".

NTIS DATA RESOURCE MANAGEMENT EXECUTIVE SUMMARY



DATA MANAGEMENT

The process of defining, monitoring and improving data quality; ensuring privacy, confidentiality and appropriate access; enabling access to decision support data for reporting and analysis; storing, protecting, indexing and enabling access to data found in unstructured sources; integrating, controlling and delivering meta data

DAMA-DMBOK Functional Framework Version 3, Sept 10,2008

- GOALS
- OBJECTIVES
- ENDS

DATA GOVERNANCE

The exercise of authority, control and shared decision-making (planning, monitoring and enforcement) over the management of data assets. Data Governance is high-level planning and control over data management

DAMA-DMBOK Functional Framework Version 3, Sept 10,2008

- VISION
- WISDOM
- UNDERSTANDING

DATA IN ACTION

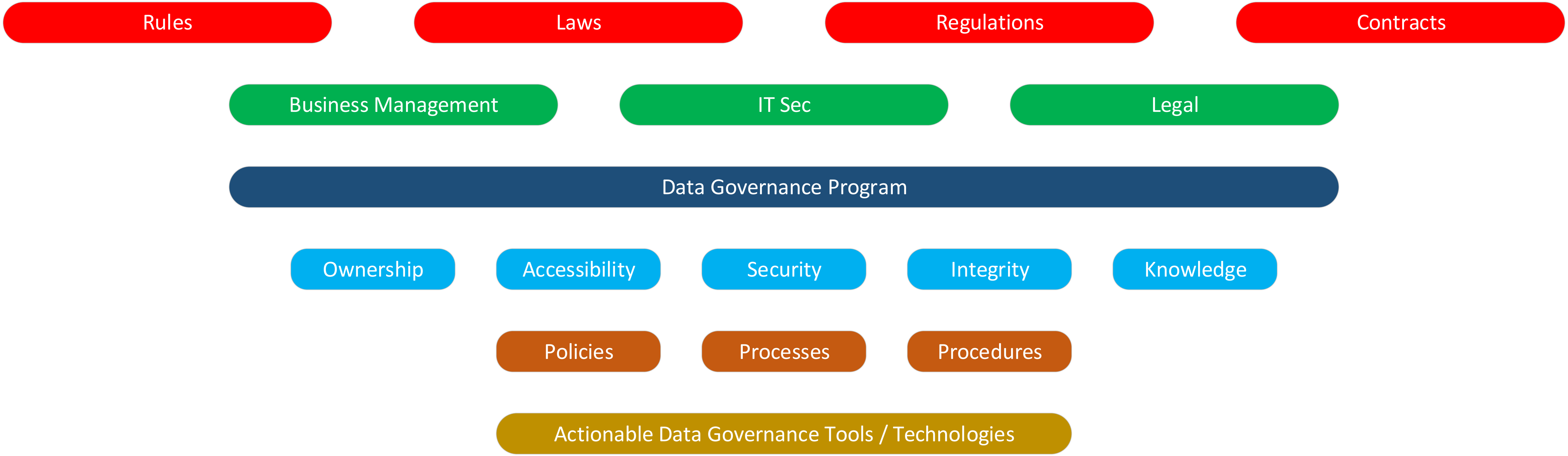
Using data to make decisions that fulfill the organization's mission

- Data Driven Decisions -

- ASSESS
- ASSOCIATION
- ACCOUNT

- https://www.ntis.gov/TheDataCabinet/assets/Executives%20Guide%20to%20DRM.docx

DATA GOVERNANCE VISUALIZED



Rules

Laws

Regulations

Contracts

Business Management

IT Sec

Legal

Data Governance Program

Ownership

Accessibility

Security

Integrity

Knowledge

Policies

Processes

Procedures

Actionable Data Governance Tools / Technologies

DATA GOVERNANCE GOALS

Goals of Data Governance:

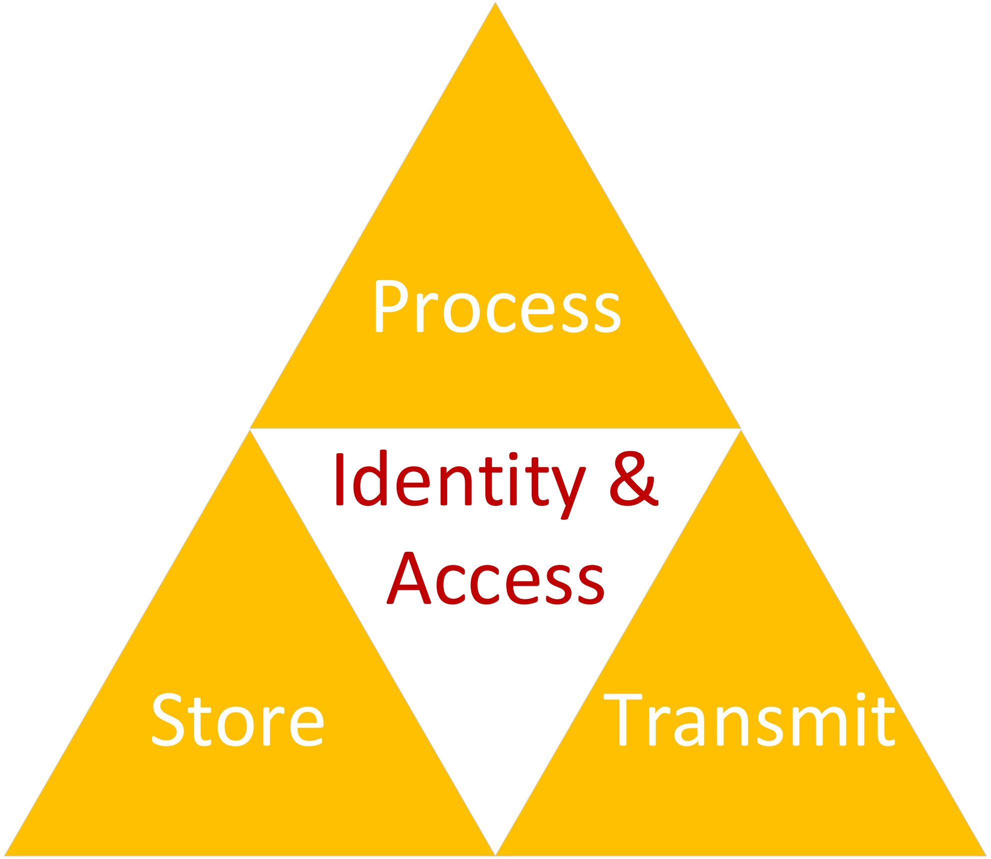
- **Enable better decision making.**
- **Reduce operational friction.**
- **Train managers and staff to adopt common approaches to data issues.**
- **Build standard and repeatable processes.**
- **Reduce costs and increase effectiveness through coordination of efforts.**
- **Ensure transparency of processes.**

