



**WELCOME TO THE**

**MARCH 2, 2022**

**ISOAG MEETING**





## AGENDA

- **WELCOME/INTRODUCTION: MIKE WATSON**
- **DEBI SMITH/VITA**
- **DAVID BROWN/GEORGE WASHINGTON UNIVERSITY**
- **MARCUS THORNTON/OFFICE OF DATA GOVERNANCE & ANALYTICS**
- **HERB SENING, KEITH HILLIARD & GRAYSON WALTERS/SAIC**
- **DARRELL RAYMOND & ERIC TOMPKINS/ATOS**
- **UPCOMING EVENTS**
- **ADJOURN**

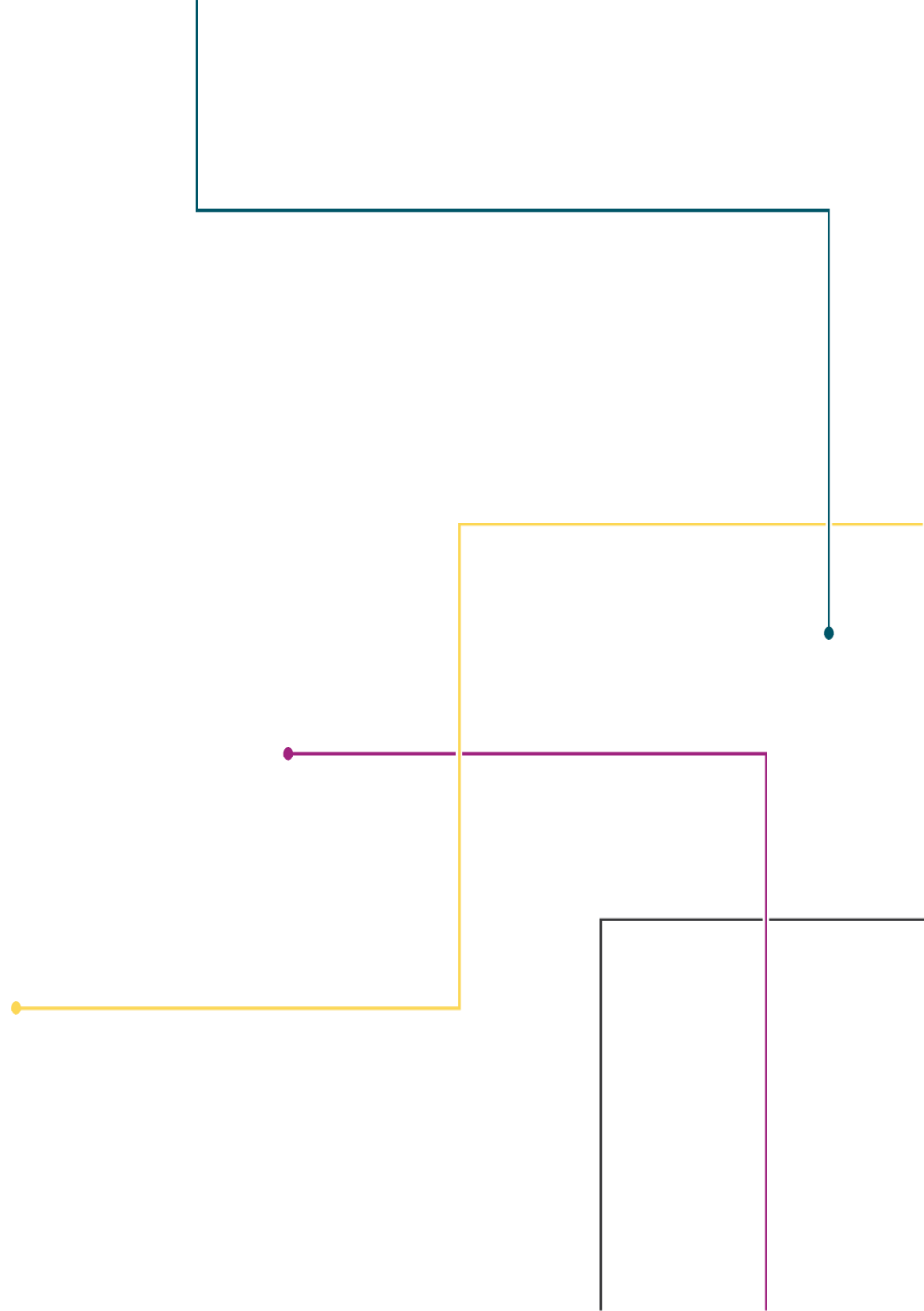


# BLACK KITE OVERVIEW

**DEBI SMITH**  
Security Architect Manager

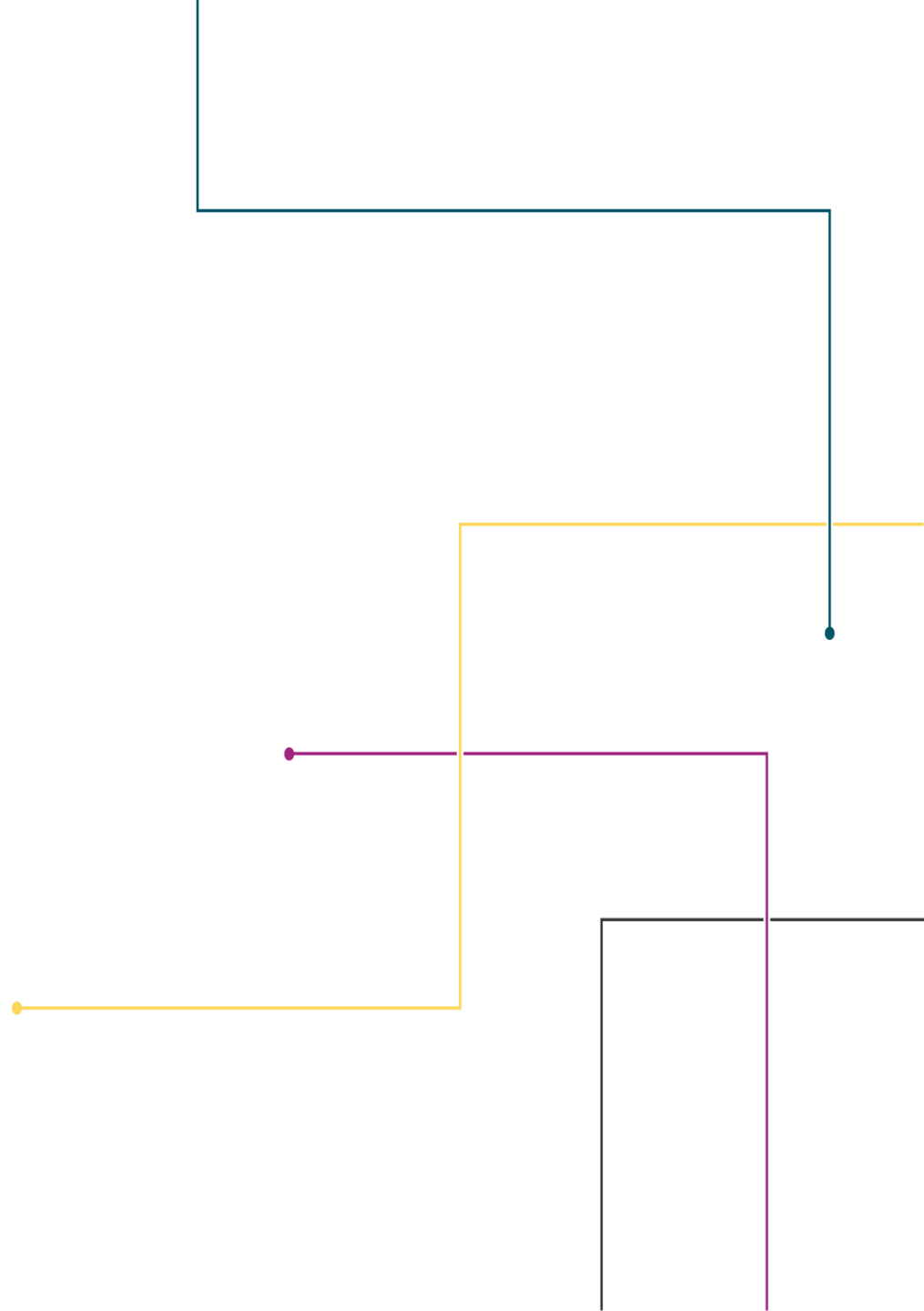
VITA CSRM – ISOAG MEETING

3/2/2022



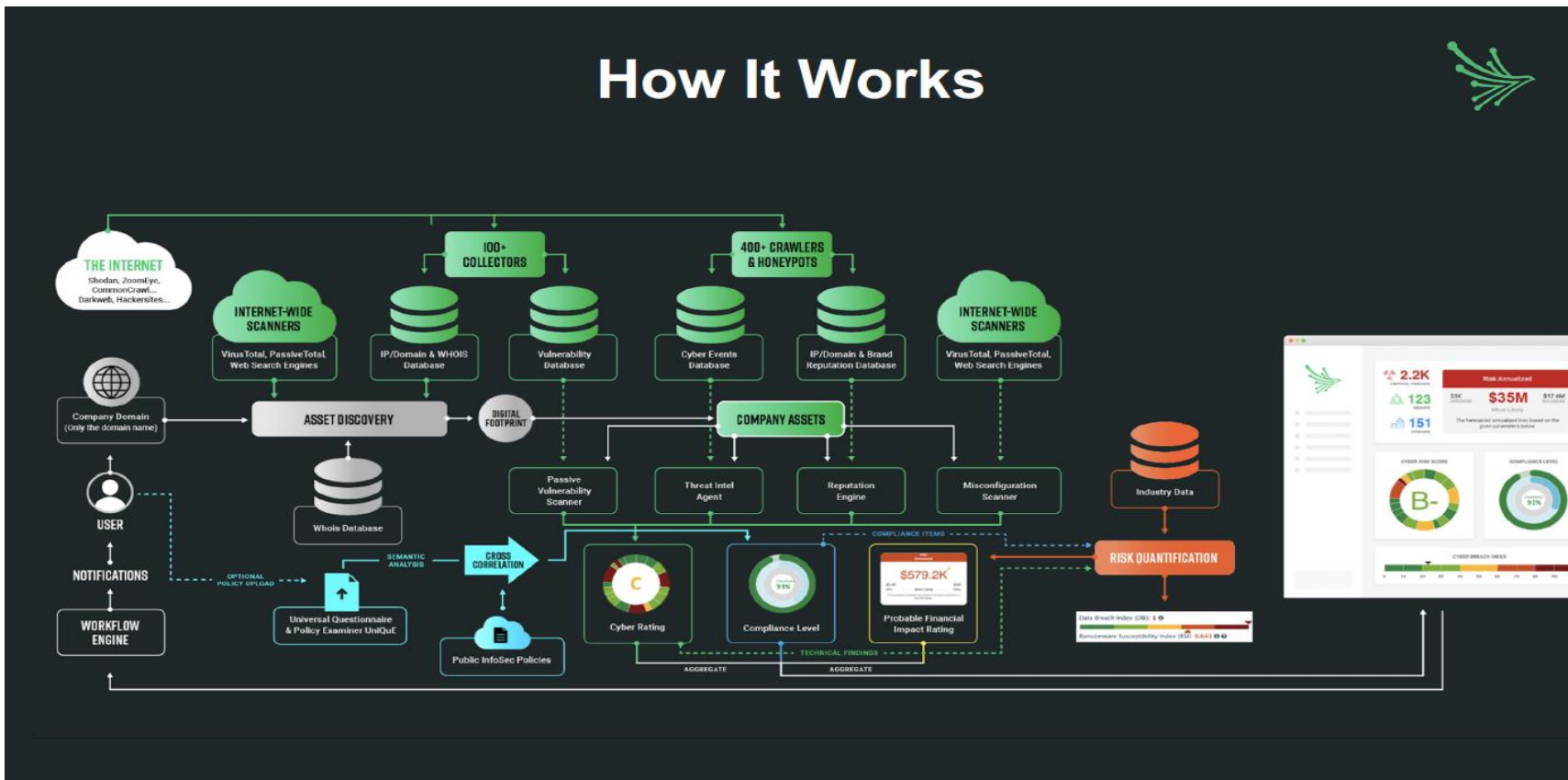
# BLACK KITE

Third Party Risk Platform Tool



- Black Kite Overview
  - Third Party Risk Platform Tool
    - Used for ECOS Assessment Rating & Validation
    - Used for ECOS Oversight Compliance
      - Technical Cyber Rating
      - Risk Quantification
      - Compliance Correlation
      - Ransomware Susceptibility
        - <https://www.blackkite.com>

# How It Works



- Who can request access:
  - Agencies that have an ECOS application in Active Oversight
- How to request access:
  - Have your Agency ISO or Authorized Designee submit a request to the Enterprise Services Mailbox: (enterpriseservices@vita.virginia.gov)
- Notes:
  - Due to the licensing model, we can only offer “Read Only” access at this time



# Why I Quit the IT Security Arms Race

David Brown

George Washington University MFA

ISOAG

March 2, 2022

[www.menti.com](http://www.menti.com)

enter code 6631 3842







# Why I Quit the IT Security Arms Race

David Brown

George Washington University MFA

ISOAG

March 3, 2022

[www.menti.com](https://www.menti.com)

enter code 6631 3842



# Why I Quit the IT Security Arms Race

## David Brown

After completing this session, the participant will be able to ask the right questions to determine their greatest vulnerability

After completing this session, the participant will be able to put a monetary value on all identified vulnerabilities

After completing this session, the participant will be able to develop a strategy for mitigating their greatest vulnerabilities

