Virginia Information Technologies Agency

Welcome and Opening Remarks

Michael Watson

Aug. 1, 2018

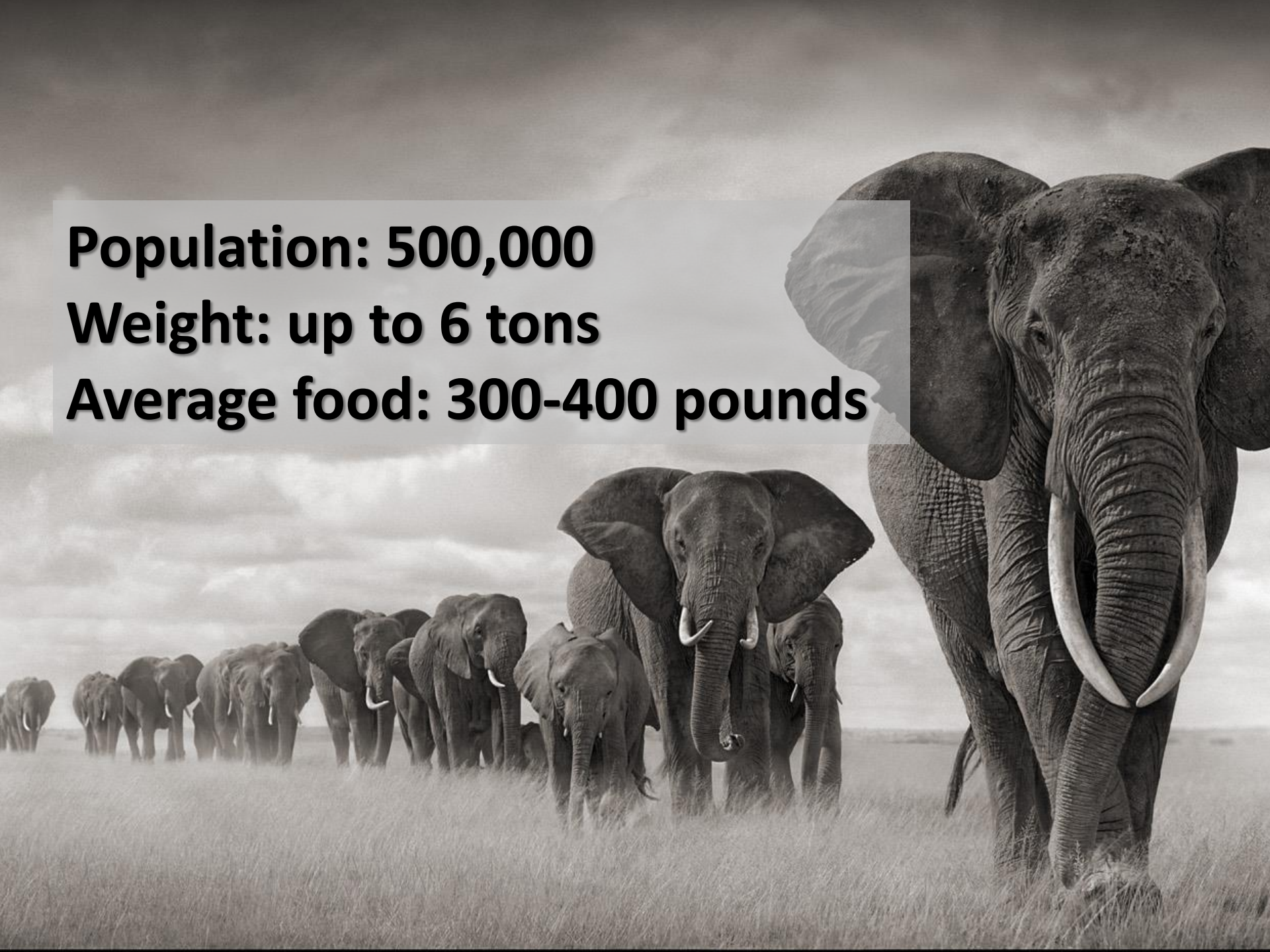
Virginia Information Technologies Agency

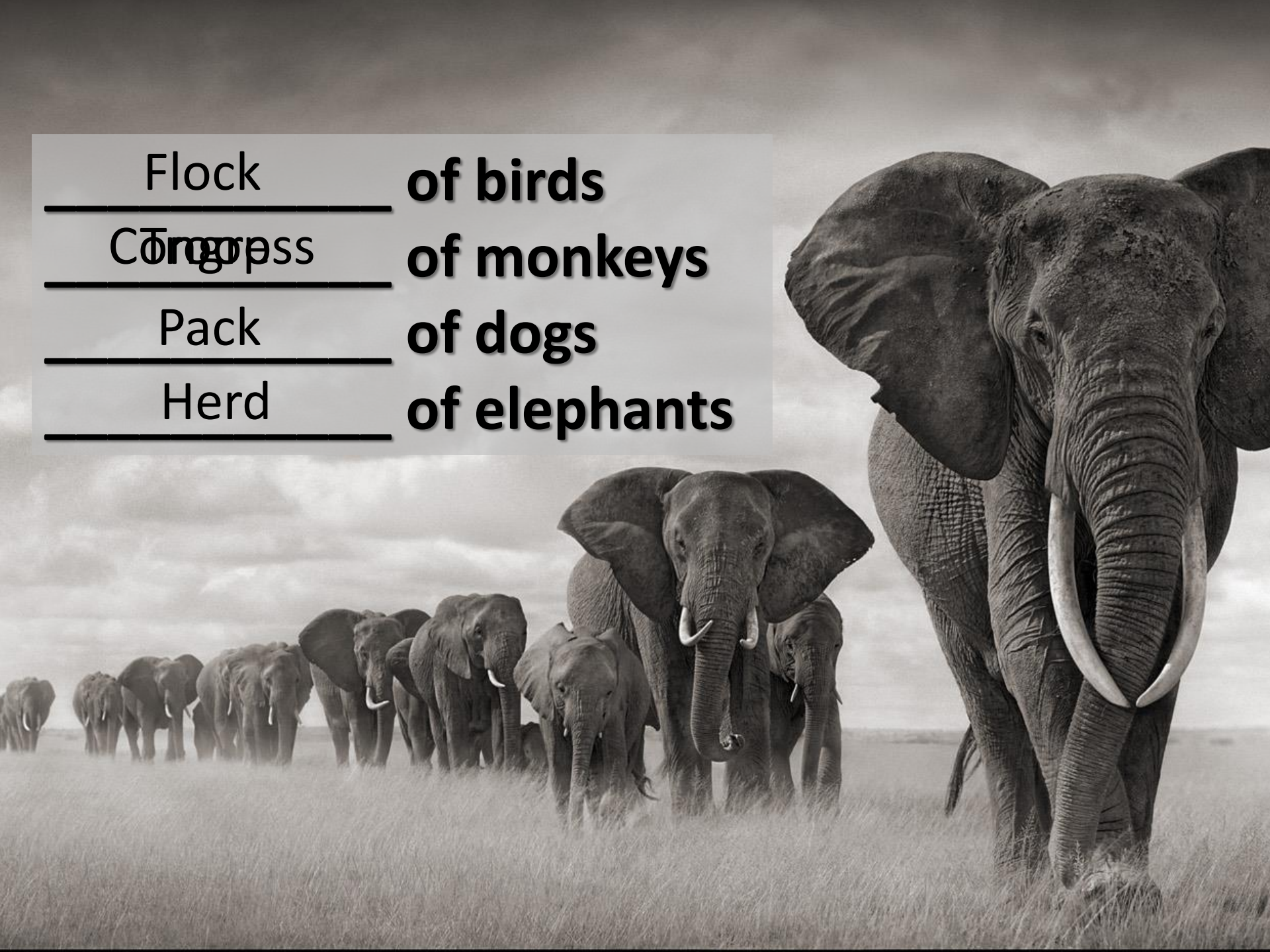
ISOAG Aug. 1, 2018

I. Welcome & Opening Remarks	Mike Watson, VITA
II. How to Train Your Elephant	David Brown, DBHDS
III. IAM Overview	Grayson Walters, SAIC
IV. How To Keep Your Web Sites/Services From Becoming "Low Hanging Fruit"	Kyle Lindsay, VITA
V. SAIC Transition Update	John Craft, VITA
VI. Upcoming Events	Mike Watson, VITA
VII. Operations Update	NG