DATA GOVERNANCE VS ACTIONABLE DATA GOVERNANCE TOOL

An 'Actionable Data Governance tool' is a technology or control that allows the business to enforce data policies in alignment with the output of the Data Governance Program.

These actions can be:

- **Permit**
- **Permit with special condition (digital signing, or encryption)**
- **Permit with justification**
- **Permit with alert**
- **Deny with alert**
- **Deny without an alert**



THE STATES OF DATA IN OUR ENVIRONMENT

Effective Data Governance is made up of many different policies, controls, and tools that work together.

DATA GOVERNANCE: THE PLAYERS

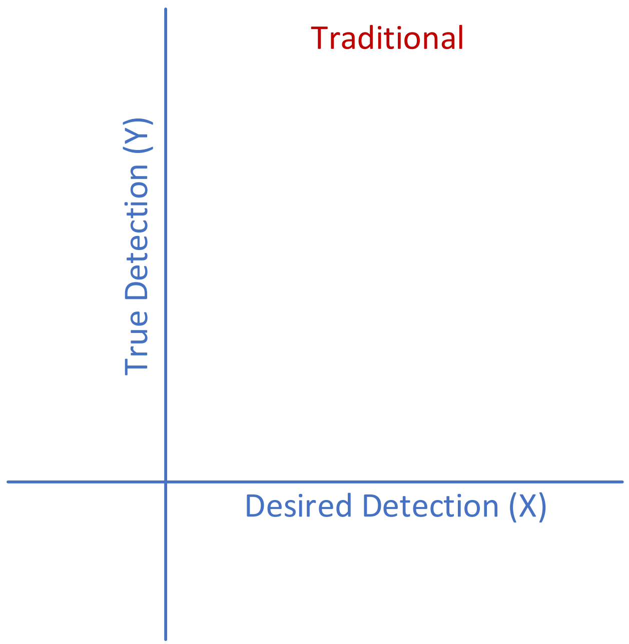
- Data Ower
- Data User
- Data Subject (internal and external)

Now more critical than ever with laws such as GDPR, NYDFS, and California Consumer Privacy Act.

- SR Management
- Risk Management
- Legal and Compliance
- Auditors (internal and external)
- IT Security
- IT (Service Delivery)
- 3rd Party / Partners

There are no FALSE POSITIVES, only poorly written rules*

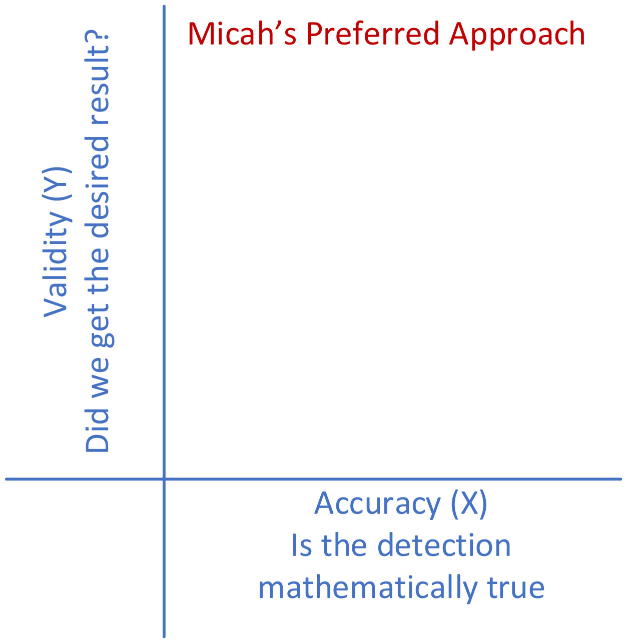
MEASURING DATA GOVERNANCE TOOLS



Traditional

True Detection (Y)

Desired Detection (X)



Micah’s Preferred Approach

Validity (Y)
Did we get the desired result?