After completing this session, the participant will be able to realign their budgets to meet strategic needs rather than industry trends

# Why I Quit the IT Security Arms Race

David Brown

## Four Recommended Books

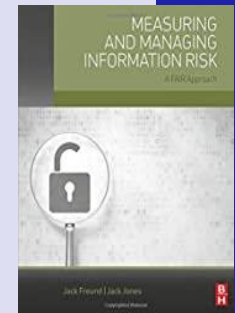
Roger Grimes “A Data Driven Computer Security Defense”



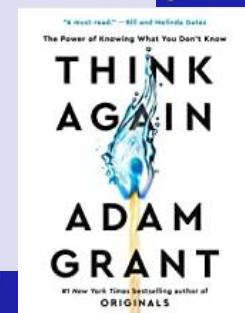
Douglas Hubbard and Richard Seiersen  
“How to Measure Anything in Cybersecurity Risk”



Jack Freund/Jack Jones  
“Measuring and Managing Information Risk”



Adam Grant “Think Again”



# Why I Quit the IT Security Arms Race

David Brown

## Survey Question 1

Which of these attack vectors is the most likely way your organization will be breached in 2022?

Go to:

[www.menti.com](https://www.menti.com)

Enter code 6631 3842

# Why I Quit the IT Security Arms Race

## David Brown

### The Answer

Which of these attack vectors is the most likely way your organization will be breached in 2022?

**a. Social Engineering (Phishing, Vishing, Impersonation)**



# 2020 Threat Landscape

Relentless credential phishing

Sophisticated attacks on Office 365 & G Suite accounts

Complex multi-stage threats

Legitimate filesharing abuse

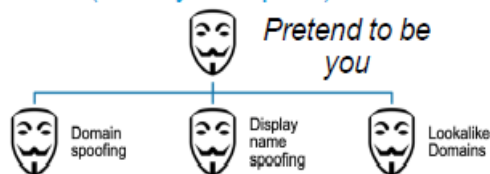
More BEC + EAC variants

**Almost 100% of threats are human-activated**

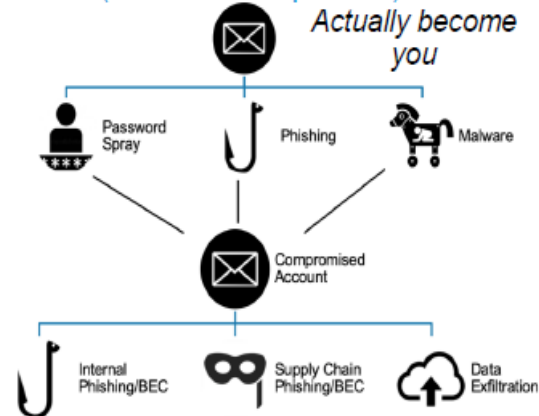
**U.S. Healthcare incurs the highest average per breach costs at \$7.13M**

*Source: IBM Security*

## Business Email Compromise (Identity Deception)



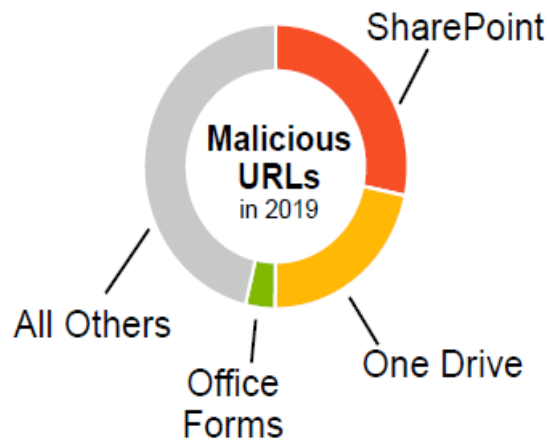
## Email Account Compromise (Technical Compromise)



**\$26.2B+**  
Losses worldwide from BEC and EAC (June 2016 – July 2019)  
[Source: FBI](#)

## O365/G SUITE ACCOUNT COMPROMISES

- 93%** Organizations targeted over 6 months (1H 2020)
- 45%** Organizations with compromised accounts
- 6%** Organizations with a compromised VIP account
- 13** Average compromised accounts per breached organization

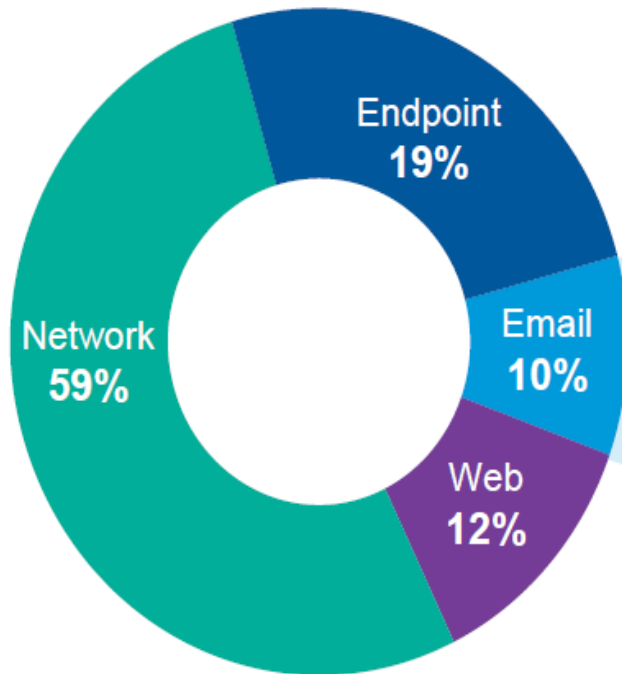


Microsoft  
**53.7%**  
of malicious URLs from legitimate file shares



# Defenders Don't Focus on People, Attackers Do

## SECURITY SPENDING



Source: Gartner Information Security, Worldwide 2017-2023, 2Q 2019 update (2019 forecast)