How to Train Your Elephant

VITA ISOAG August 2018


Population: 500,000
Weight: up to 6 tons
Average food: 300-400 pounds


Flock
of birds
Troop
Congress
of monkeys
Pack
of dogs
Herd
of elephants

Confidentiality
Integrity
Availability
People
Processes
Technology

Technology =

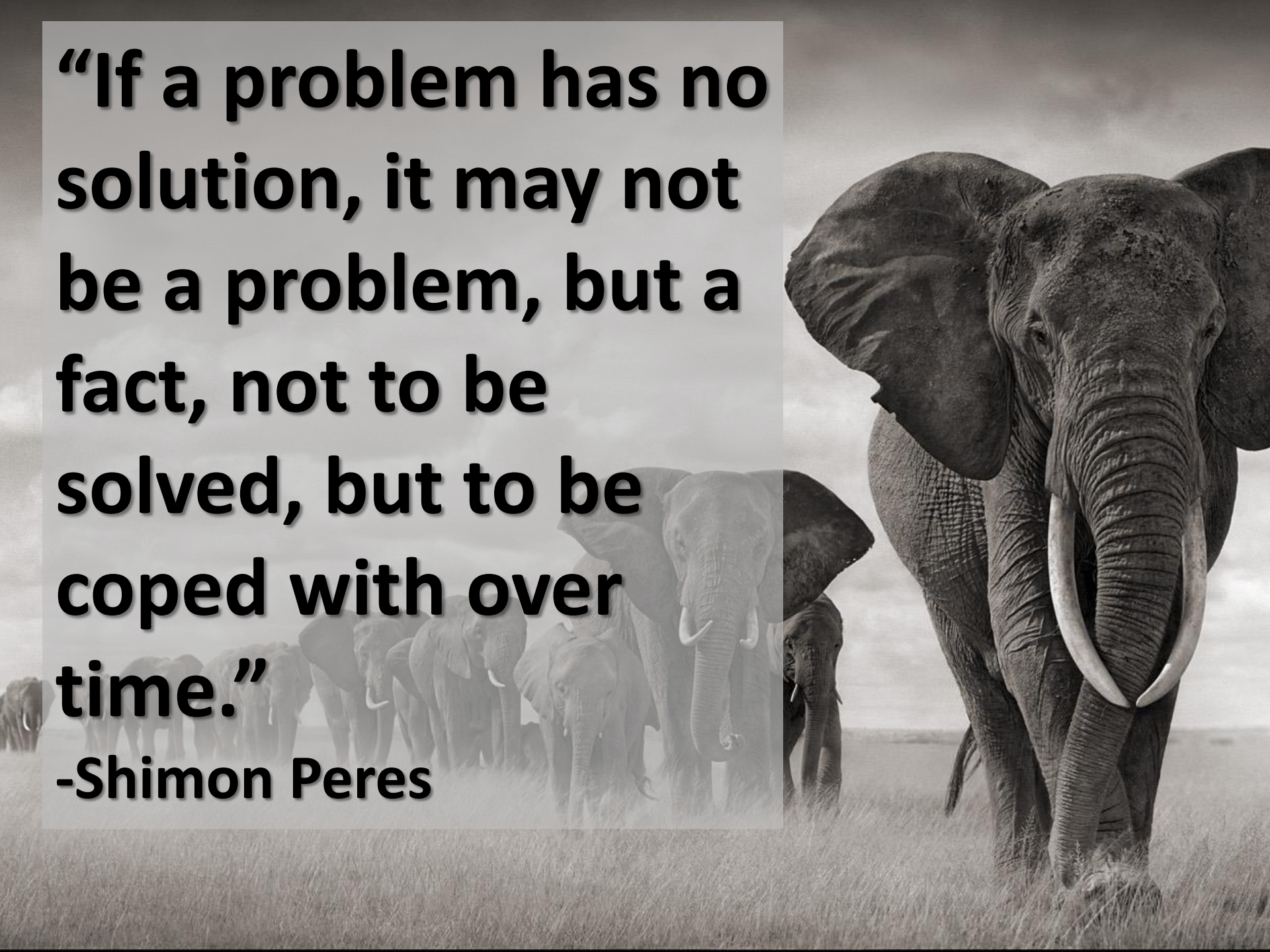
Processes =

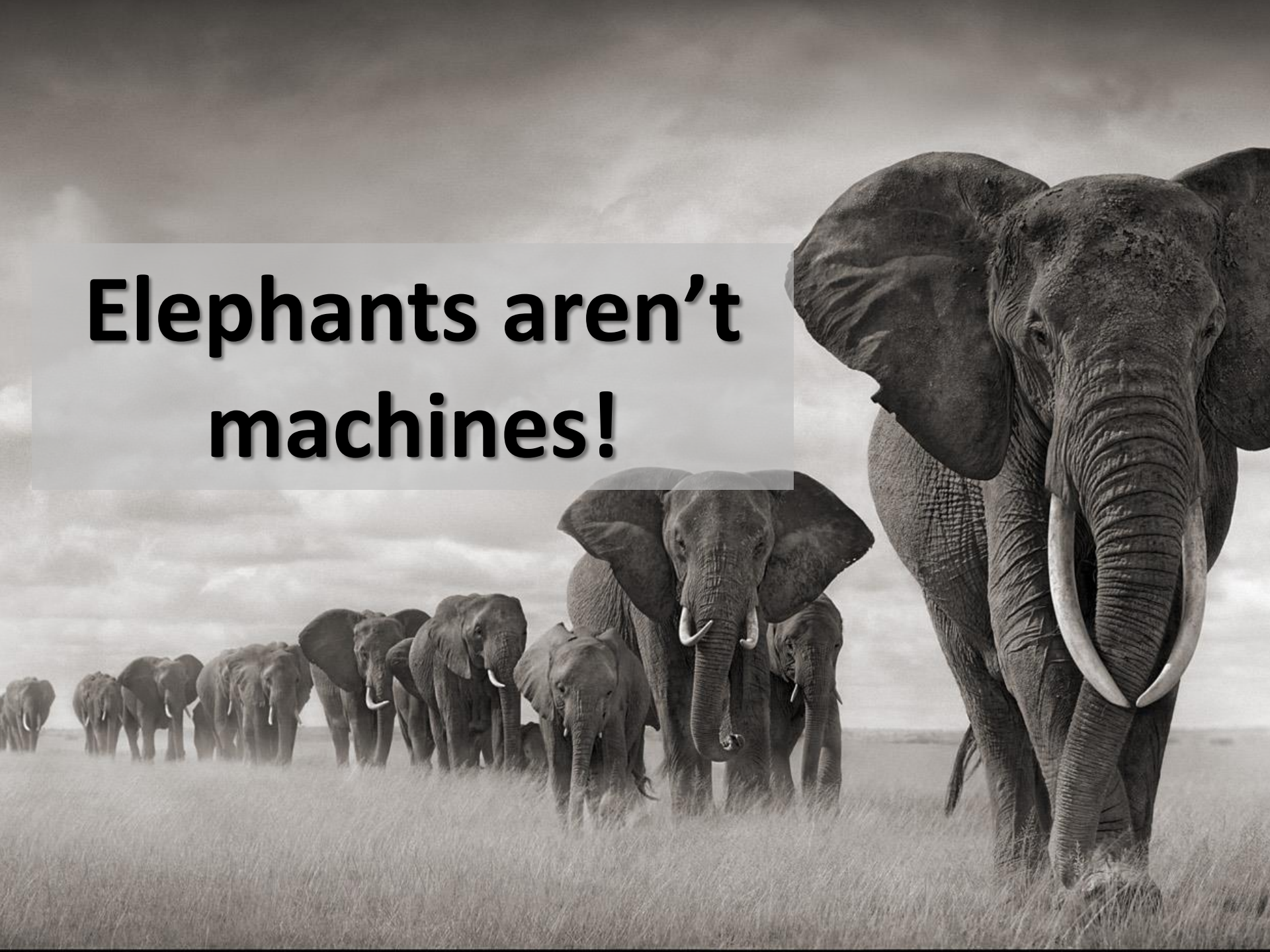
People =

CULTURE

Here's the bottom line:

You can't control your elephant!


“If a problem has no solution, it may not be a problem, but a fact, not to be solved, but to be coped with over time.”