Accuracy (X)
Is the detection
mathematically true

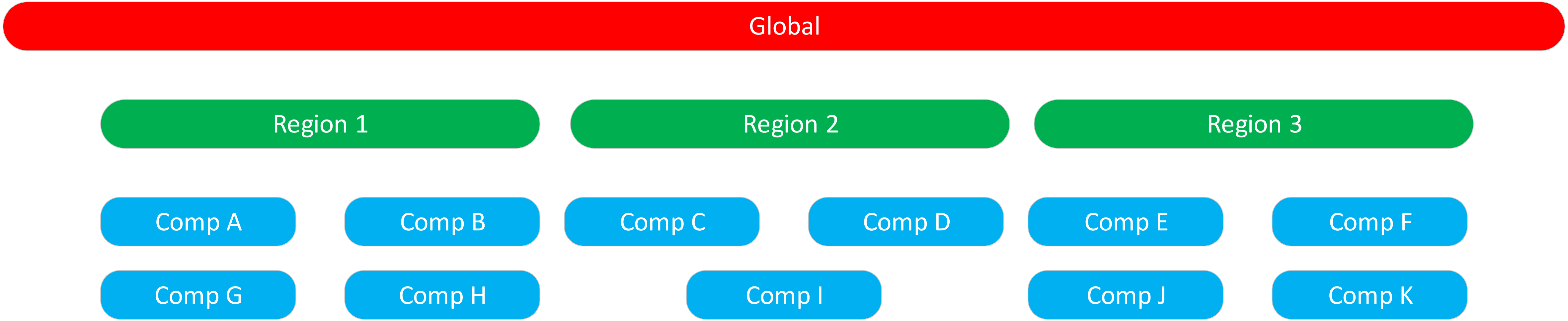
Measuring data is not an exact science

- **Traditional ([True | False], [Positive | Negative]) vs (Validity, Accuracy)**
- **Qualitative vs Quantitative**
- **@InfoSecBenjaminDisraeli: “lies, damned lies, and spreadsheets”**

ACTIONABLE DATA GOVERNANCE CONTROLS?