## BREACHES



Source: 2019 Verizon DBIR



# Why I Quit the IT Security Arms Race

David Brown

## Why the disconnect?

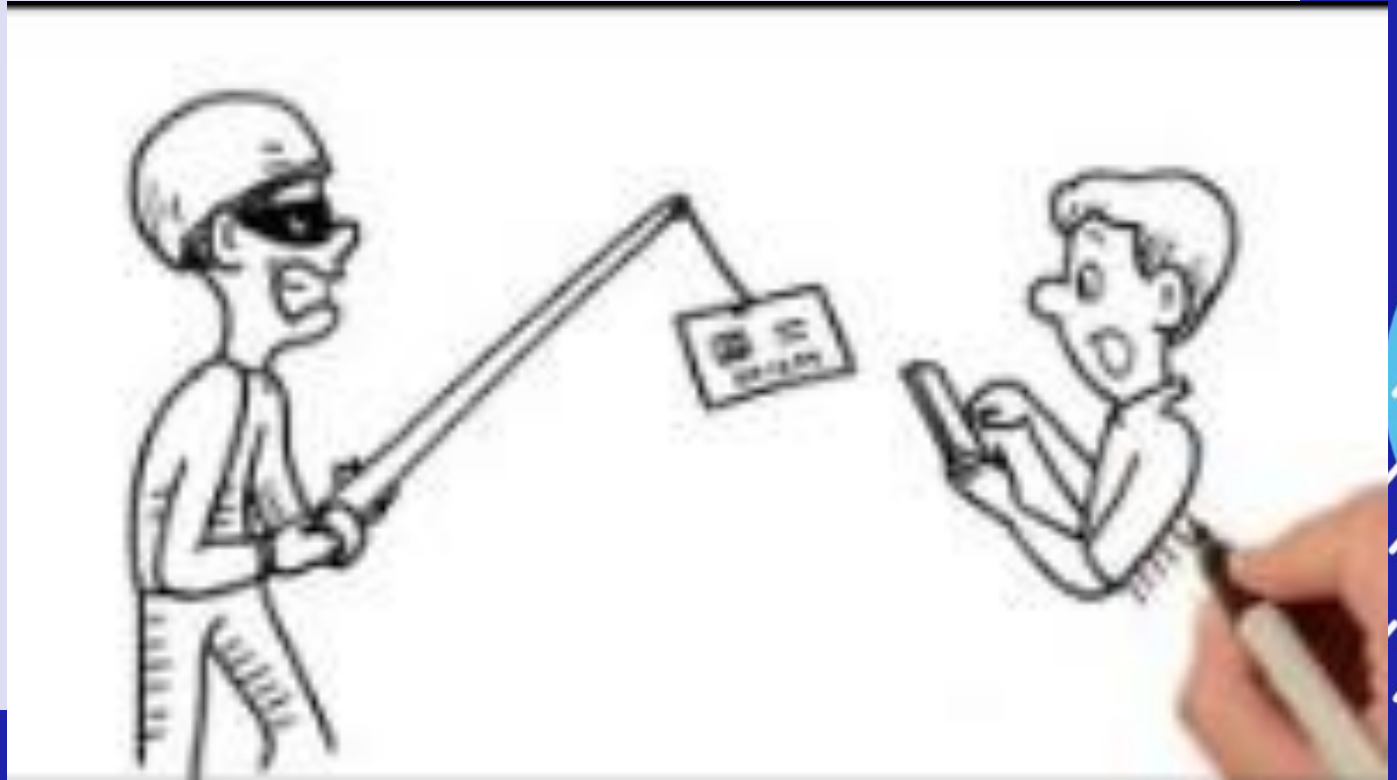
1. We are not asking the right questions.



# Why I Quit the IT Security Arms Race

David Brown

Hacknotice.co  
m



# Why I Quit the IT Security Arms Race

## David Brown

**HACKNOTICE** Business Individual Use Cases Partners Company Blog Resources [LOGIN](#) [REQUEST A DEMO](#) [Q](#)

# Build a culture of security using actionable threat intelligence

With a continuous security awareness platform, all employees protect the company and build good habits

[LEARN MORE](#)

Get an instant risk report now

Term \*

[SUBMIT](#)

# Why I Quit the IT Security Arms Race

David Brown

## Hacknotice.com

2018 29,562 breaches reported  
2019 44,863 breaches reported (51% increase)  
2020 67,529 breaches reported (50% increase)

“Hackers are winning the cyberwar largely because they don’t target the infrastructure, but they target people. “

# Why I Quit the IT Security Arms Race

David Brown





# Why I Quit the IT Security Arms Race

David Brown

## BAD RABBIT

If you access this page your computer has been encrypted.

Time left before the  
price goes up

41:18:14

Price for decryption:

 - 0.05

Enter your personal key or your bitcoin address



# Why I Quit the IT Security Arms Race

David Brown

## Why the disconnect?

1. We are not asking the right questions.  
Focus on root causes not the damage done!

# Why I Quit the IT Security Arms Race

David Brown

## Why the disconnect?

1. We are not asking the right questions.  
Focus on root causes not the damage done!
2. End users are HARD!

# Why I Quit the IT Security Arms Race

## David Brown

### Why the disconnect?

1. We are not asking the right questions.  
Focus on root causes not the damage done!
2. End users are **HARD!**





# Why I Quit the IT Security Arms Race

David Brown

## Why the disconnect?

1. We are not asking the right questions.  
Focus on root causes not the damage done!
2. End users are HARD!



# Why I Quit the IT Security Arms Race

## David Brown

What are the right questions?

1. What attacks have occurred in the last 12 months?

# Why I Quit the IT Security Arms Race

## David Brown

What are the right questions?

1. What attacks have occurred in the last 12 months?
2. Which were successful?

# Why I Quit the IT Security Arms Race

## David Brown

What are the right questions?

1. What attacks have occurred in the last 12 months?
2. Which were successful?
3. What was the cost/damage?

# Why I Quit the IT Security Arms Race

## David Brown

What are the right questions?

1. What attacks have occurred in the last 12 months?
2. Which were successful?
3. What was the cost/damage?
4. Which users/departments are attacked the most?



# Why I Quit the IT Security Arms Race

## David Brown

What are the right questions?

1. What attacks have occurred in the last 12 months?
2. Which were successful?
3. What was the cost/damage?
4. Which users/departments are attacked the most?
5. Which hardware/software is attacked the most?

# Why I Quit the IT Security Arms Race

## David Brown

What are the right questions?

1. What attacks have occurred in the last 12 months?
2. Which were successful?
3. What was the cost/damage?
4. Which users/departments are attacked the most?
5. Which hardware/software is attacked the most?
6. What is the most likely successful attack for this year?

# Why I Quit the IT Security Arms Race

## David Brown

What are the right questions?

1. What attacks have occurred in the last 12 months?
2. Which were successful?
3. What was the cost/damage?
4. Which users/departments are attacked the most?
5. Which hardware/software is attacked the most?
6. What is the most likely successful attack for this year?
7. How would you detect it? What detection gaps do you have?



# Why I Quit the IT Security Arms Race

## David Brown

### What are the right questions?

1. What attacks have occurred in the last 12 months?
2. Which were successful?
3. What was the cost/damage?
4. Which users/departments are attacked the most?
5. Which hardware/software is attacked the most?
6. What is the most likely successful attack for this year?
7. How would you detect it? What detection gaps do you have?
8. What attacks are trending in our industry?

# Why I Quit the IT Security Arms Race

## David Brown

### What are the right questions?

1. What attacks have occurred in the last 12 months?
2. Which were successful?
3. What was the cost/damage?
4. Which users/departments are attacked the most?
5. Which hardware/software is attacked the most?
6. What is the most likely successful attack for this year?
7. How would you detect it? What detection gaps do you have?
8. What attacks are trending in our industry?
9. How well do the people in our organization understand our top risks?