-Shimon Peres


Elephants aren’t machines!

CULTURE

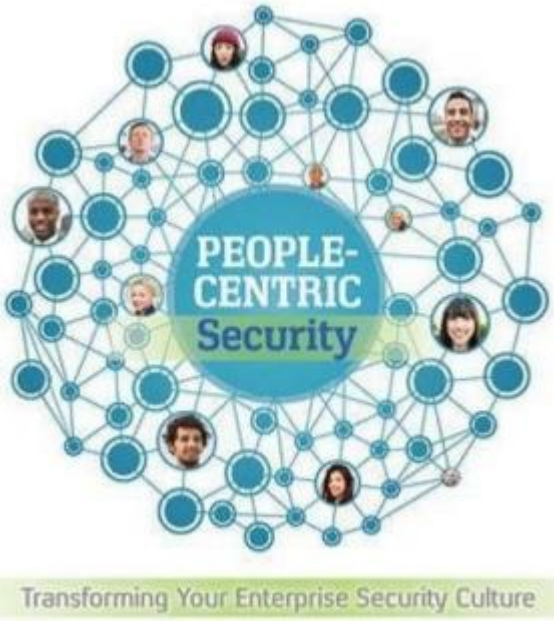
The Ultimatum Game

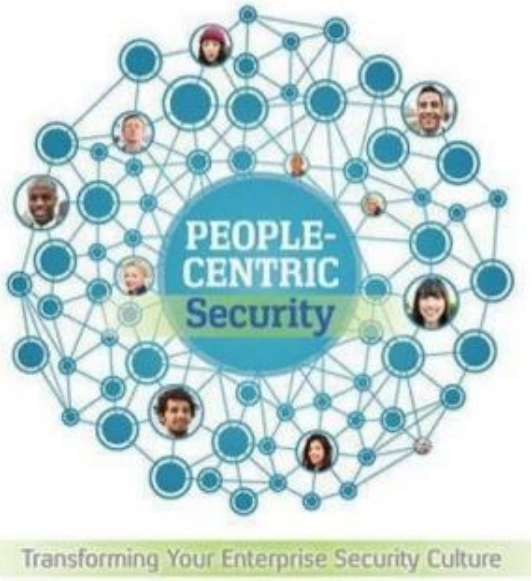
High School

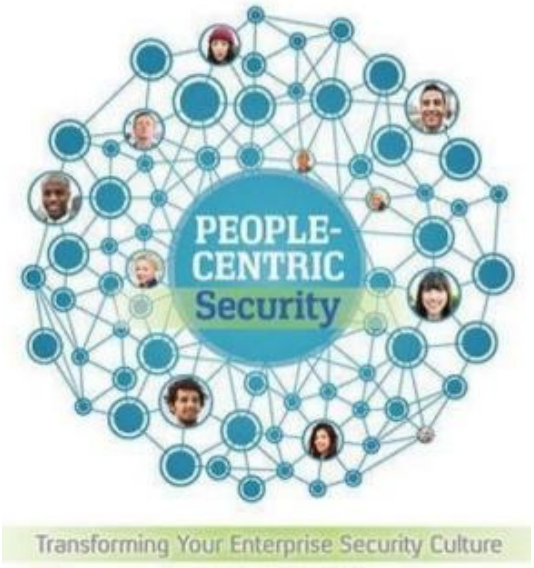
CULTURE

Introduction - Lance Hayden, Ph.D

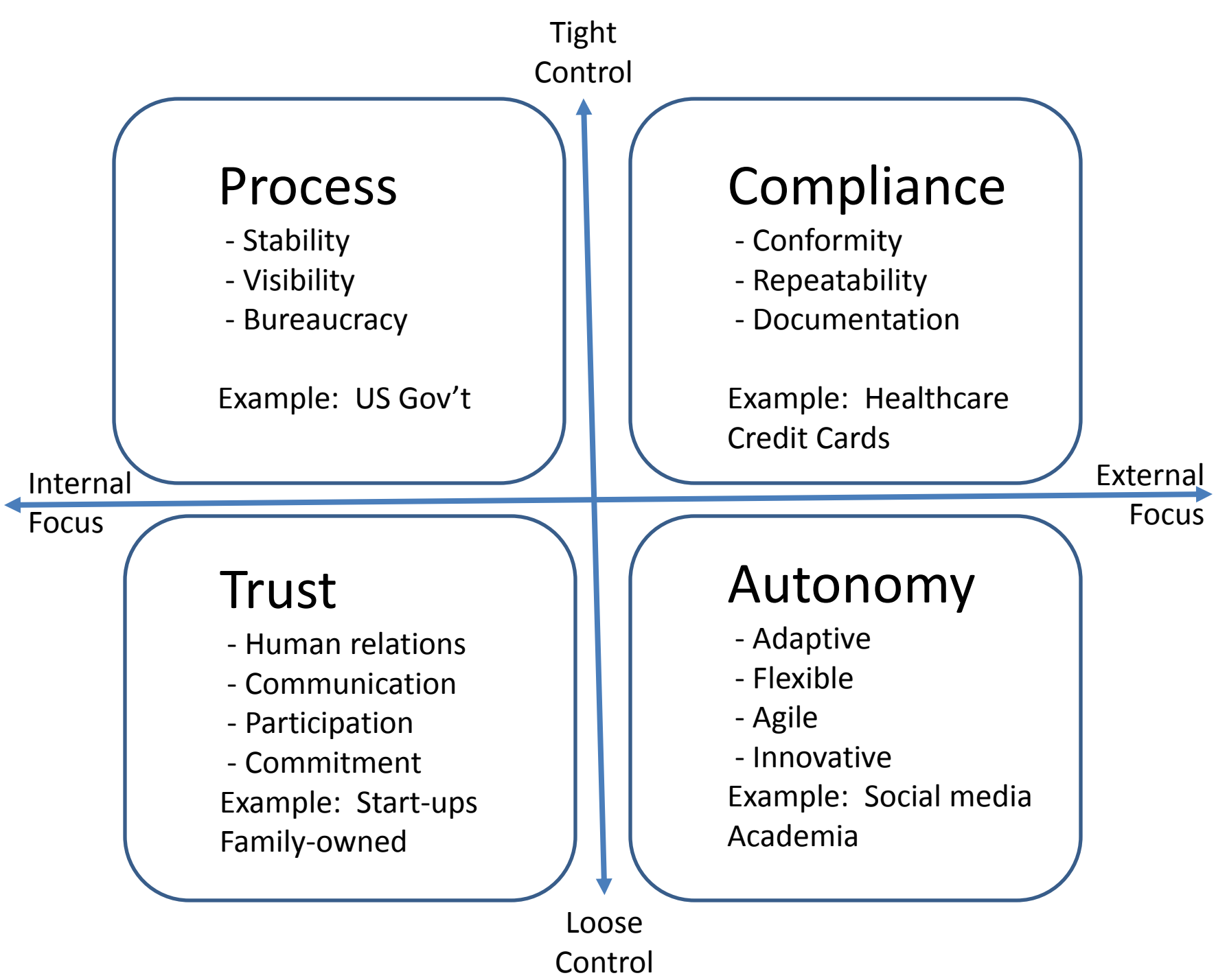
- Managing Director at Berkeley Research Group
- Leads BRG's Cybersecurity Culture Practice
- Research and consulting to help organizations understand, measure, and transform security culture