OVERVIEW

POLICY ARCHITECTURE



Global

Region 1

Region 2

Region 3

Comp A

Comp B

Comp C

Comp D

Comp E

Comp F

Comp G

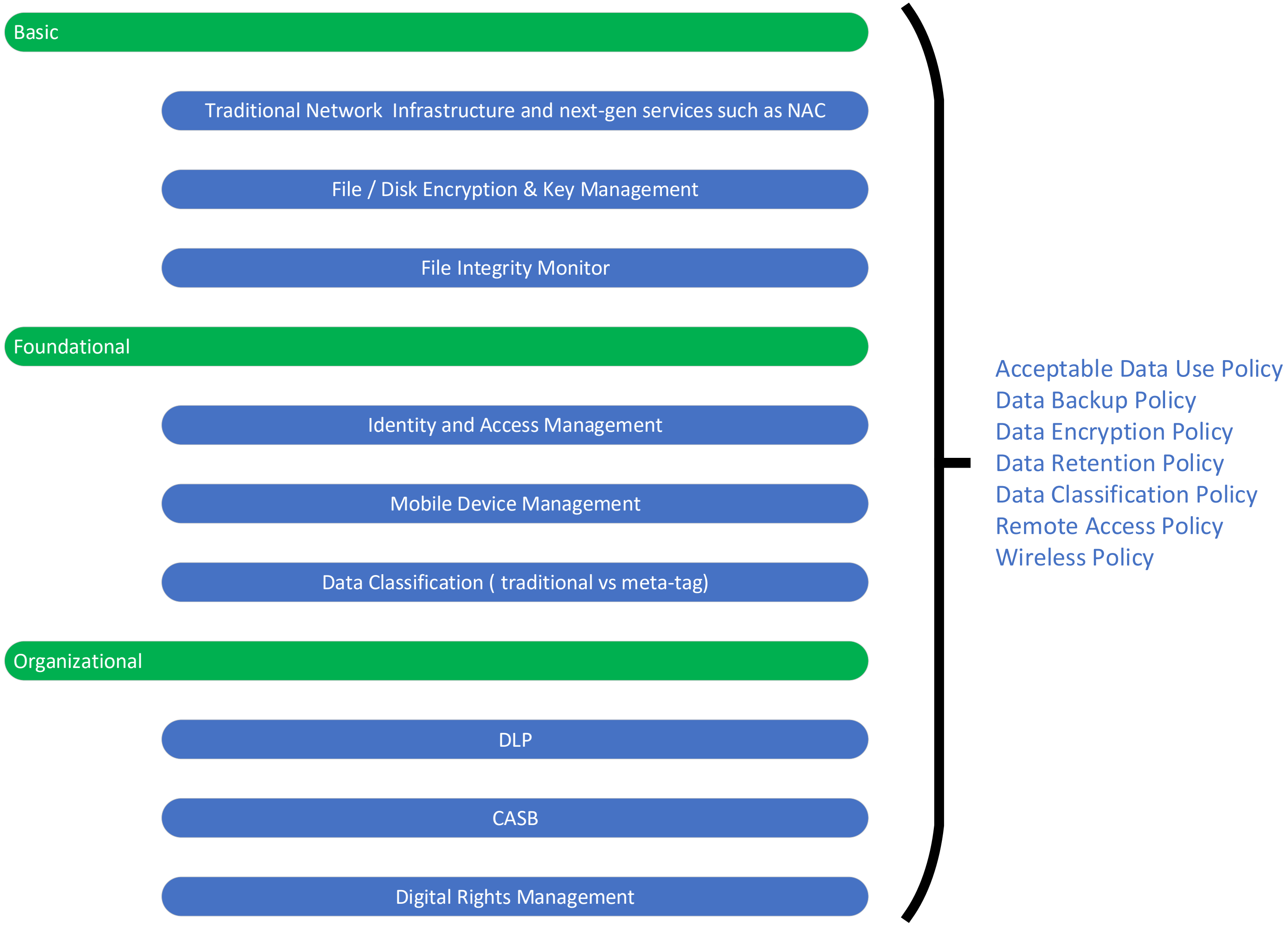
Comp H

Comp I

Comp J

Comp K

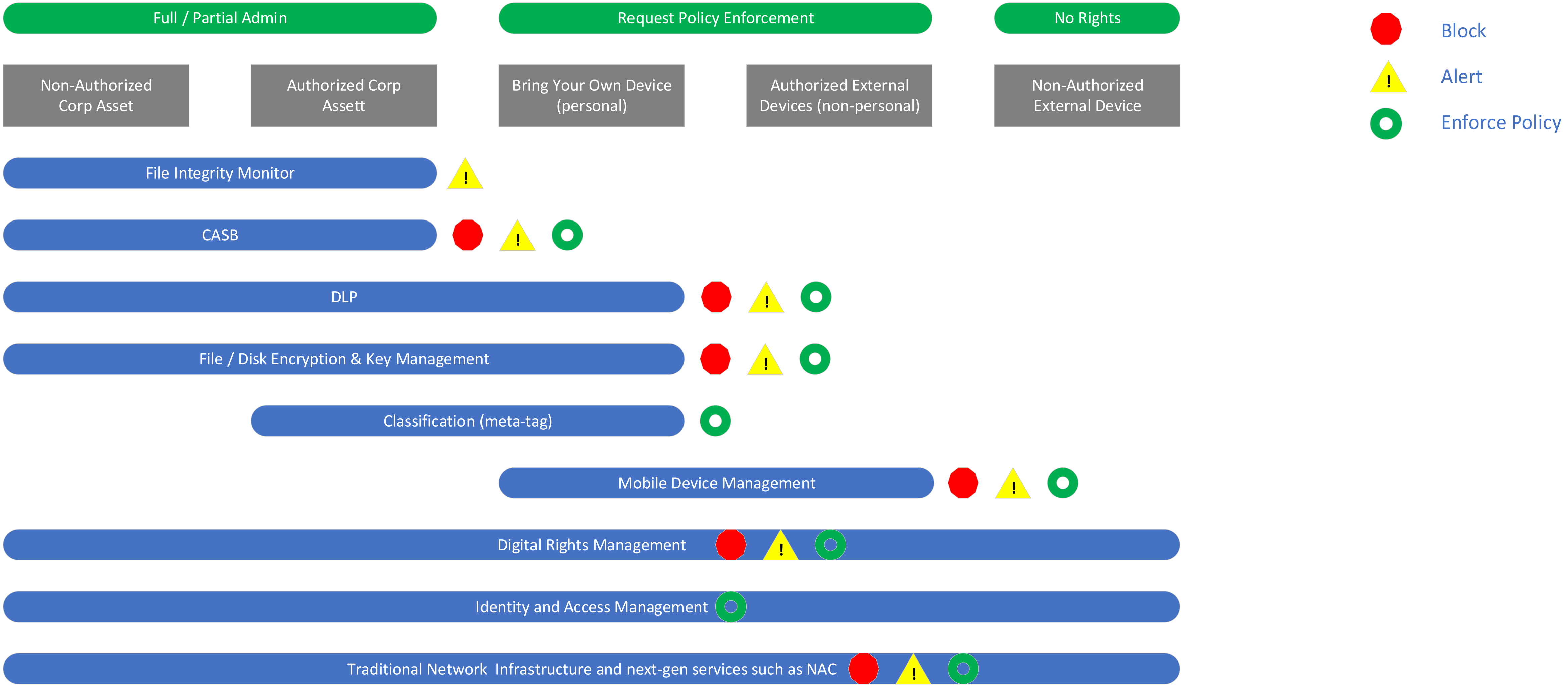
MEASURING DATA GOVERNANCE TOOLS



- Basic
  - Traditional Network Infrastructure and next-gen services such as NAC
  - File / Disk Encryption & Key Management
  - File Integrity Monitor
- Foundational
  - Identity and Access Management
  - Mobile Device Management
  - Data Classification (traditional vs meta-tag)
- Organizational
  - DLP
  - CASB
  - Digital Rights Management

Acceptable Data Use Policy
Data Backup Policy
Data Encryption Policy
Data Retention Policy
Data Classification Policy
Remote Access Policy
Wireless Policy

MEASURING DATA GOVERNANCE TOOLS



Full / Partial Admin

Request Policy Enforcement

No Rights

Non-Authorized Corp Asset

Authorized Corp Assett

Bring Your Own Device (personal)

Authorized External Devices (non-personal)

Non-Authorized External Device

File Integrity Monitor ⚠

CASB 🛑 ⚠ ○

DLP 🛑 ⚠ ○

File / Disk Encryption & Key Management 🛑 ⚠ ○

Classification (meta-tag) ○

Mobile Device Management 🛑 ⚠ ○

Digital Rights Management 🛑 ⚠ ○

Identity and Access Management ○

Traditional Network Infrastructure and next-gen services such as NAC 🛑 ⚠ ○

🛑 Block

⚠ Alert

○ Enforce Policy

ACTIONABLE DATA GOVERNANCE CONTROLS

THE BASIC CONTROLS

DG: BASIC CONTROLS
TRADITIONAL NETWORK INFRASTRUCTURE

- One of the hardest challenges that an enterprise faces is doing the "simple things" at scale.
- Find a way to automate and routinely test that your basic controls such as firewall rules, VLAN restriction, and protocols can not be used and abused!
- Even controls once put into place can erode and need some TLC (Tender Loving Care).
- Identify any gaps and work to close with responsible groups to close.
- Wash, rinse, and repeat!