Why I Quit the IT Security Arms Race  
David Brown

{Fear • Uncertainty • Doubt}

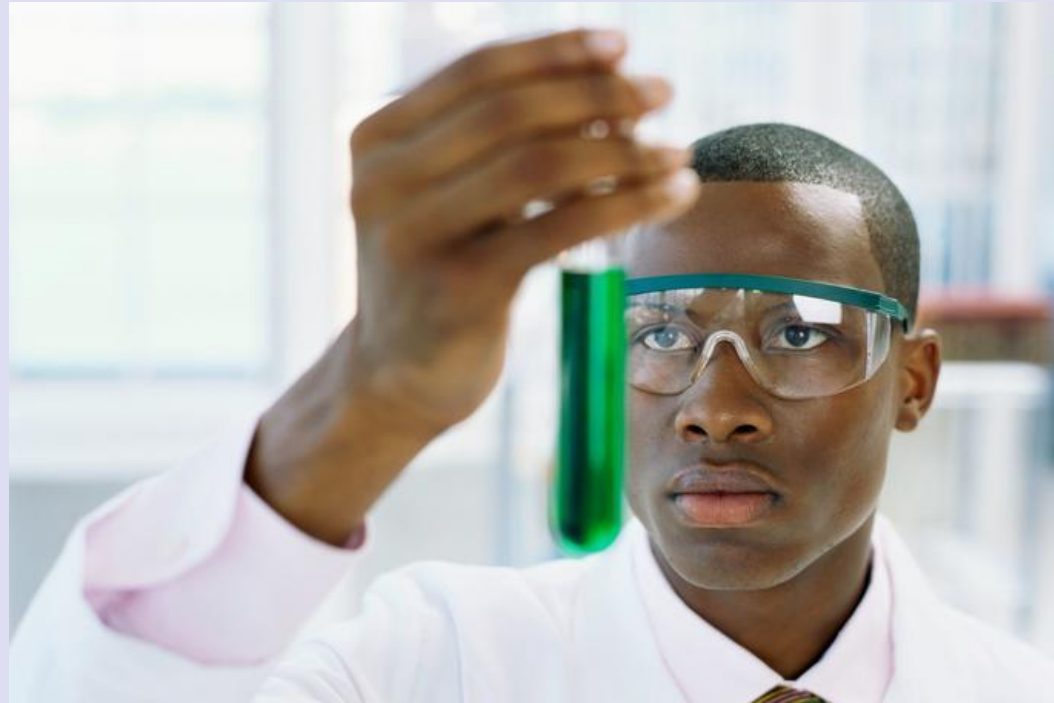


# Why I Quit the IT Security Arms Race

David Brown

Adam Grant  
Think Again

- Scientist



# Why I Quit the IT Security Arms Race

David Brown

Adam Grant  
Think Again

- Preacher





# Why I Quit the IT Security Arms Race

David Brown

Adam Grant  
Think Again

- Prosecutor

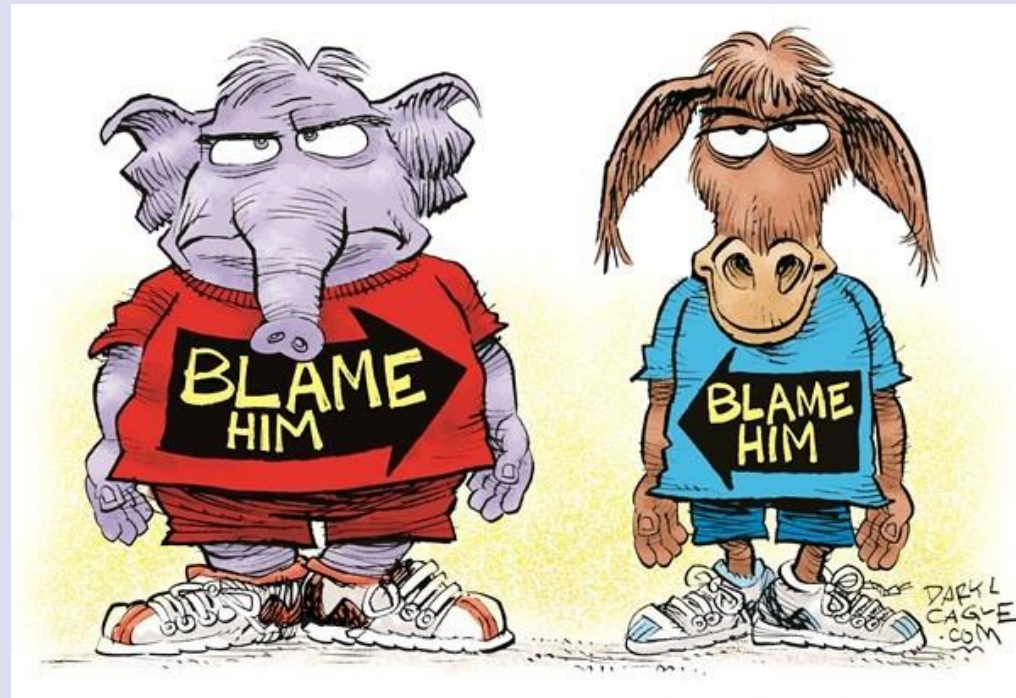


# Why I Quit the IT Security Arms Race

David Brown

Adam Grant  
Think Again

- Politician

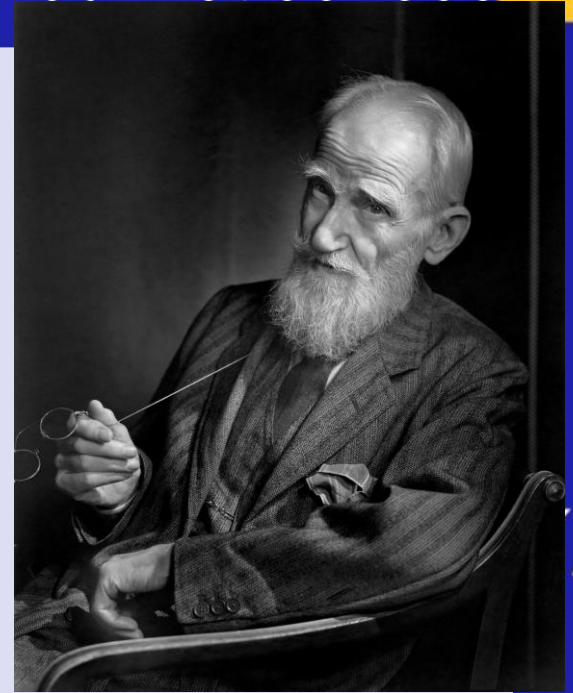


## Why I Quit the IT Security Arms Race

David Brown

George Bernard Shaw

“Progress is impossible without change; and those who cannot change their minds cannot change anything.”





# Why I Quit the IT Security Arms Race

David Brown

FAIR

Factor  
Analysis  
of  
Information  
Risk



# Why I Quit the IT Security Arms Race

David Brown

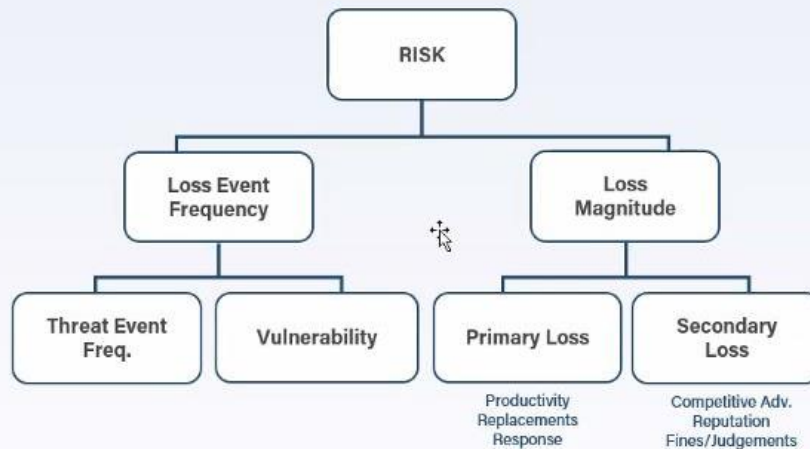
Deductive  
Logic:

Start with  
what you  
know



# Why I Quit the IT Security Arms Race

## David Brown



The **FAIR standard** enables risk to be quantitatively defined, measured, managed and communicated

Accredited as an Industry Standard by



Complementary to Risk Frameworks



NIST COSO

Supported by a Community of 10,000+



Wide Industry Adoption  
40% Fortune 1000



FAIR Book Inducted in Cybersecurity Canon



# Why I Quit the IT Security Arms Race

David Brown

## COMMUNICATING CYBER RISK IS CHALLENGING

### BOARD

"How much risk do we have?  
Are we spending too little or  
too much on cybersecurity?"

### AUDIT

"Have you fixed  
those high priority  
findings?"

### CEO

"How much risk is involved with  
our new digital and cloud  
initiatives?"

### CFO

"Are we spending our cybersecurity  
budget on the right things? What is  
the ROI?"

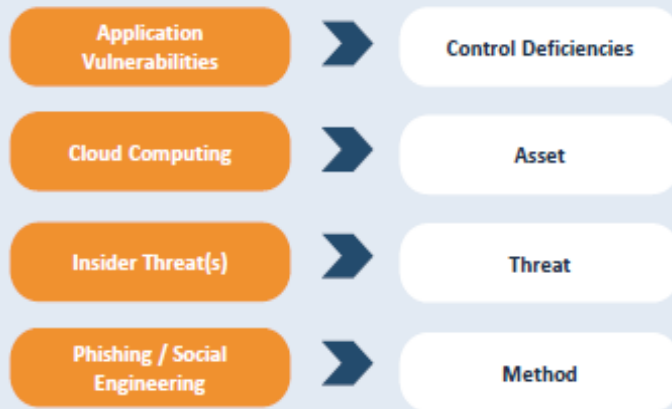
### CISO

"Έχουμε πάνω από  
δέκα χιλιάδες  
τρωτά σημεία,  
είναι συμβατό  
με το ογδόντα  
τοίς εκατό"