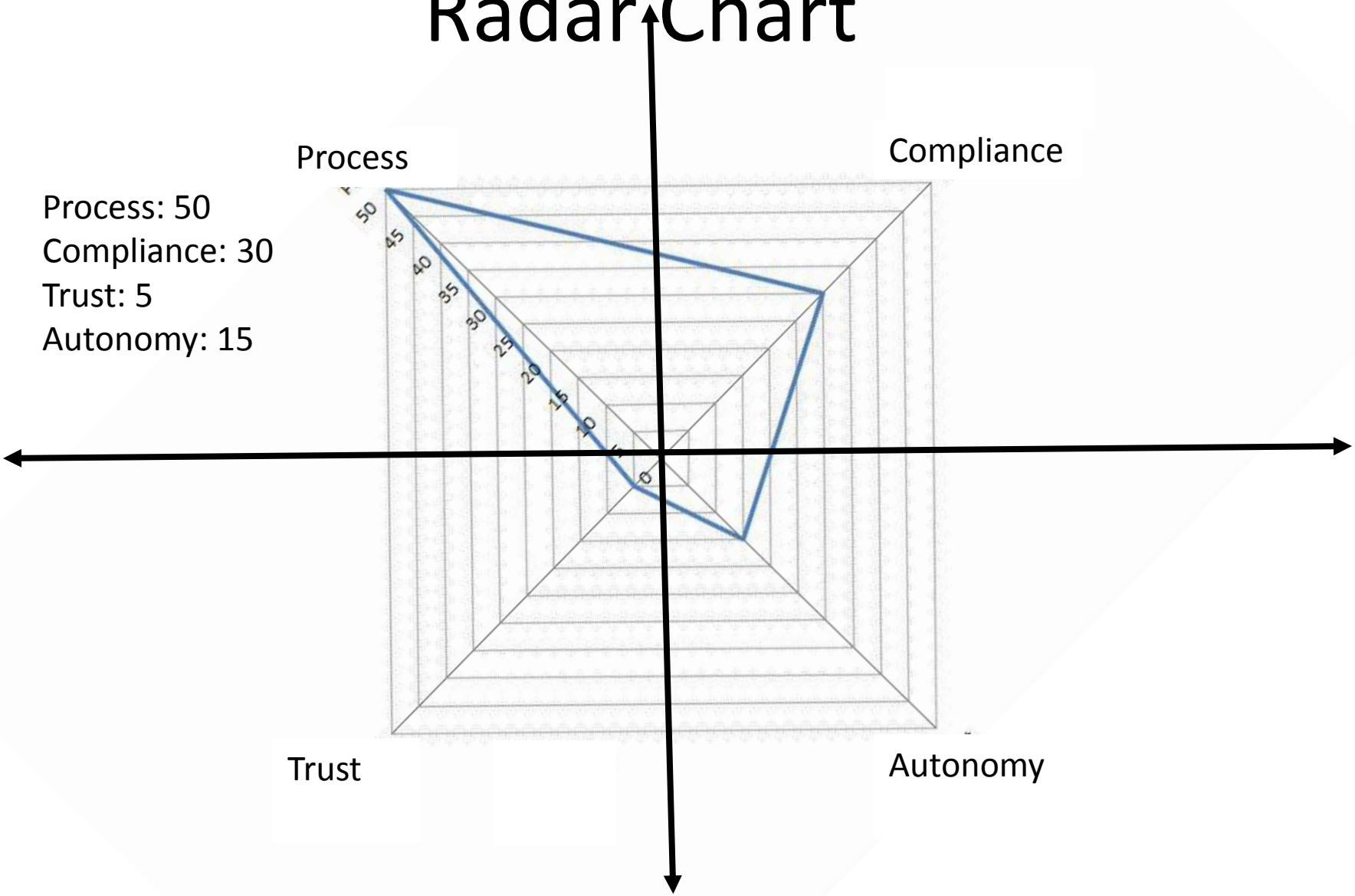


Take the test!