DG: BASIC CONTROLS
FILE / DISK ENCRYPTION & KEY MANAGEMENT

- When it comes to any type of encryption, strong key management is paramount!

- Strongly encrypting the system drive of client systems is best practice.
  - Pay attention to any rules, laws, and regulations that might force protocol / strength restrictions.
  - Know that under some technologies, enforcing strong encryption (such as FIPS-140) might have functionality impacts.

- Encrypting of any files written to portable media might be a popular decision for the business, but prepare to face push back from users / clients.
  - Could effect current business process (exemption vs. edit the process).
  - Take precautions not to 'brick' non-company devices / data.

- Encryption of files at the network share level might seem attractive. Consider implications of key management.

DG: BASIC CONTROLS
FILE AND INTEGRITY MONITOR

- File and Integrity Monitors is software that will monitor and record user / machine interactions with data in targeted data repositories
  - Audit Read / Write / Modify on each.
  - Provide alerts / reports of specific user activities.
  - Automate data / folder ACLs for gaps.
  - Automate data provisioning requests.
  - Automate User Entitlement.
  - Often have overlap with Data Loss Prevention Discover Servers.
  - Alert / Identify files effected by crypto-ware (some new solutions have the ability to prevent spread of crypto-ware).
  - Detect Malicious users (both internal and externals pretending to be internals).

ACTIONABLE DATA GOVERNANCE CONTROLS

THE FOUNDATIONAL CONTROLS

DG: FOUNDATIONAL CONTROLS
MOBILE DEVICE MANAGEMENT

- Mobile Device Management (MDM) has continued to grow and mature to support Bring Your Own Device, external non-trusted external devices, and Business Assets that fall outside the normal baselines.
- MDM provides the ability to apply rich policy attributes to a system that you might have limited administrative and legal controls – be open and honest with those whom are enrolling into MDM with the tool, configuration, and intent.
- In the case of BYOD and non-trusted external deceives we must always respect that the user is the King or Queen of their device!
  - You are just providing them a service that they can opt out of at any time, for any reason.
  - This enrollment and de-enrollment are equally important.
- The MDM space now contains a rich mix of players in both open source and traditional business packages. Find the solution that meets your needs.
- Be sensitive to the additional overhead you are adding to the user.

DG: FOUNDATIONAL CONTROLS
IDENTITY AND ACCESS MANAGEMENT

- While one could assert that Identity and Access Management could be thought to be outside of a Data Governance program. (Mathematically I agree)
- I would counter that many of our Data Governance tools have a fundamental assumption that the user / machine account interacting with the data is the true user / system the initiated actions.
- Risks are not just limited to user IDs, we are also seeing dedicated strategies to compromise, use, and abuse: computer accounts, multi-factor authentication, cryptographic keys.
- Many have asserted that Active Directory is "insecure by default"
  - https://www.dbdr.com/windows-domain-accounts-insecure-by-default/
  - https://adsecurity.org/?p=1684
  - https://adsecurity.org/wp-content/uploads/2018/08/2018-DEFCON-ExploitingADAdministratorInsecurities-Metcalf.pdf
- Those organizations that wish to harden Active Directory have gone though a significant domain migration.

DG: FOUNDATIONAL CONTROLS
DATA CLASSIFICATION (TRADITIONAL VS META-TAG)

- **Traditional Data Classification is based on a series of data objects (text dictionaries, regular expressions, pattern matching) and Boolean logic. This can be problematic:**
  - Multiple different versions of Reg-EX
  - Often it is difficult to extract and convert Traditional Data Classifications from one tool to another.

- **Recently many popular office software suites provide a way in which you can empower your users to tag your data with your organization's data classifications leveraging meta-tag!**
  - This meta-tag data is saved in the document meta-data and is viewable by anyone or any software that has access to the document or document properties.
  - This data tag is vendor agnostic and can be leveraged by multiple Actionable Data Governance Tools.
  - Classification plus traditional classification rules (REG-EX and word dictionaries) is powerful!
  - Engender proper data ownership culture by including your workforce.

HOW DO WE DEFINE OUR DATA 'CLASSIFICATIONS'

- **Traditional Data 'Classifications' is built upon Regular Expressions (REG-EX) and word dictionaries. The logic used is very similar to the way we write IDS / IPS rules. This can be problematic:**
  - **50 US states each have multiple definitions of driver's license. This results in 26 different regular expressions!**
  - **Many websites use 15/16 digit numeric codes to reference content. This overlaps with traditional credit card definitions.**
  - **REG-EX and word dictionaries are not ~~sufficient~~ optimal.**
  - **We have to do better . . .**
- **When possible follow the main rule of improve "YES AND" in building traditional classification.**
- **Enabling users to embed data classification tags into the document meta-data is very powerful.**
- **"Proximity" rules are your friend!**