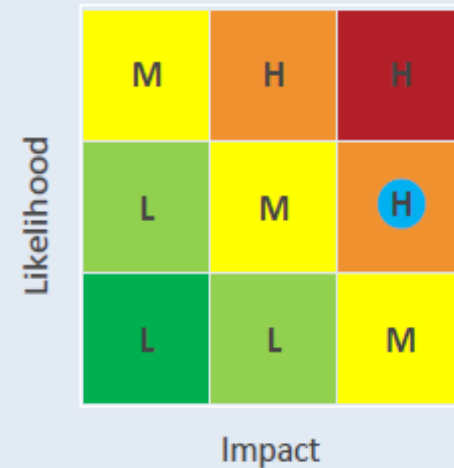
# Why I Quit the IT Security Arms Race

## David Brown

### INCONSISTENT DEFINITIONS



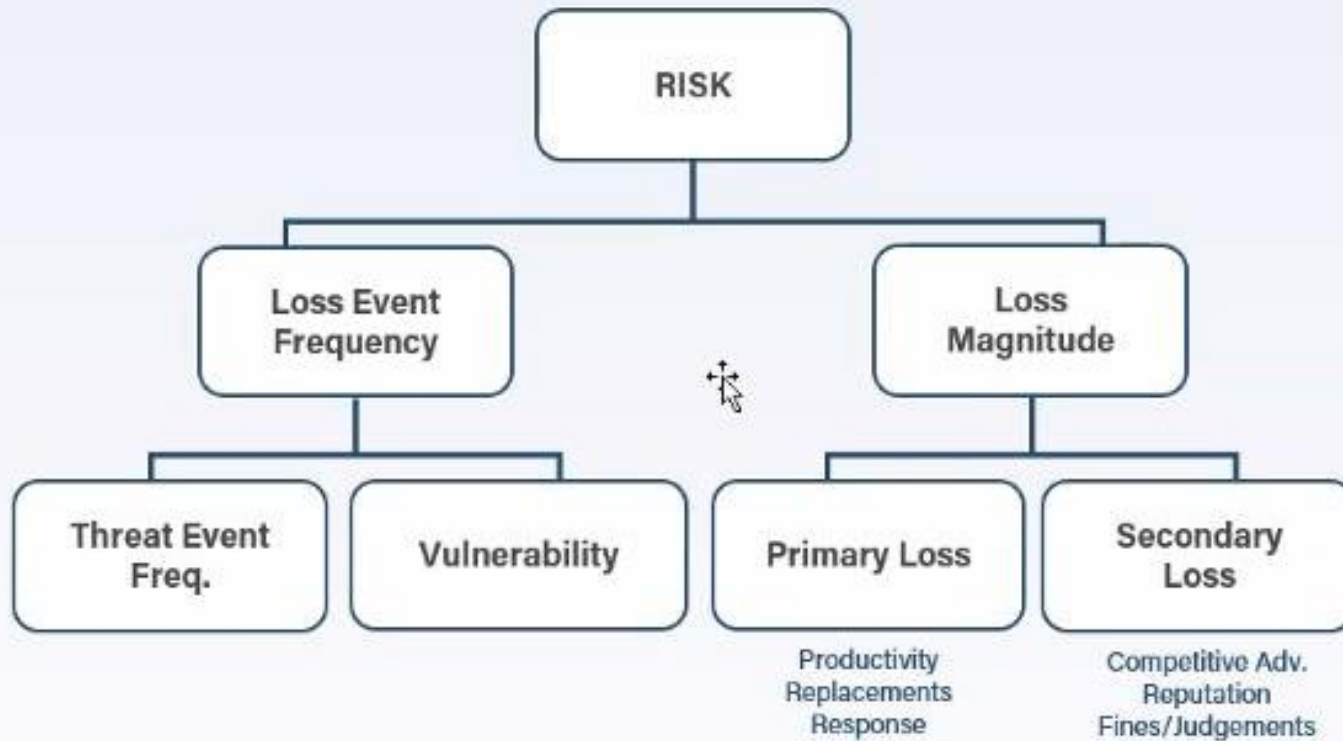
### MEANINGLESS MEASUREMENTS





# Why I Quit the IT Security Arms Race

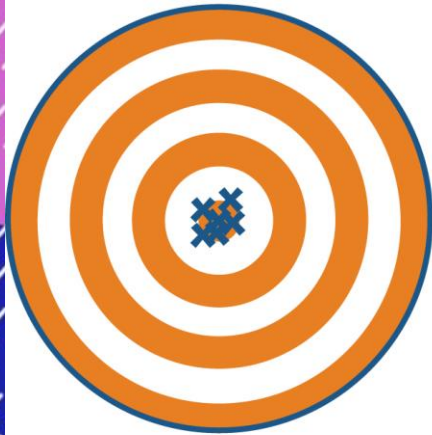
David Brown





# Why I Quit the IT Security Arms Race

David Brown



**High Accuracy  
High Precision**



**Low Accuracy  
High Precision**



**High Accuracy  
Low Precision**

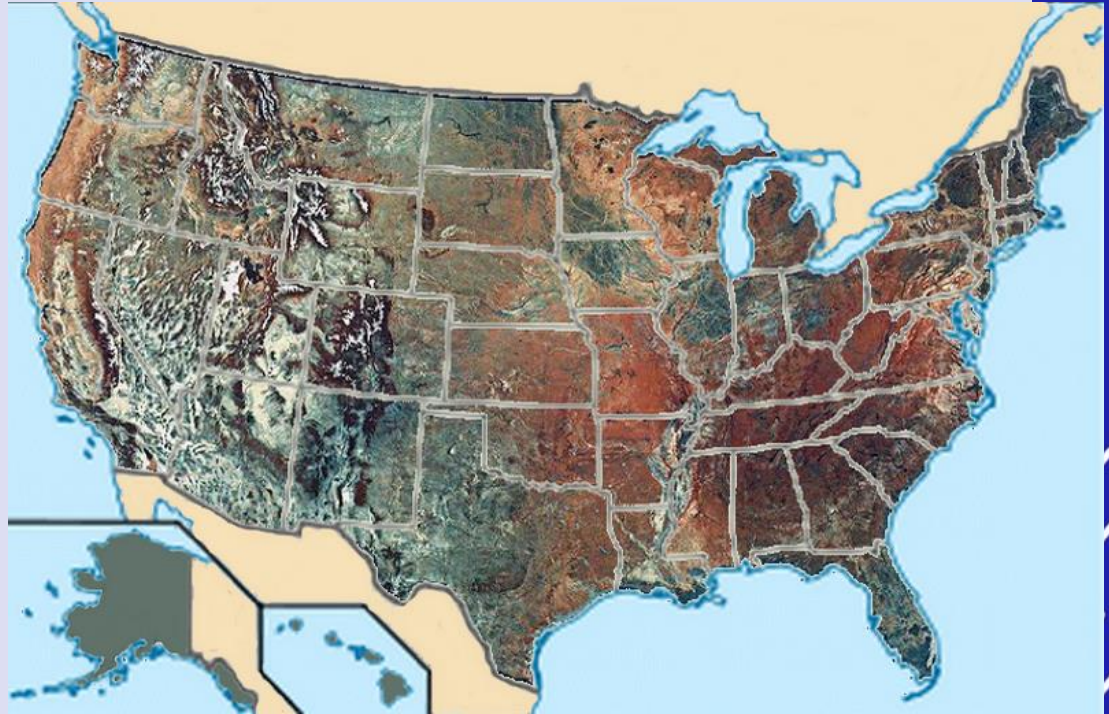


**Low Accuracy  
Low Precision**

# Why I Quit the IT Security Arms Race

David Brown

## US Shoreline





# Why I Quit the IT Security Arms Race

David Brown

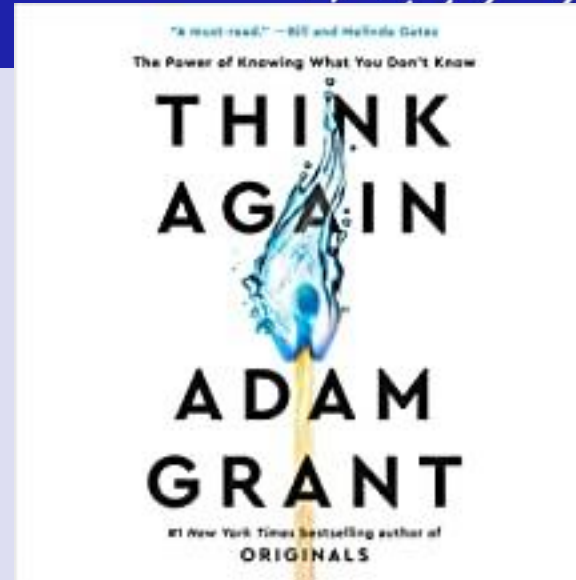
US Shoreline

12,000 Miles



## Why I Quit the IT Security Arms Race David Brown

Adam Grant  
Think Again



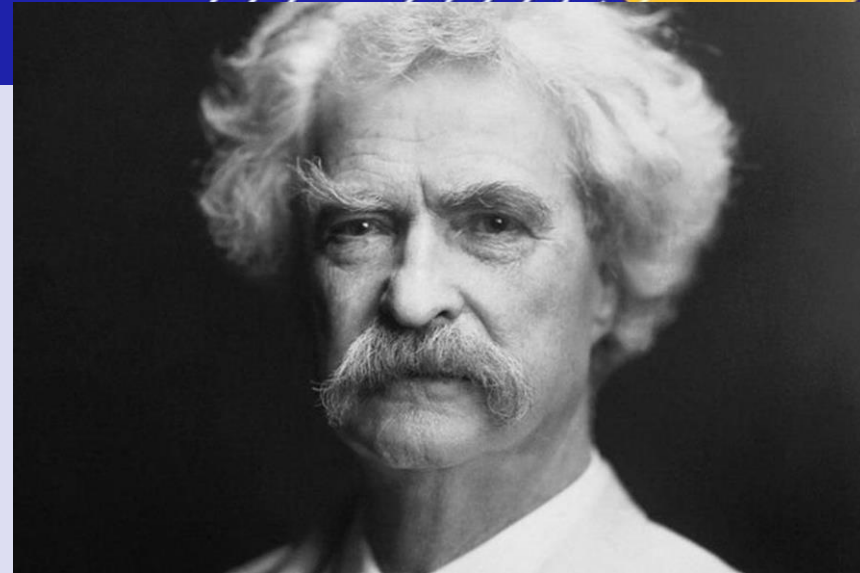
We underestimate our abilities when we think we don't know.

We overestimate our abilities when we think we do know.

# Why I Quit the IT Security Arms Race

David Brown

Mark Twain



“It’s not what you don’t know that will hurt you; it’s what you know that ain’t so”

# Why I Quit the IT Security Arms Race

David Brown





# Why I Quit the IT Security Arms Race

David Brown

Survey Question 3  
True or False

Go to:

[www.menti.com](https://www.menti.com)

Enter code  
6631 3842

# Why I Quit the IT Security Arms Race

David Brown

## Survey Answer #3

**FALSE!**

The way to play chess like a master is to be able to think about every possible move your opponent might make and then know how to counter them.

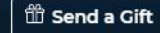
# Why I Quit the IT Security Arms Race

## David Brown



All ▾

Courses, Lectures, Professors



Start Free Trial



## How to Play Chess: Lessons from an International Master



JEREMY SILMAN, INTERNATIONAL CHESS MASTER

Whether you're a novice or a seasoned player, these 24 lessons on gameplay and strategies will boost your skills and turn you into a more formidable chess player.

★★★★★ 4.7 (292)



WATCH TRAILER



ADD COURSE TO WATCHLIST

START FREE TRIAL

# How to Play CHESS



LECTURES (24)

YOUR PROFESSOR

SHARE COURSE

REVIEWS (292)

## Great Courses now called "Wondrium"

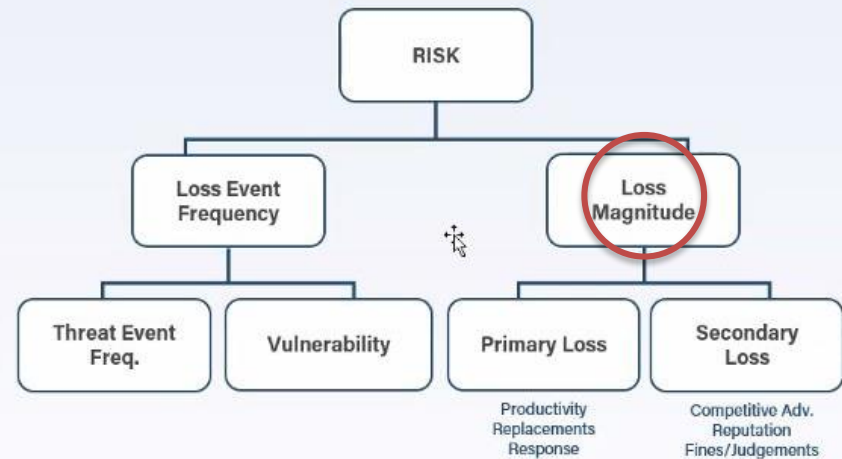


# Why I Quit the IT Security Arms Race

David Brown

Biggest value from  
FAIR:  
Loss Magnitude

What is REALLY at  
stake?



# Why I Quit the IT Security Arms Race

David Brown

## SPEAK THE LANGUAGE OF THE BUSINESS

**Communicate** cybersecurity risk in financial terms

**Provide** clear visibility into the top risks to the business

**Measure** the impacts of cyber risks and decisions on digital initiatives









# Why I Quit the IT Security Arms Race

David Brown

Biggest value from FAIR:  
Loss Magnitude

What is REALLY at stake?