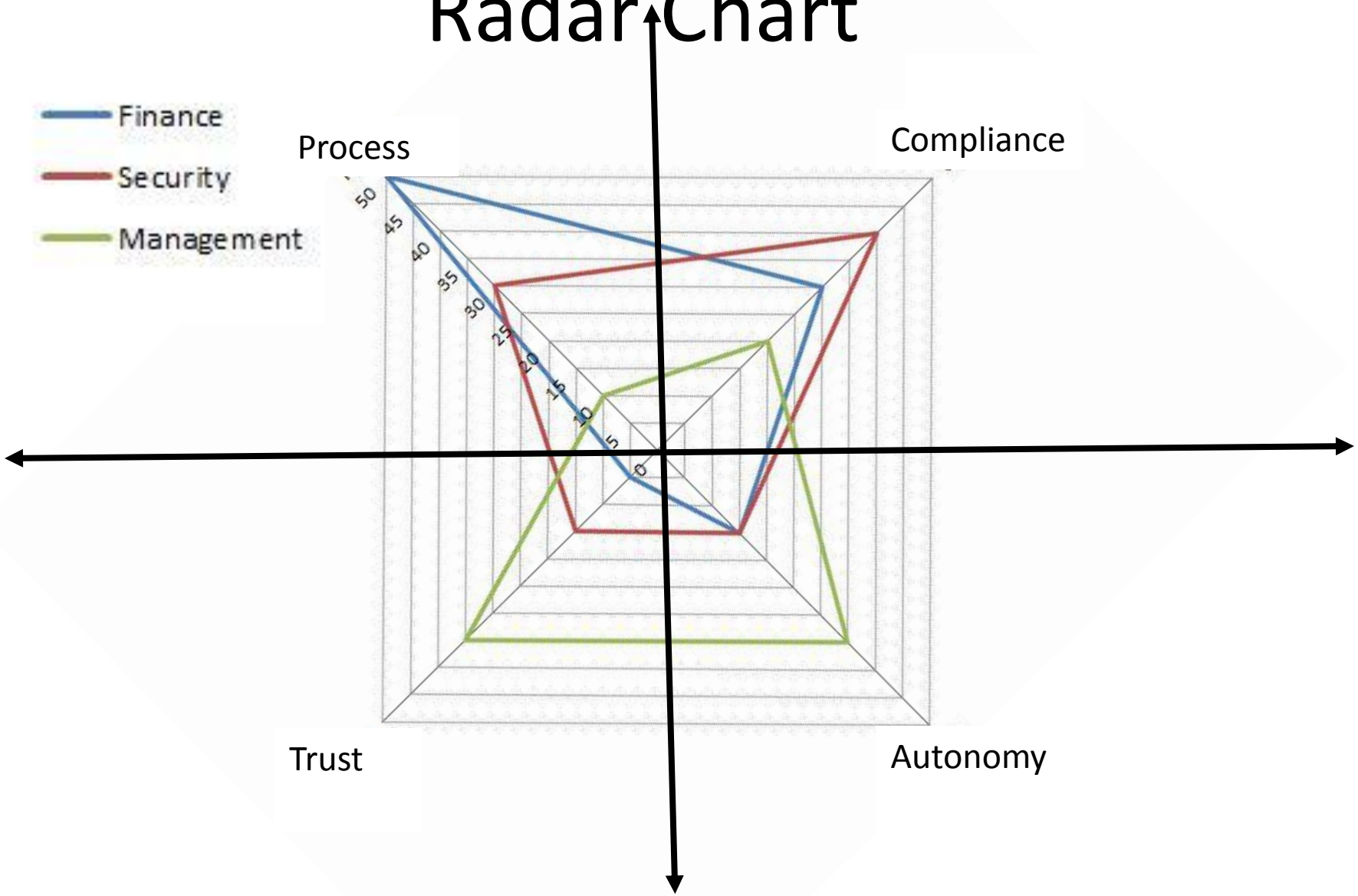

Tight
Control
Process
- Stability
- Visibility
- Bureaucracy
Example: US Gov't
Compliance
- Conformity
- Repeatability
- Documentation
Example: Healthcare
Credit Cards
Internal
Focus
External
Focus
Trust
- Human relations
- Communication
- Participation
- Commitment
Example: Start-ups
Family-owned
Autonomy
- Adaptive
- Flexible
- Agile
- Innovative
Example: Social media
Academia
Loose
Control

Radar Chart

Process: 50
Compliance: 30
Trust: 5
Autonomy: 15



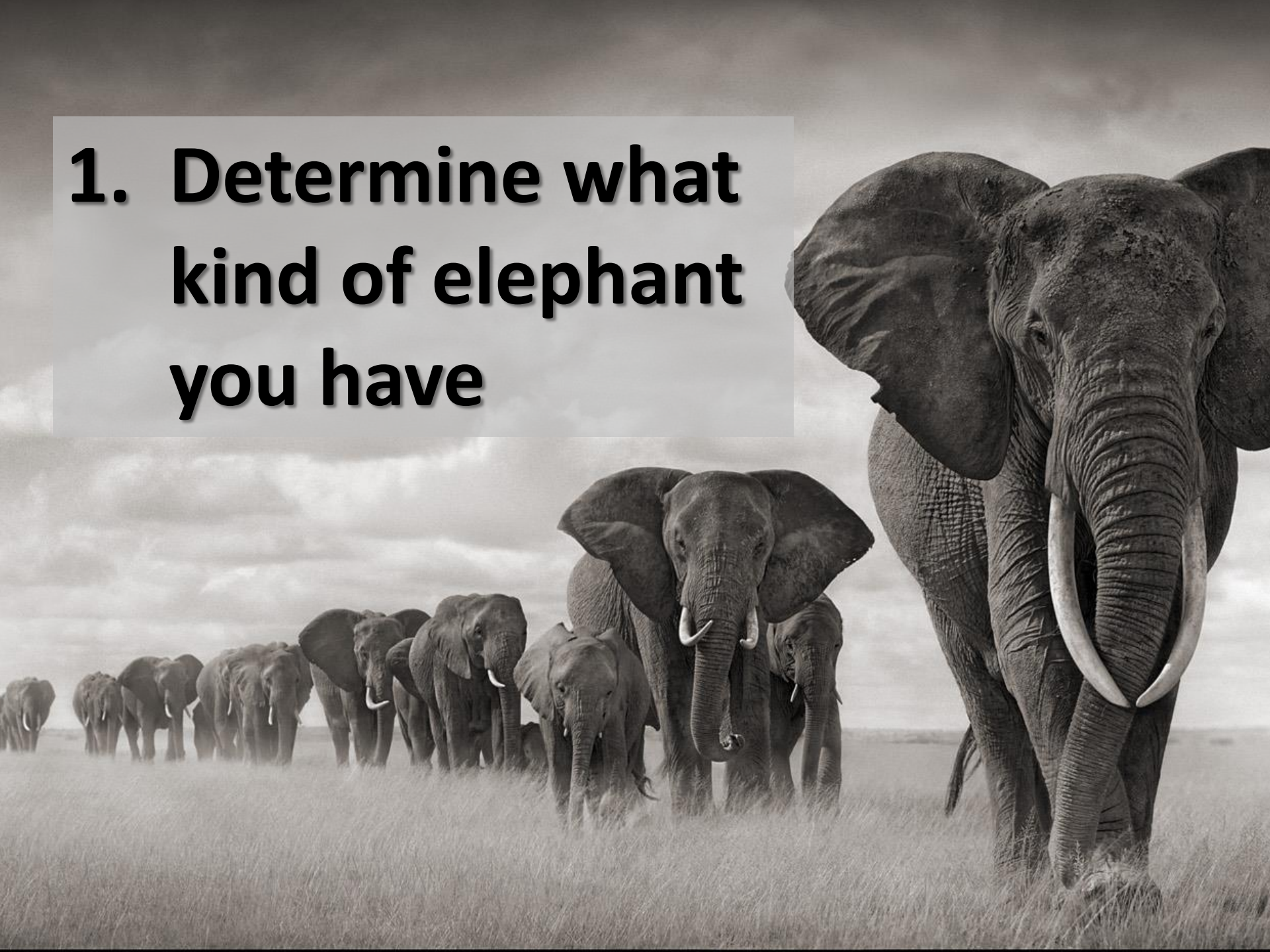
Radar Chart


Finance
Security
Management
Process
Compliance
Trust
Autonomy
50
45
40
35
30
25
20
15
10
5
0