DLP: THE TYRANNY OF THE DRIVER'S LICENSE

Driver's License Positive match

```
[ .,-]00\d\d\d\d\d\d\d[ .,-]
[ .,-][xX]\d\d\d\d\d\d\d\d[ .,-]
[ .,-]\d\d\d\d\d\d\d[aA][ .,-]
[ .,-][rtRT]\d\d\d\d\d\d\d\d[ .,-]
[ .,-][a-zA-Z][a-zA-Z][a-zA-Z][a-zA-Z][a-zA-Z][a-zA-Z][a-zA-Z]\d\d\d\w\w[ .,-]
[ .,-][a-zA-Z]\d\d\d\d\d\d[ .,-]
[ .,-]\d\d\d\d\d\d\d\s
[ .,-]\d\d\d\d\d\d\d\0x2C
[ .,-][a-zA-Z]\d\d\d\d\d\d\d\d[ .,-]
[ .,-]\d\d\d\d\d\d\d\d\s
[ .,-]\d\d\d\d\d\d\d\d\0x2C
[ .,-]\d\d\d\d\d\d\d\d\d\s
[ .,-]\d\d\d\d\d\d\d\d\d\0x2C
[ .,-][a-zA-Z]\d\d\d\d\d\d\d[ .,-]
[ .,-][a-zA-Z]\d\d\d\d\d\d\d\d\d\d\d\d[ .,-]
[ .,-][a-zA-Z][a-zA-Z]\d\d\d\d\d\d[a-zA-Z][ .,-]
[ .,-][a-zA-Z]\d\d\d\d\d\d\d\d\d\d\d[ .,-]
[ .,-]\d\d\d\d\d\d\d\d\d\d\s
[ .,-]\d\d\d\d\d\d\d\d\d\d\0x2c
[ .,-]\d\d\d[a-zA-Z][a-zA-Z]\d\d\d\d[ .,-]
[ .,-]\d\d\d\d\d\d\d\d\d\d\d\d\s
[ .,-]\d\d\d\d\d\d\d\d\d\d\d\d\0x2c
[ .,-]\d\d[a-zA-Z][a-zA-Z][a-zA-Z]\d\d\d\d\d[ .,-]
[ .,-][a-zA-Z]\d\d\d\d\d\d\d\d\d\d\d\d\d\d[ .,-]
[ .,-][a-zA-Z][a-zA-Z]\d\d\d\d\d\d[ .,-]
[ .,-][a-zA-Z]\d\d\d\d\d\d\d\d\d\d\d\d\d[ .,-]
```

Exceptions:

REDACTED: exempted pastern that matched user ID

```
[ .,-][iI][mM]\d\d\d\d\d\d\d[ .,-]
[ .,-][pP][mM]\d\d\
d\d\d\d\d\d[ .,-]
[ .,-][sS][dD]\d\d\d\d\d\d\d\d[ .,-]
[ .,-][qQ][cC][ ]\d\d\d\d\d\d\d[ .,-]
[ .,-][qQ][cC]\d\d\d\d\d\d\d[ .,-]
[ .,-][cC][hH]\d\d\d\d\d\d\d[ .,-]
20[012]\d[01]\d[0123]\d
[0123]\d[01]\d20[012]\d
[ .,-][cC]\d\d\d\d\d\d\d[ .,-]
[ .,-][tT]\d\d\d\d\d\d\d[ .,-]
[ .,-][rR][fF]\d\d\d\d\d\d[ .,-]
```

ACTIONABLE DATA GOVERNANCE CONTROLS

THE ORGANIZATIONAL CONTROLS

DG: ORGANIZATIONAL CONTROLS
DATA LOSS PREVENTION: THE MAIN PLAYERS

- **DLP Client** – a software that sits on the client system / server. Can have overlap with other parts of the DLP environment if not careful. Can impact performance.
- **DLP Network** – Think of an IDP / IPS Sitting on your network only instead of looking for attack patterns on a network segment, it looks for potentially sensitive information. Can be put inline or out of line.
- **DLP Repository Scanner** – a physical or virtual appliance that sits on your networks and scans data repositories (shares, SharePoint sites, databases, and more) for potentially sensitive information.
- **DLP Email** – a physical or virtual appliance that partners with your email subsystem to scan outgoing and / or incoming email for sensitive information. Similar AV for email.
- **DLP Web -** a physical or virtual appliance that partners with your internet proxy to scan outgoing and / or incoming web requests for sensitive information. Similar AV for web proxy.
- **DLP Management console** – the physical or virtual appliance that manages all of the individual DLP parts. This also includes reporting, incident management, and evidence management.

DG: ORGANIZATIONAL CONTROLS
DLP: CONCERNS

- **Most DLP Client implementations have a lot of functionality overlaps with the rest of the environment (DLP network, DLP Repository Scanner, DLP Email, DLP Web). Why not do it all on the client?**
  - DLP client can have high performance hit (CPU / Memory / Disk I/O) on the user given a sufficiently advance policy.
  - You can run into incompatibles with local software such as Chrome and Firefox that can break client web inspection.
  - Incompatibilities with other applications can spike CPU / Memory/ Disk I/O.
  - Client must be connected to network to get updates.
  - The client might not be on every user system / server.
- **DLP Network can overlap with DLP Email and DLP Web.**
  - This traditionally happens with unencrypted conversations.
- **DLP Management console can be a high value target due to access to evidence and may be governed by rules / laws / regulations / contractual agreements.**
- **Many different products are adding on "DLP" functionality. Interoperability might be a challenge between diverse systems.**

DG: ORGANIZATIONAL CONTROLS
CLOUD ACCESS SECURITY BROKER (CASB)

- Cloud access security brokers (CASBs) are on-premises, or cloud-based security policy enforcement points, placed between cloud service consumers and cloud service providers to combine and interject enterprise security policies as the cloud-based resources are accessed. CASBs consolidate multiple types of security policy enforcement. Example security policies include authentication, single sign-on, authorization, credential mapping, device profiling, encryption, tokenization, logging, alerting, malware detection/prevention and so on. https://www.gartner.com/it-glossary/cloud-access-security-brokers-casbs/
- If on-site:
  - These devices generally need to be connected in-line. In case of a hardware failure, I suggest known and tested procedures to re-establish business.
  - Acknowledge the high cost of intercepting, breaking, and inspecting encrypted traffic could introduce additional burdens both legal and increased attack surface.
- If cloud based we need to make sure that we can still meet all of your use-cases.
- This like DLP is going to need to leverage your data classifications and meta-data tags to identify your organizations crown jewel data.