## Why I Quit the IT Security Arms Race

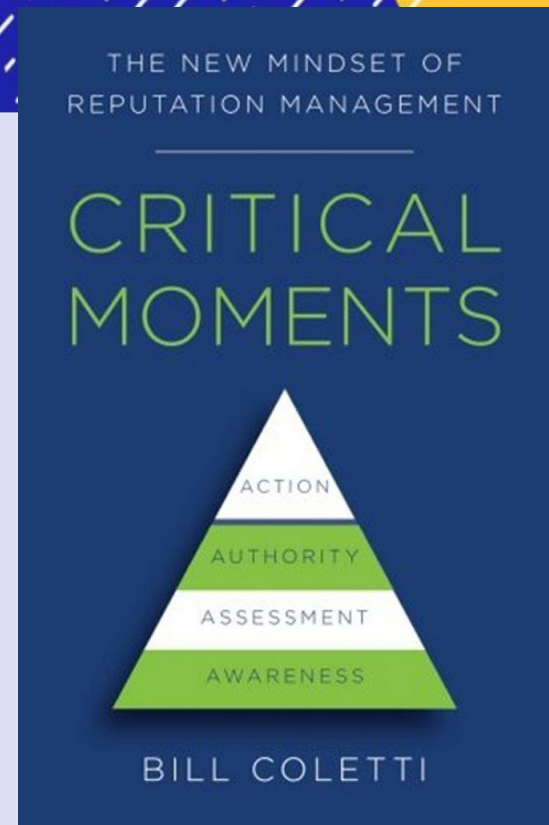
David Brown

### Critical Moments:

#### The new Mindset of Reputation Management

Bill Coletti

“The company goal in an external situation is to get back to doing what the business does best as quickly as possible, while simultaneously reminding customers that the company is simply part of the herd and not alone in facing this type of situation.”



# Why I Quit the IT Security Arms Race

David Brown

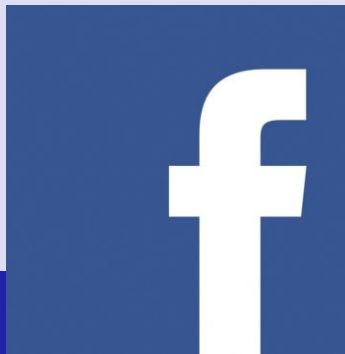
Big breaches:



**TARGET**



**EQUIFAX**



# Why I Quit the IT Security Arms Race

David Brown





# Why I Quit the IT Security Arms Race

David Brown

A little  
fun with  
FAIR ...





# Why I Quit the IT Security Arms Race

David Brown

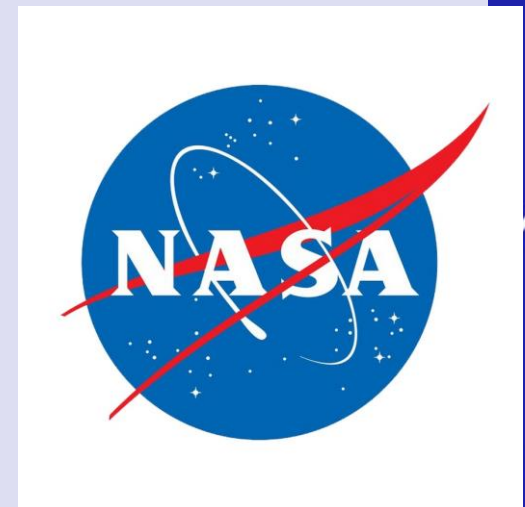
A little fun with FAIR.....

30% chance over 100 years = .3%

TEF = .3% a year

Hiroshima = 16 kilotons of TNT

8 Asteroids that hit earth from 2000-2013 were  $\geq$  16 kiloton



# Why I Quit the IT Security Arms Race

David Brown

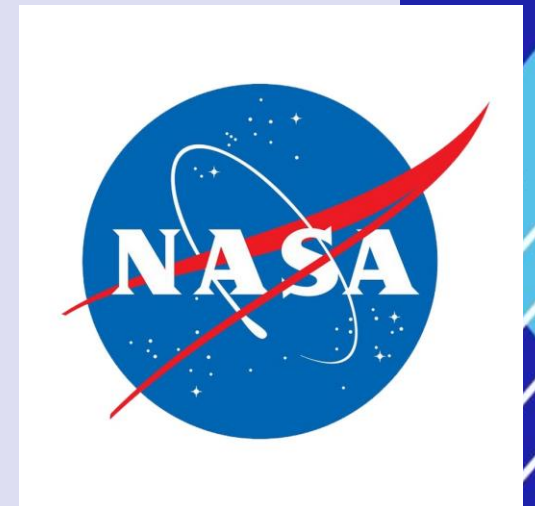
A little fun with FAIR.....

TEF = .3% a year

70% of earth is water – 30% inhabitable  
95% of population lives on 10% of land

10% of 30% is vulnerable

Vulnerability = 3%



# Why I Quit the IT Security Arms Race

David Brown

A little fun with FAIR.....

TEF = .3% a year

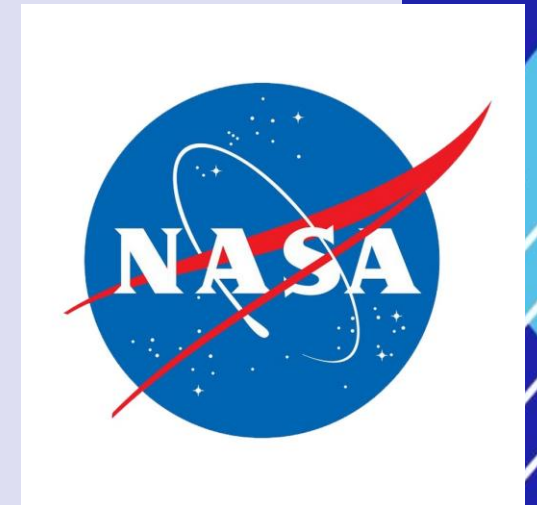
Vulnerability = 3%

$.3\% \times 3\% = .9\%$

LEF = .009 per year

90-140k people died at Hiroshima

Human life = \$10 Million



# Why I Quit the IT Security Arms Race

David Brown

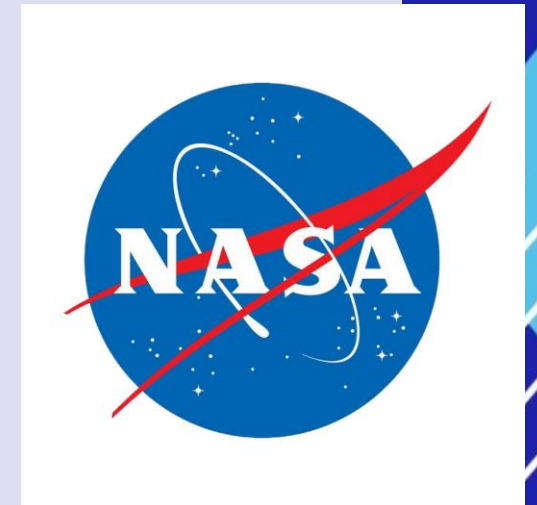
A little fun with FAIR.....

TEF = .3% a year

Vulnerability = 3%

LEF = .009 per year (.3% X 3%)

Loss Magnitude = \$1.4 quadrillion  
(140k X 10 Million)



# Why I Quit the IT Security Arms Race

David Brown

A little fun with FAIR.....

TEF = .3% a year

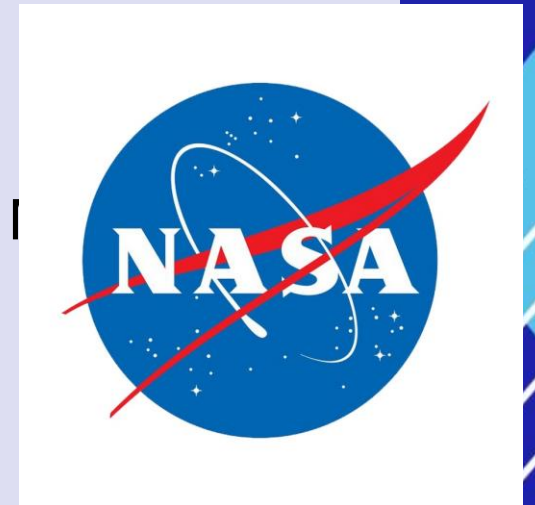
Vulnerability = 3%

LEF = .009 per year (.3% X 3%)

Loss Magnitude = \$1.4 quadrillion (140k X 10<sup>10</sup>)

**1.4Q (LM) X .009 (LEF) = 12.6B**

Risk = \$12.6 Billion a year





# Why I Quit the IT Security Arms Race

David Brown

A little fun with FAIR.....

TEF = .3% a year

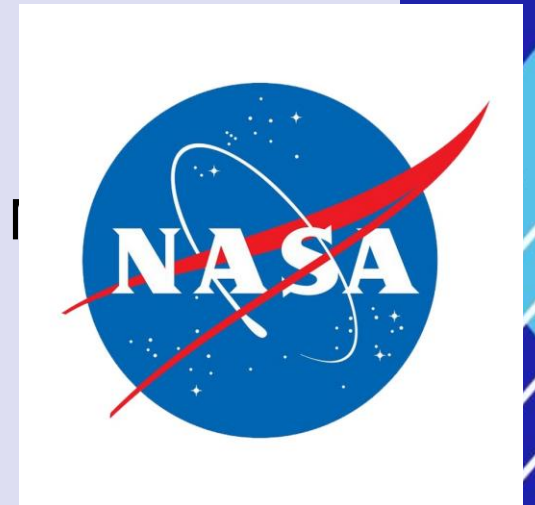
Vulnerability = 3%

LEF = .009 per year (.3% X 3%)

Loss Magnitude = \$1.4 quadrillion (140k X 10<sup>10</sup>)

Risk = \$12.6 Billion a year

NASA current budget is \$23.3 Billion



# Why I Quit the IT Security Arms Race

## David Brown

After completing this session, the participant will be able to ask the right questions to determine their greatest vulnerability