Clara

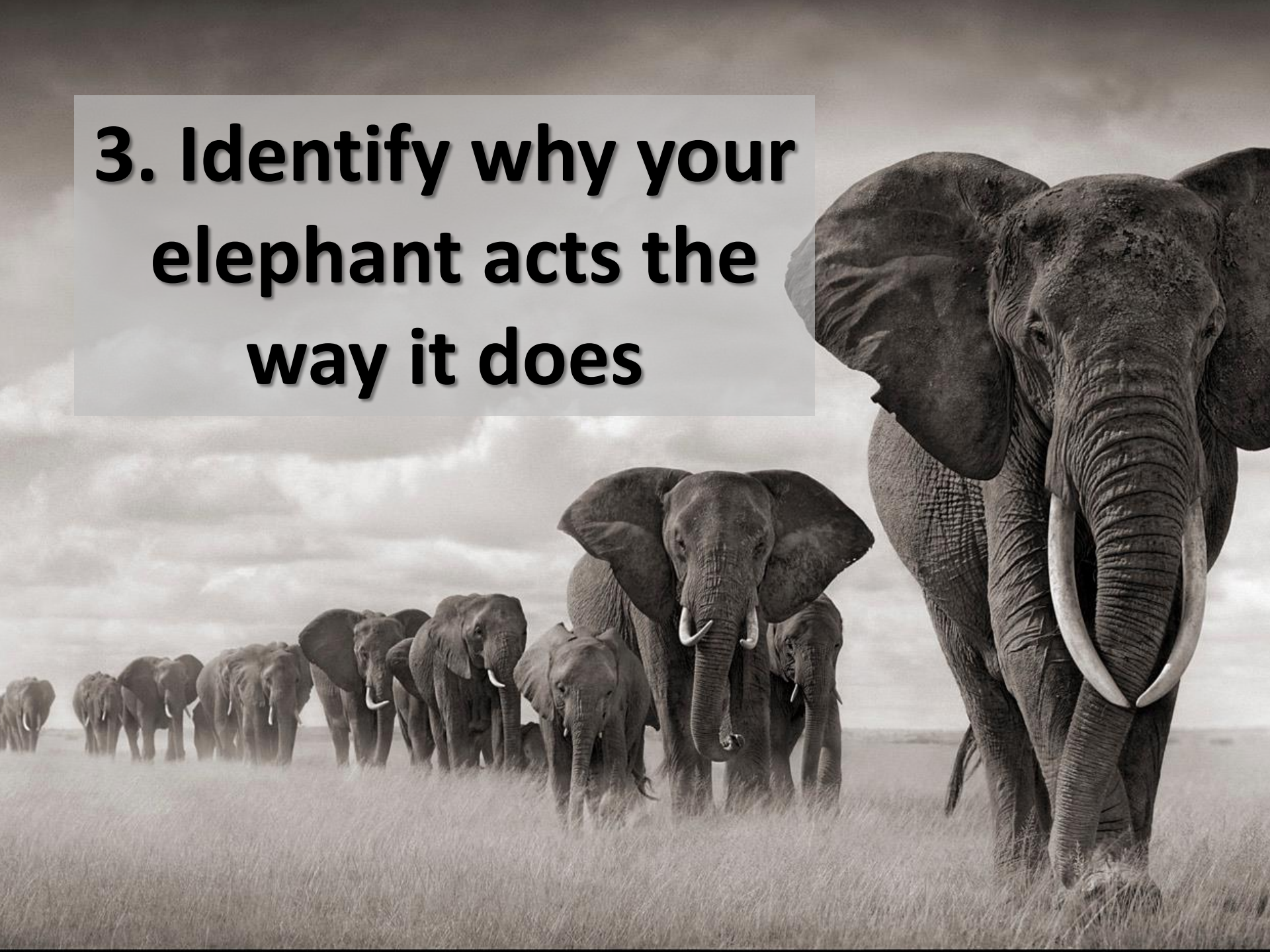
Remember:

You can't control your elephant!


1. Determine what kind of elephant you have

2. Determine what kind of elephant culture you need

3. Identify why your elephant acts the way it does

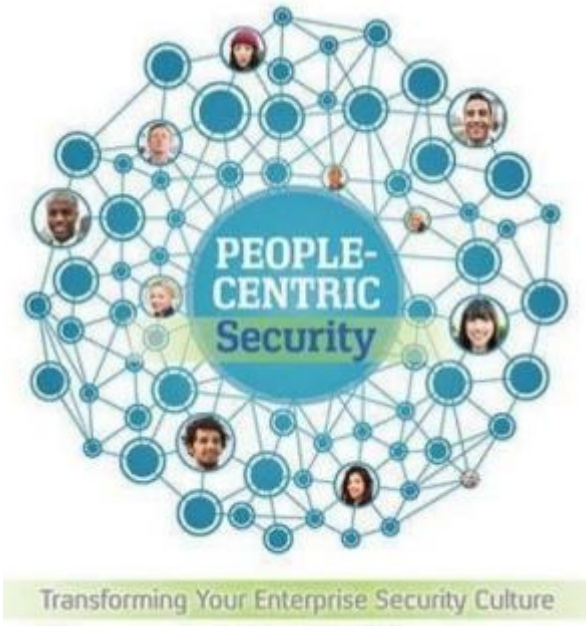


4. Determine how to reward the actions you want

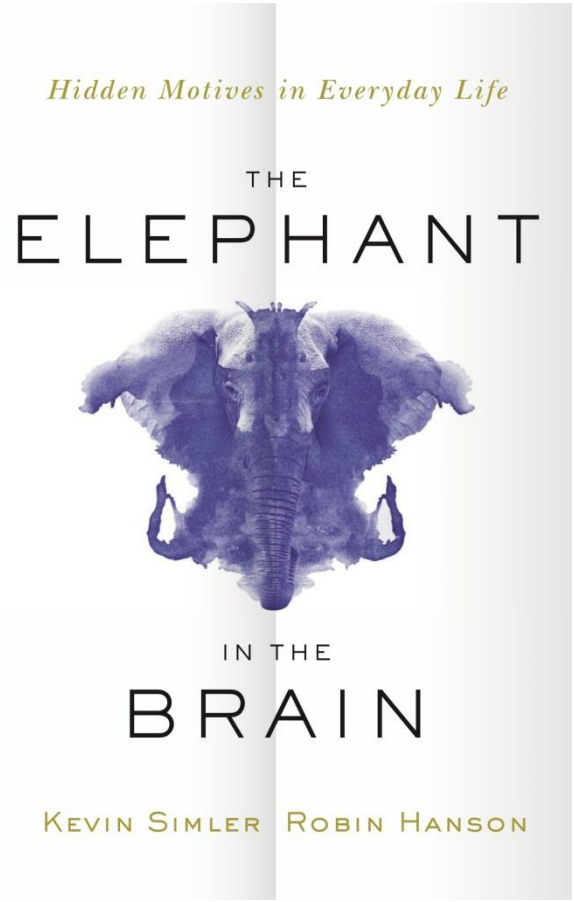
5. Start the process of training your elephant

Culture eats
strategy for
BREAKFAST

Two Great Books



Lance Hayden



How to Train Your Elephant

VITA ISOAG August 2018

Virginia Information Technologies Agency

How To Keep Your Web Sites/Services From Becoming 'Low-Hanging Fruit'

Kyle Lindsay
Security and Incident Response Intern

ISOAG
Aug.1, 2018

Don't Be The Low-Hanging Fruit!

Based on:
RSI Security

Objectives

I. Limit Recon Information

II. Plan and Follow A Patching Schedule

III. Utilize VITA Vulnerability Scan Reports

IV. Avoid Use of Insecure Protocols

Verbose HTTP Headers and Responses

```
HTTP/1.1 200 OK
Date: Thu, 12 Jun 2014 14:15:01 GMT
Server: Apache/2.2.21 (Win32) PHP/5.4.7
Content-Length:226
Connection: close
Content-Type: text/html; charset=iso-8859-1
```

```
HTTP/1.1 200 OK
Date: Thu, 12 Jun 2014 14:15:01 GMT
Server: Apache
Content-Length:226
Connection: close
Content-Type: text/html; charset=iso-8859-1
```

Follow A Patching Schedule

- VITA/server providers handle patching of the OS and base web server software ONLY
  - **ANY** addition software is the responsibility of the agency

- **Research – Test – Deploy**
  - Stay up-to-date on updates to your environment
  - Compare risks to costs