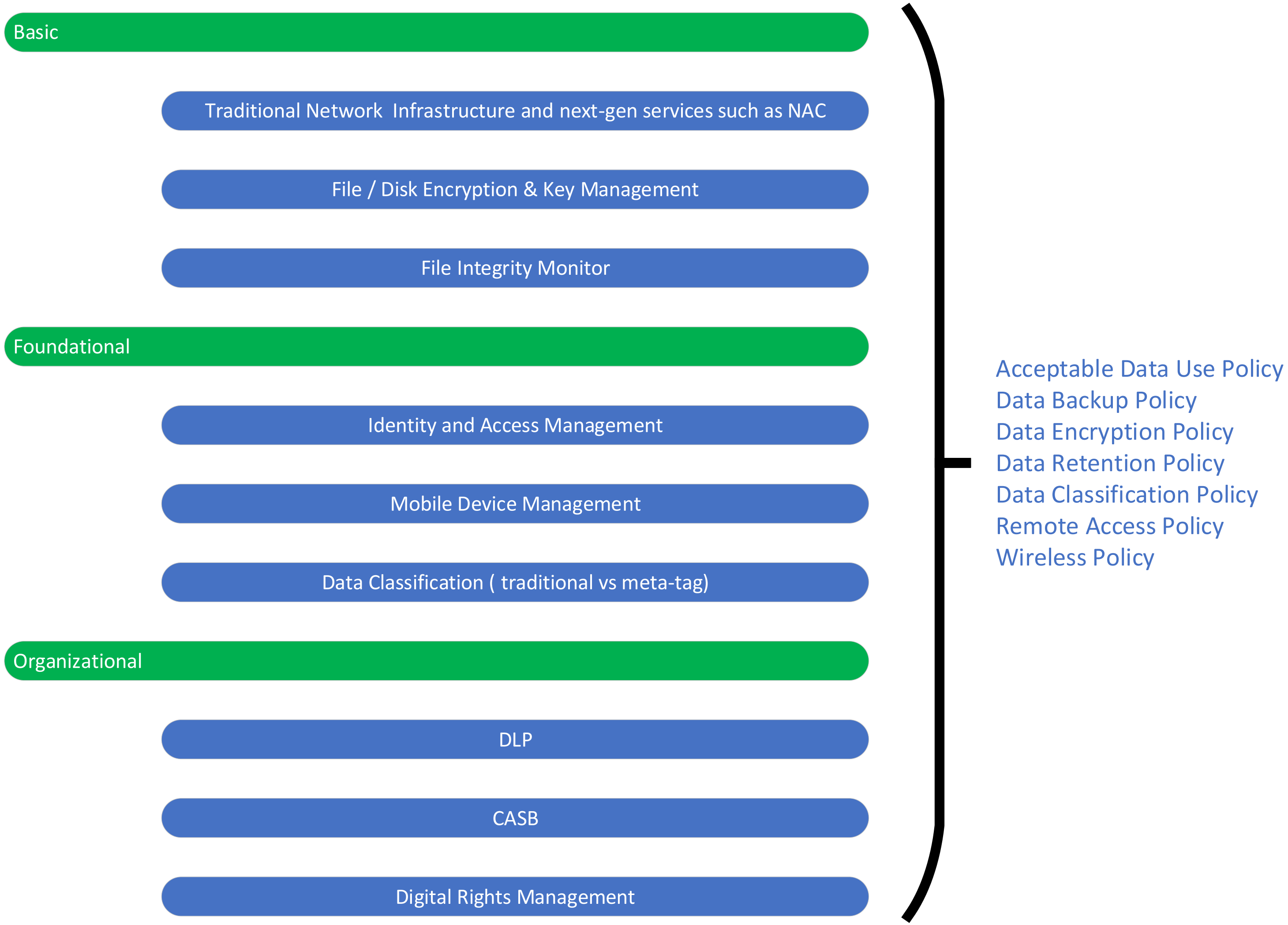
DG: ORGANIZATIONAL CONTROLS
DIGITAL RIGHTS MANAGEMENT (DRM)

- Digital Rights Management (DRM) technologies control how data owned by the publishing organization is used by other people and machines. DRM is all about limiting the ways in which authorized users can interact with the digital content. For consumers we see DRM included in music, video files, and text in e-books. For the enterprise user this could include the ability use, modification, and distribution protected content.
- DRM is a very decisive technology with proponents on both sides.
- DRM cracking is also something we have seen celebrated in 'hacker' communities. So many tools, techniques, and tactics are well defined and communicated.
- Something as simple as a "ping home" embedded into a document could introduce legal liability so consult your legal team with your proposed controls.