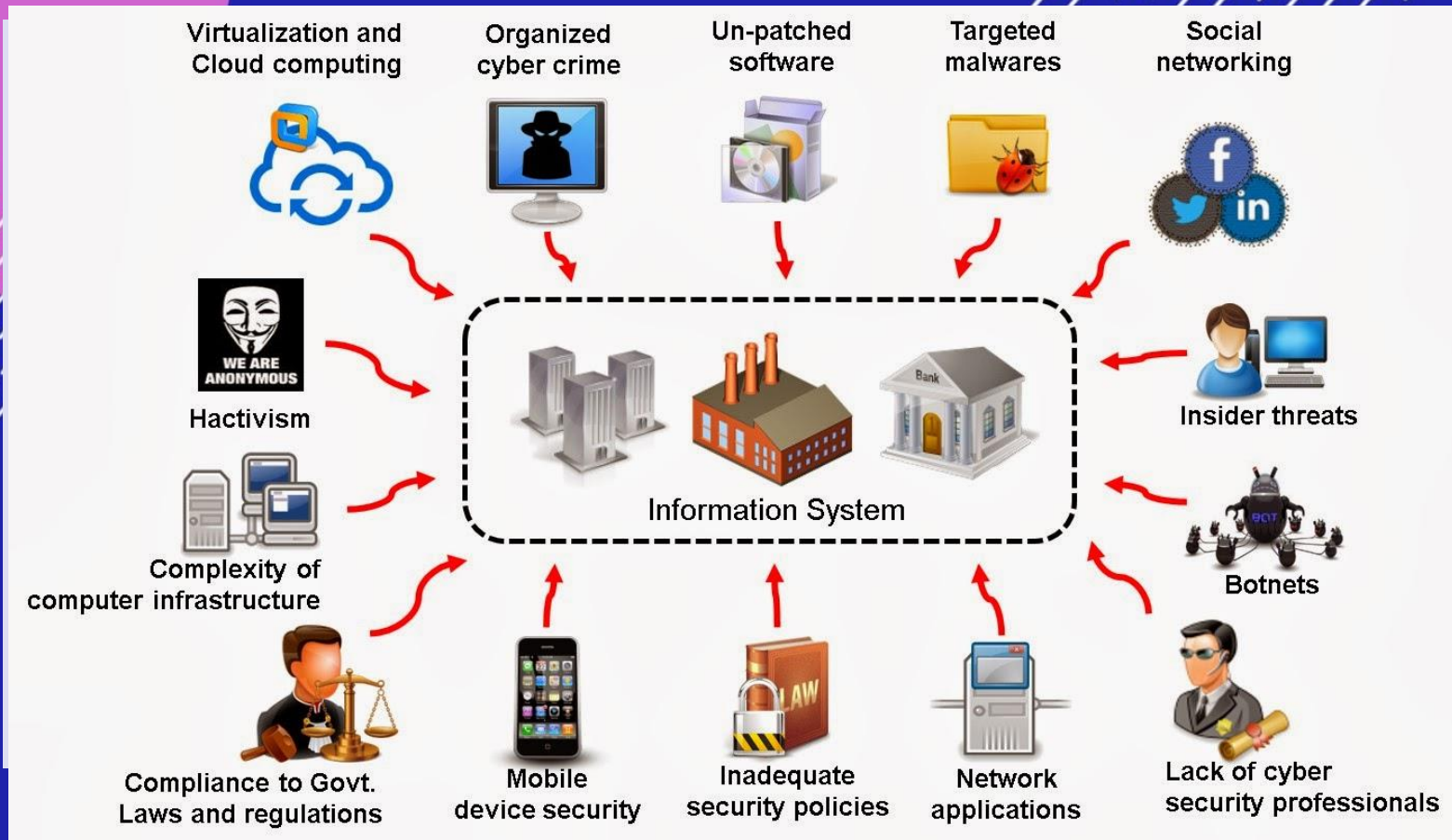
After completing this session, the participant will be able to put a monetary value on all identified vulnerabilities

After completing this session, the participant will be able to develop a strategy for mitigating their greatest vulnerabilities

After completing this session, the participant will be able to realign their budgets to meet strategic needs rather than industry trends

# Why I Quit the IT Security Arms Race

## David Brown





# Why I Quit the IT Security Arms Race

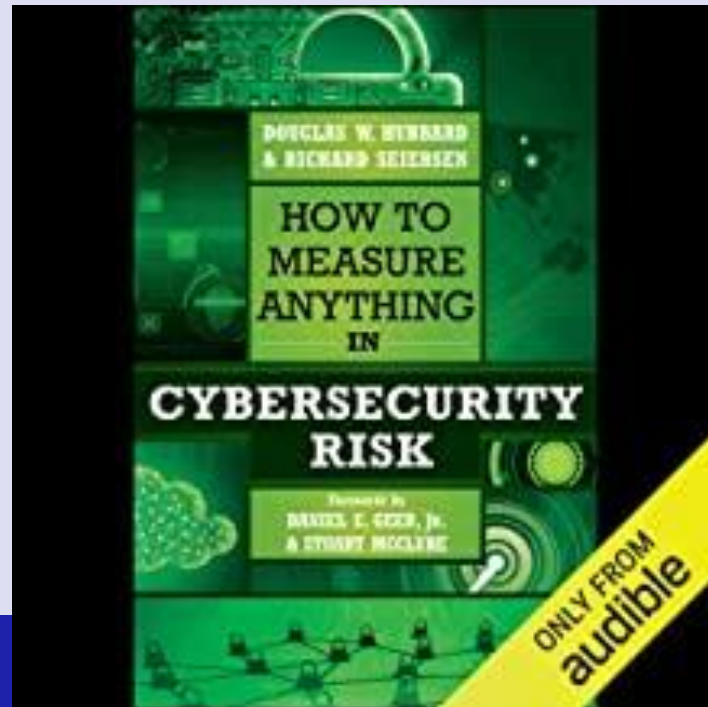
## David Brown



# Why I Quit the IT Security Arms Race

David Brown

- <http://www.howtomeasureanything.com/cybersecurity/>





# Why I Quit the IT Security Arms Race

David Brown

## Top three Areas of focus in 2022

1. Social Engineering
2. Patching
3. Business Impact Analysis (BIA)



# Why I Quit the IT Security Arms Race

David Brown

Survey Question 4  
Which is best?

Go to:

[www.menti.com](https://www.menti.com)

Enter code  
6631 3842

# Why I Quit the IT Security Arms Race

David Brown

The answer is to improve the **laggards**

# Why I Quit the IT Security Arms Race

## David Brown

The road is 24 miles long

### Scenario 1

10 mph on country road

1.20

50 mph on highway

0.24

Total time: 1.44 hours

### Scenario 2

22 mph on country road

0.55

50 mph on highway

0.24

Total time: 0.79 <---way better

### Scenario 3

10 mph on country road

1.20

200 mph on highway

0.06

Total time: 1.26 hours

# Why I Quit the IT Security Arms Race

David Brown







# Why I Quit the IT Security Arms Race

David Brown

Patching is not my job!

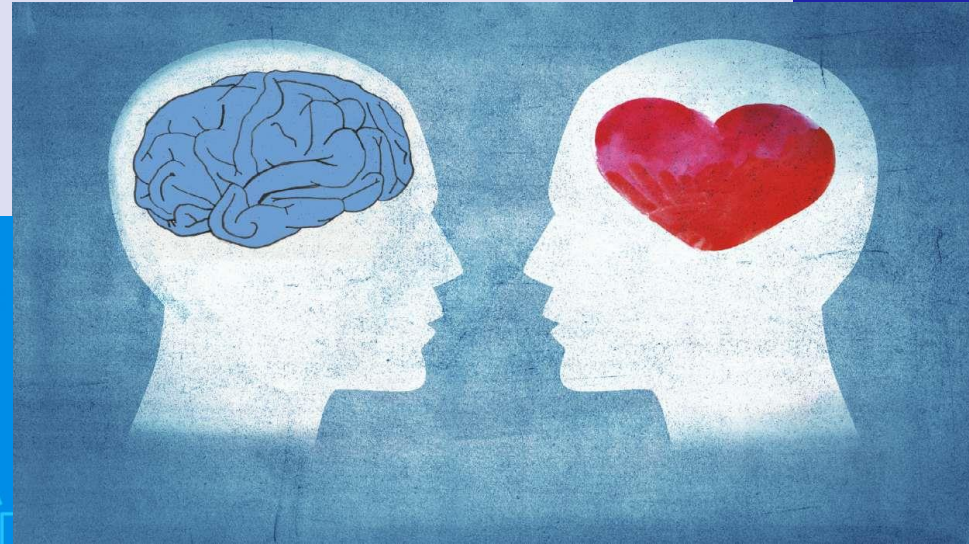
But influence is!

## Patch Management Software and Tools



# Why I Quit the IT Security Arms Race

David Brown



## Why I Quit the IT Security Arms Race

David Brown

There are more important things for my staff to do than look at log files!

AHEAD



# Why I Quit the IT Security Arms Race

## David Brown

After completing this session, the participant will be able to ask the right questions to determine their greatest vulnerability

After completing this session, the participant will be able to put a monetary value on all identified risks

After completing this session, the participant will be able to develop a strategy for mitigating their greatest vulnerabilities

After completing this session, the participant will be able to realign their budgets to meet strategic needs rather than industry trends





# Why I Quit the IT Security Arms Race

David Brown

George Washington University MFA

ISOAG

March 3, 2022



Why I Quit the IT Security Arms Race  
David Brown

Questions?

[www.menti.com](http://www.menti.com)

Code 6631 3842



# Why I Quit the IT Security Arms Race

David Brown

George Washington University MFA

ISOAG

March 2, 2022



March 2022 ISOAG  
Meeting : Data Security  
and  
Cybersecurity...Friends till  
the end



OFFICE OF DATA GOVERNANCE  
AND ANALYTICS

## WHO WE ARE

- ▶ Data engineers, data analytics specialists, business intelligence specialists, project managers, data architects, data curators, communications professionals
- ▶ We are where business strategy meets technical expertise
- ▶ Our culture embodies trust, respect, transparency, innovation, and a people-centered approach that leverages data intelligence over intuition for every decision
- ▶ The Office of Data Governance and Analytics was established July 1, 2021 through Senate Bill 1365



## WHAT WE DO

- ▶ Oversee data sharing among state, regional, local public entities & public institutions of higher education
- ▶ Implement data governance strategies
- ▶ Promote & increase access to Commonwealth data
- ▶ Develop innovative data analysis and intelligence methodologies to promote data-driven policy making, decision making, research, and analysis
- ▶ Manage the Commonwealth Data Trust
- ▶ Identify, coordinate, and oversee data analytics projects studies linking government services to stakeholder outcomes
- ▶ Manage the Open Data Portal ([data.virginia.gov](https://data.virginia.gov))
- ▶ Provide operational support to the Virginia Data Commission, Executive Data Board, Data Governance Council, Data Stewards Group



## WHO WE SERVE

- ▶ State agencies and other public entities
- ▶ Public institutions of higher education
- ▶ Non-profit organizations
- ▶ Constituents of Virginia

# What is Cybersecurity?

Cybersecurity refers to the body of technologies, processes, and practices designed to protect networks, devices, programs, and data from attack, damage, or unauthorized access. Cybersecurity may also be referred to as information technology security.