Maintenance Cycle Coordination

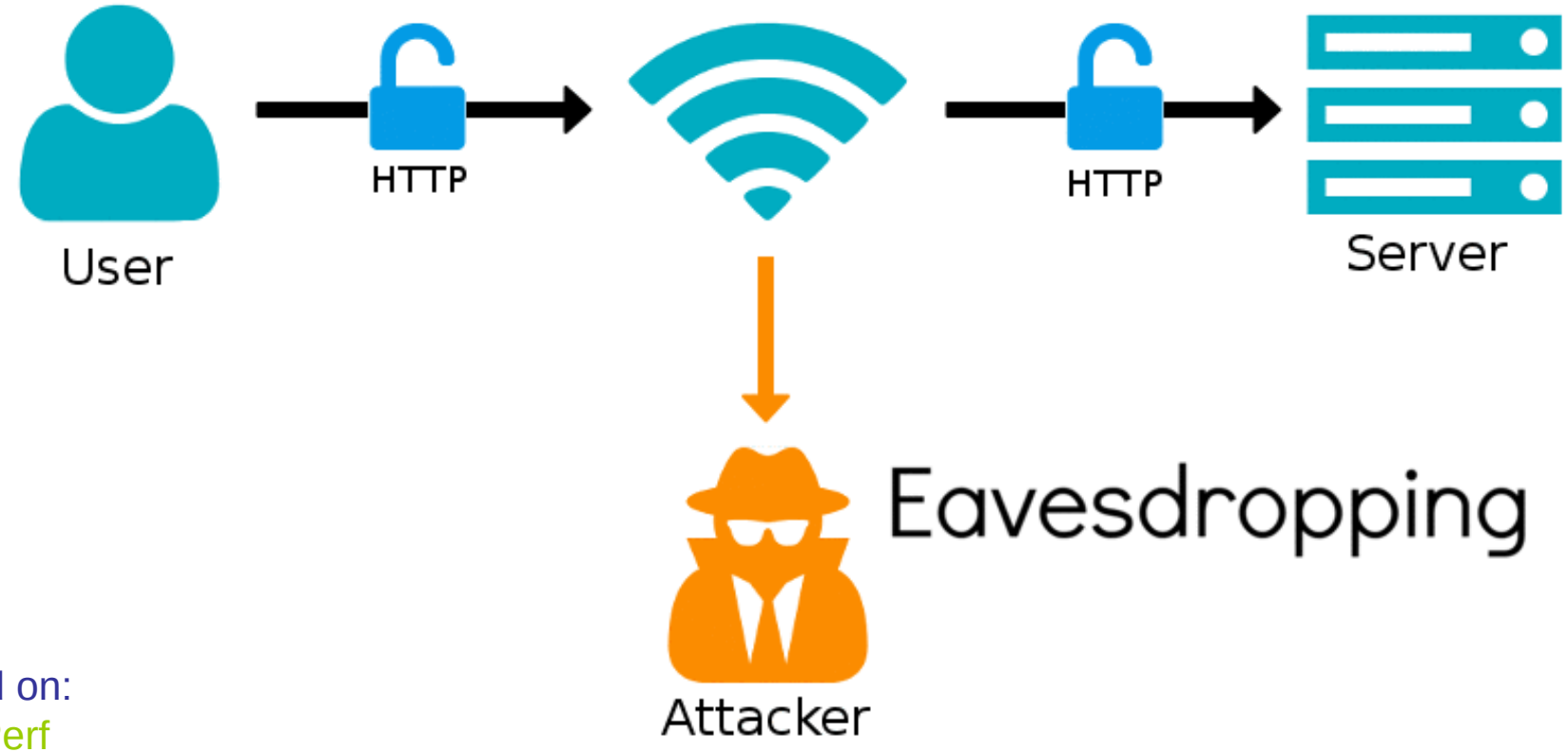
- Verify your team is on the same page
  - Everyone should be aware of the expectations
  - Environment should be understood by all
  - 'Cycles' implies that these processes never end
- Track vulnerabilities and updates
- Set regular intervals to revisit and verify

Utilize Vulnerability Scan Reports

- Reports hold identical data to what malicious parties will utilize for attacks
  - You receive advanced warning
  - Service is included at no addition cost
- Most vulnerabilities are relatively simple to fix
  - Software vendors create patching guides
  - Incorporate quarterly scan results in to your patching schedule if possible

Avoid Insecure Protocols

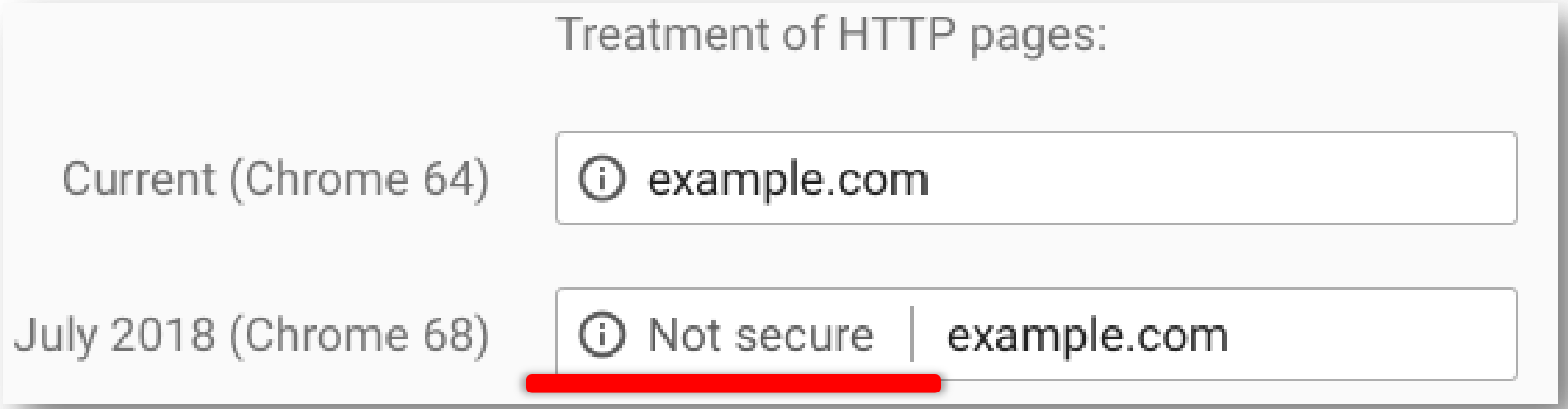
- Allow for practically effortless attacks



Based on:
OctoPerf

HTTP Websites Marked Insecure

Google Chrome now lists **ALL** HTTP websites as "Not secure"



The Hard Truth

- "Update *X* will break my legacy system."
  - Is it time to explore upgrading the system?
  - Can you afford an incident? Would an incident cost less than an upgrade?

- "Security patch *Y* doesn't allow old or outdated clients to connect."
  - Balance security and reduced interoperability
  - Is it ethical to let citizens risk compromise of their own PII by allowing the use legacy clients?

Takeaways

- Don’t make it easy!
- Preemptive actions will safeguard your nights and weekends in the future
- VITA Security is here to help
  - Just ask!

Questions?