MEASURING DATA GOVERNANCE TOOLS

	Store	Process	Transmit	Access	Data Classification	Encrypt	Integrity
Basic							
Traditional Network Infrastructure and next-gen services such as NAC	★		★	★			
File / Disk Encryption & Key Management	★		★			★	★
File Integrity Monitor				★	★		
Foundational							
Identity and Access Management				★			
Mobile Device Management	★	★	★	★		★	★
Data Classification (traditional vs meta-tag)					★		
Organizational							
DLP	★	★	★		★	★	★
CASB	★	★	★		★	★	★
Digital Rights Management				★		★	★

MEASURING DATA GOVERNANCE TOOLS



Basic

- Traditional Network Infrastructure and next-gen services such as NAC
- File / Disk Encryption & Key Management
- File Integrity Monitor

Foundational

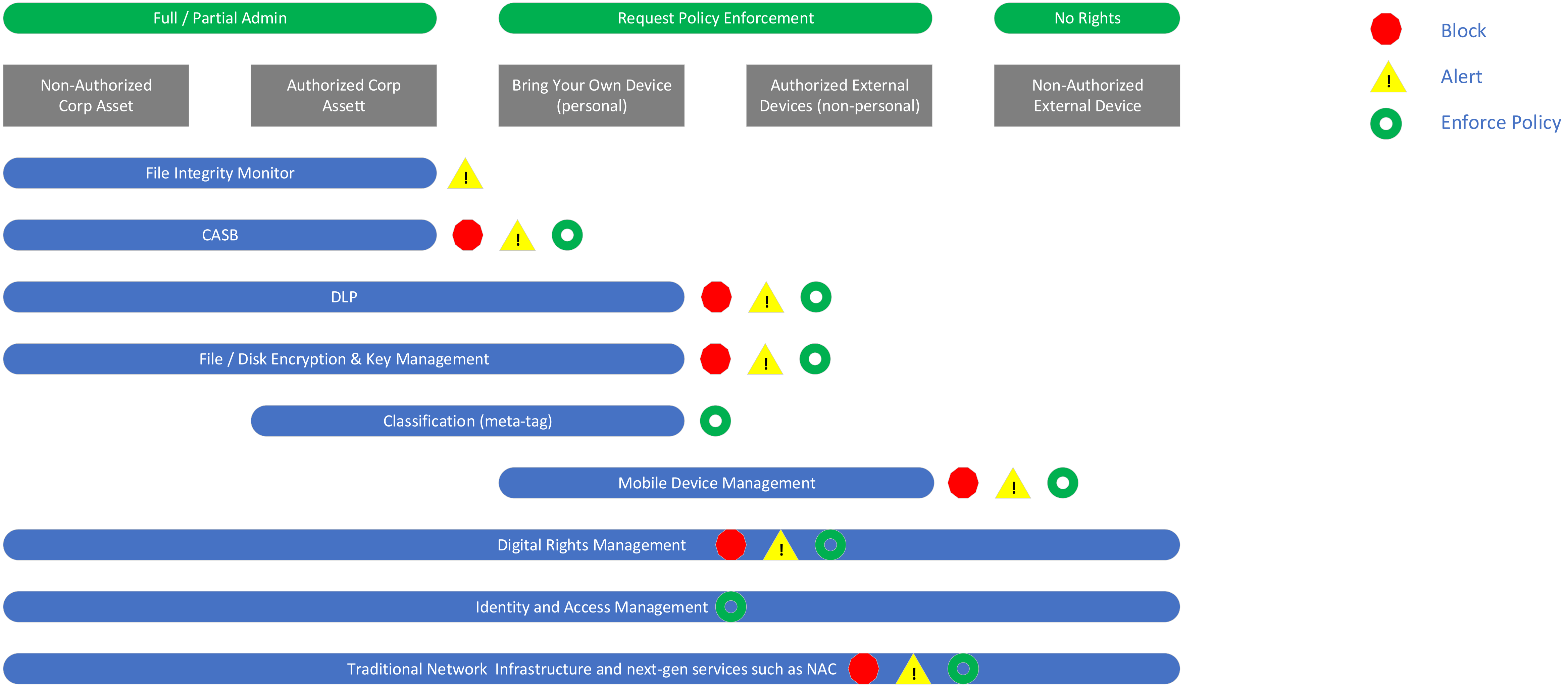
- Identity and Access Management
- Mobile Device Management
- Data Classification (traditional vs meta-tag)

Organizational

- DLP
- CASB
- Digital Rights Management

Acceptable Data Use Policy
Data Backup Policy
Data Encryption Policy
Data Retention Policy
Data Classification Policy
Remote Access Policy
Wireless Policy

MEASURING DATA GOVERNANCE TOOLS



Full / Partial Admin

Request Policy Enforcement

No Rights

Non-Authorized Corp Asset

Authorized Corp Assett

Bring Your Own Device (personal)

Authorized External Devices (non-personal)

Non-Authorized External Device

🛑 Block

⚠ Alert

⭕ Enforce Policy

File Integrity Monitor ⚠

CASB 🛑 ⚠ ⭕

DLP 🛑 ⚠ ⭕

File / Disk Encryption & Key Management 🛑 ⚠ ⭕

Classification (meta-tag) ⭕

Mobile Device Management 🛑 ⚠ ⭕

Digital Rights Management 🛑 ⚠ ⭕

Identity and Access Management ⭕

Traditional Network Infrastructure and next-gen services such as NAC 🛑 ⚠ ⭕

Greater Cincinnati IT Security groups

ISSA

http://www.cincy-issa.org/

SMBA

https://sites.google.com/view/cincysmba

CiNPA

Cincinnati Networking Professionals Association

Security Special Interest Group

SECURITY SIG

https://www.meetup.com/TechLife-Cincinnati/events/

(ISC)²®

https://www.infoseccincy.org/

Thank you! Questions?