Links

- CIS Best Practices
- How to disable verbose HTTP headers

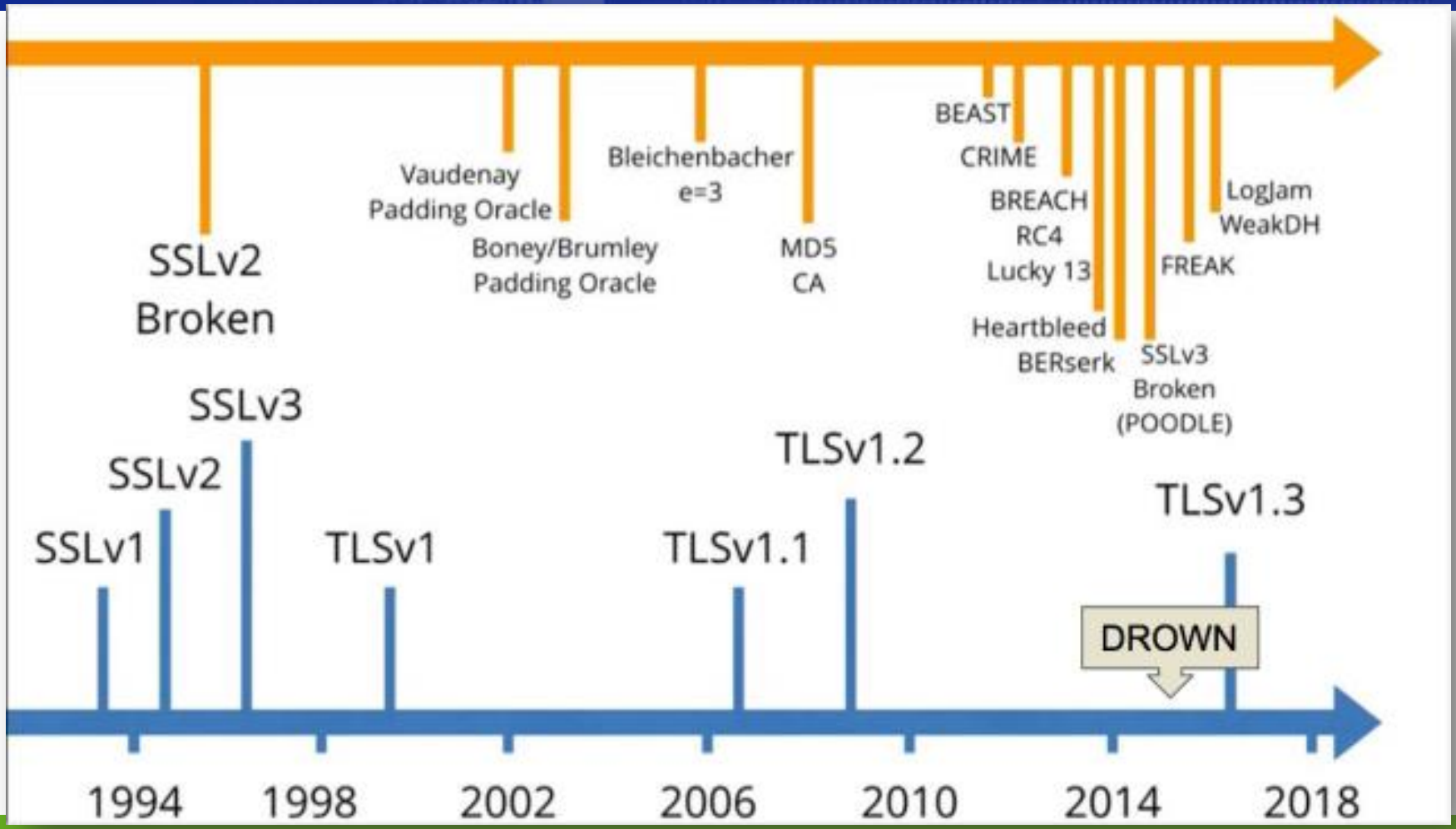
Appendix

1. How To Move to HTTPS
2. Evolution of SSL/TLS Protocols
3. TLSv1.0 Deprecation Notice by PCISSC

How To Move To HTTPS

- Private websites can obtain certificates for free
- Public websites can obtain certificates for a fee
  - Ask your customer account manager for pricing and details

SSL/TLS Evolution



TLS1.0 Deprecated By CC Industry

- Payment Card Industry Security Standards Council set due date for all eCommerce websites of June 30th, 2018
- Also includes all versions of SSL!

  **SSL was replaced by TLS*
- Official Information Supplement

Redefining Ingenuity®

Information Security Officer's Advisory Group

IAM Overview

01 August 2018

Prepared for:

SAIC®
Redefining Ingenuity

© SAIC. All rights reserved.

Security Operations

Grayson Walters

© SAIC. All rights reserved.

Security Clearance Management

Redefining Ingenuity®

Ensuring Compliance for Service Tower Supplier (STS) Personnel

SAIC is providing a comprehensive security clearance database for STS personnel

- The database will track items such as:
  - Completion of background checks
  - Completion of specialized or agency required training
  - Facility Badges

SAIC® Redefining Ingenuity

© SAIC. All rights reserved.

Redefining Ingenuity®

Clearance Database Criteria

Based on Appendix C of the VITA Agency MOU

SAIC®
Redefining Ingenuity

© SAIC. All rights reserved.

© SAIC. All rights reserved.

Identity and Access Management (IAM)

Redefining Ingenuity®

Managing Access

- Changes to access can be initiated from the service portal.
- Many types of access will be provisioned automatically upon completion of the request and approval process.
- Notifications, audit logging, and compliance record retention occur as part of the workflow
- Approved personnel will be able to pull live records from connected systems.

SAIC®
Redefining Ingenuity

© SAIC. All rights reserved.

Redefining Ingenuity®

Getting ahead of the game:

Start looking at your groups in CoV Active Directory

- Clean up descriptions
  - If you mean “Provides Read Only Access to the S Drive” say that instead of the current descriptions which generally say nothing.
- Begin thinking of logical groupings for access
  - Collections of groups that add up to provide a type of access
  - How these collections relate to user roles

SAIC® Redefining Ingenuity

© SAIC. All rights reserved.

Long Term

Solution Designs that provide Identity and Access Management for your applications.

As the BRM group starts up, inform them if you will be interested in deploying the IAM solution for your applications as well.

© SAIC. All rights reserved.

Redefining Ingenuity®

Questions?

SAIC®
Redefining Ingenuity

© SAIC. All rights reserved.

Virginia Information Technologies Agency

SAIC Transition Update

John Craft
Deputy CISO

ISOAG Meeting
August 1, 2018

Transition Patch Hold for 8/17 Cycle

- VITA has authorized a server patch hold for the weekend of 8/17
- Server patching will resume on 8/24
- Servers originally scheduled for patching the weekend of 8/17 will receive August and September patches during the September patch cycle.
- Agencies who wish to make up patches in a later August patch window should coordinate through their CAM.

Clearances

- To ensure a smooth operational changeover, existing VITA security clearances for transitioning NG incumbent staff will be carried over until those employees transition to the new service tower provider. Clearances will be re-certified as part of new service tower employment transition.
- New hires and non-incumbent staff will follow established clearance procedures.
- Agencies should contact their CAMs if they will require re-certification of clearances as part of the transition.

Agency Badges

- VITA is directing NG to not collect agency-issued badges for NG employees transitioning to SAIC.
- We are aware that some agency-issued badges contain a "Northrup Grumman" identifier and will need to be re-issued.

Questions?

Upcoming Events

Future ISOAG

September 12, 2018 @ CESC 1:00-4:00

Speakers:

Prentice Kinser, SAIC

First Sergeant Eric Gowan, VSP

Jayne Holland, NIC, Inc

ISOAG meets the 1st Wednesday of each month in 2018

IS Orientation

When: Thursday, Sept 13, 2018

Time: 10:00 am

Where: CESC

Link :http://vita2.virginia.gov/registration/Session.cfm?MeetingID=10

COVITS 2018

Sept. 5-6

Greater Richmond Convention Center

ADJOURN

THANK YOU FOR ATTENDING

Picture courtesy of www.v3.co.uk