## Notable Cybersecurity Attacks in 2021

- ▶ SolarWinds
- ▶ Acer
- ▶ JBS Foods
- ▶ Kia Motors
- ▶ CNA Insurance
- ▶ Brenntag
- ▶ Colonial Pipeline
- ▶ National Basketball Association (NBA)
- ▶ Buffalo Public Schools
- ▶ Microsoft Exchange Server

# What is Data Security?

Data security is the practice of protecting digital information from unauthorized access, corruption, or theft throughout its entire lifecycle.

- Data encryption — Encoding the data so it requires a key to unlock and read.
- Data masking — Masking specified areas of data, so only authorized users can view it.
- Data erasure — Ensuring that obsolete data is completely removed.
- Data backup — Creating multiple copies of data for data recovery if the original is lost.

**The number of reported data breaches jumped 68 percent last year to the highest total ever.**

**According to the Identity Theft Resource Center's 2021 Data Breach Report, there were 1,862 data breaches last year, surpassing both 2020's total of 1,108 and the previous record of 1,506 set in 2017**



# Notable Data Breaches of 2021

- ▶ Cognnyte - 5 Billion
- ▶ LinkedIn — 700 million
- ▶ Facebook — 553 million
- ▶ Bykea — 400 million
- ▶ Brazilian Database — 223 million
- ▶ Socialarks — 214 million
- ▶ Android Users Data Leak — 100+ million

# Data Security vs. Cybersecurity

Data security focuses on the data itself. However, cybersecurity encompasses all forms of digital security including digital data and digital systems.



# Data Security and Cybersecurity Work Together

## Protecting from a Cybersecurity Attack

- Keeping Data Safe
- Password Protection protocols
- Update Security Software
- Employee Training
- Data Encryption
- Multi-Factor Authentication
- Malware Scanners
- VPN-capable firewall



“Data is not intelligence”

*~William Binney*

Sign up for the  
ODGA Newsletter at  
[odga.virginia.gov](http://odga.virginia.gov)

## BITS AND BYTES

All things data for the Commonwealth of Virginia







# THANK YOU!

Email: [odga@governor.virginia.gov](mailto:odga@governor.virginia.gov)

Web: [odga.virginia.gov](http://odga.virginia.gov)

**Social:**  [/virginia-office-of-data-governance-and-analytics](https://www.linkedin.com/company/virginia-office-of-data-governance-and-analytics)

 [@VirginiaODGA](https://twitter.com/VirginiaODGA)



# ISOAG MONTHLY MEETING

## MSI - ARS SELF SERVICE DEMO AND TRAINING

HERB SENING & KEITH HILLIARD

March 2022



## AGENDA

- I. Welcome & introductions
- II. Presenter Bio
- III. Demo of ARS/Training
- IV. Appendix
  - I. ARS Self Service Requests Performed by VCCC/AAO Team
  - II. ARS Self Service Demo Screen Shots
  - III. KB Article

Herb Sening

Chief Operations Management

VITA MSI Program

[Herb.e.sening@saic.com](mailto:Herb.e.sening@saic.com)

804-240-7381 ©

Responsibilities:

- Joint Operations Center (JOC),
- VCCC Service Desk
- Change Management
- Problem Management
- Security Incident Response Team for VITA.

Keith Hilliard

Manager Account Administration

Operations

VITA MSI Program

[hilliardk@naismc.saic.com](mailto:hilliardk@naismc.saic.com)

423-914-3475 ©

Responsibilities:

- Account Administration Operations  
(Requests related to access,  
onboarding, security, etc.)



# ARS SELF SERVICE DEMO AND TRAINING

SCREEN SHARE OF ARS

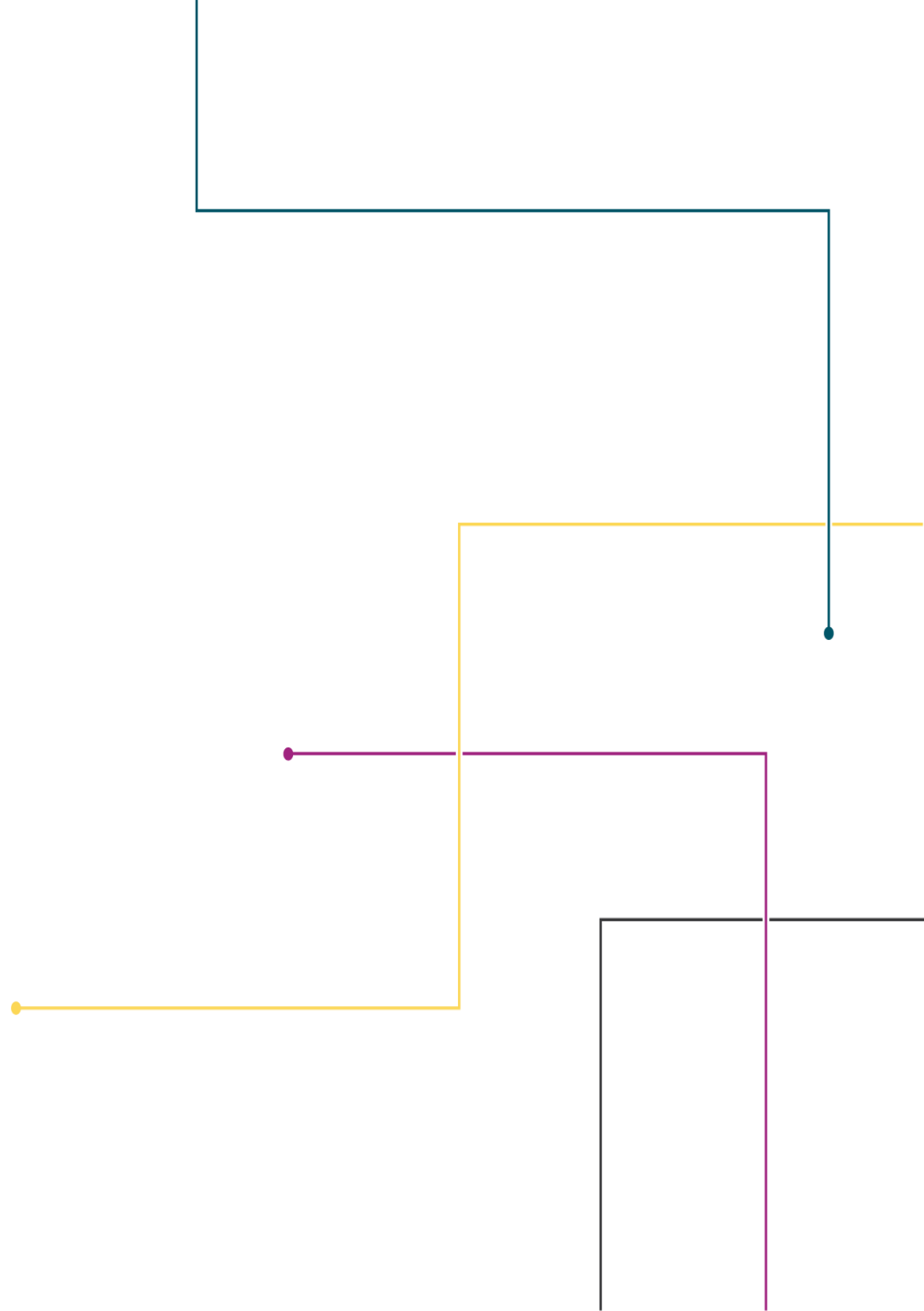
[HTTPS://ARS.VITA.VIRGINIA.GOV/ARS/](https://ars.vita.virginia.gov/ars/)

<https://ars.vita.virginia.gov/ars/>










# APPENDIX


## ARS SELF SERVICE DEMO SCREEN SHOTS





-  A136-AC-HHR-EDM-PROD-DMV-R
-  A136-AC-HHR-EDM-PROD-DMV-RW
-  A136-AC-HHR-EDM-PROD-ENTERPRISE
-  A136-AC-HHR-EDM-PROD-SEC-VSCAN
-  A136-AC-HHR-EDM-STAGE-ADMIN
-  A136-AC-HHR-EDM-STAGE-CMS-R
-  A136-AC-HHR-EDM-STAGE-CMS-RW

-  A136-DL-CSA-TAX
-  A136-DL-CSA-TRS
-  A136-DL-CSA-VCA
-  A136-DL-CSA-VDA
-  A136-DL-CSA-VDACS
-  A136-DL-CSA-VDBA
-  A136-DL-CSA-VDEM
-  A136-DL-CSA-VEC
-  A136-DL-CSA-VITA
-  A136-DL-CSA-VMFA

 A136-AC-HHR-EDM-PROD-DMV-RW

Move

Copy

Rename

Members

Member Of

Change History

---

General Properties

---

Deprovision

---

Delete

---





A136-AC-HHR-EDM-PROD-DMV-RW



Manager:

Change...

Properties

Clear

Manager can update membership list



Secondary owners:

Name	In Folder

Add...

Remove

Properties

Secondary owners can update membership list

## A136-DL-CSA-TRS (objects found: 7)

[Active Directory](#) / [cov.virginia.gov](#) / [COV-Groups](#) / [Distribution Lists](#) / [VITA](#)










Members (7, including pending members)

 Add...

 Remove

Temporary Access...

<input type="checkbox"/>	Name	Type
<input type="checkbox"/>	 A136-DL-Customer Account Managers (VITA)	Group
<input type="checkbox"/>	 Amberman Timothy zkp27798 (Timothy.Amberman@trs.virginia...)	User
<input type="checkbox"/>	 Andrews Lee yrm78594 (Lee.Andrews@trs.virginia.gov)	User
<input type="checkbox"/>	 Edwards Deborah saj29937 (Deborah.Edwards@trs.virginia.gov)	User
<input type="checkbox"/>	 Kissel John xir34163 (John.Kissel@vita.virginia.gov)	User
<input type="checkbox"/>	 Krafcik Rich hvp42785 (Rich.Krafcik@trs.virginia.gov)	User
<input type="checkbox"/>	 McRae Daniel xsa33749 (Daniel.McRae@itsupplier.virginia.gov)	User

**Select Object** ✕

Search in: cov.virginia.gov 🔍

<input type="checkbox"/> Name	Type	Description

Temporary Access...



## A136-DL-CSA-TRS (objects found: 7)

[Active Directory](#) / [cov.virginia.gov](#) / [COV-Groups](#) / [Distribution Lists](#) / [VITA](#)










Filter

Members (7, including pending members)

 Add...

 Remove

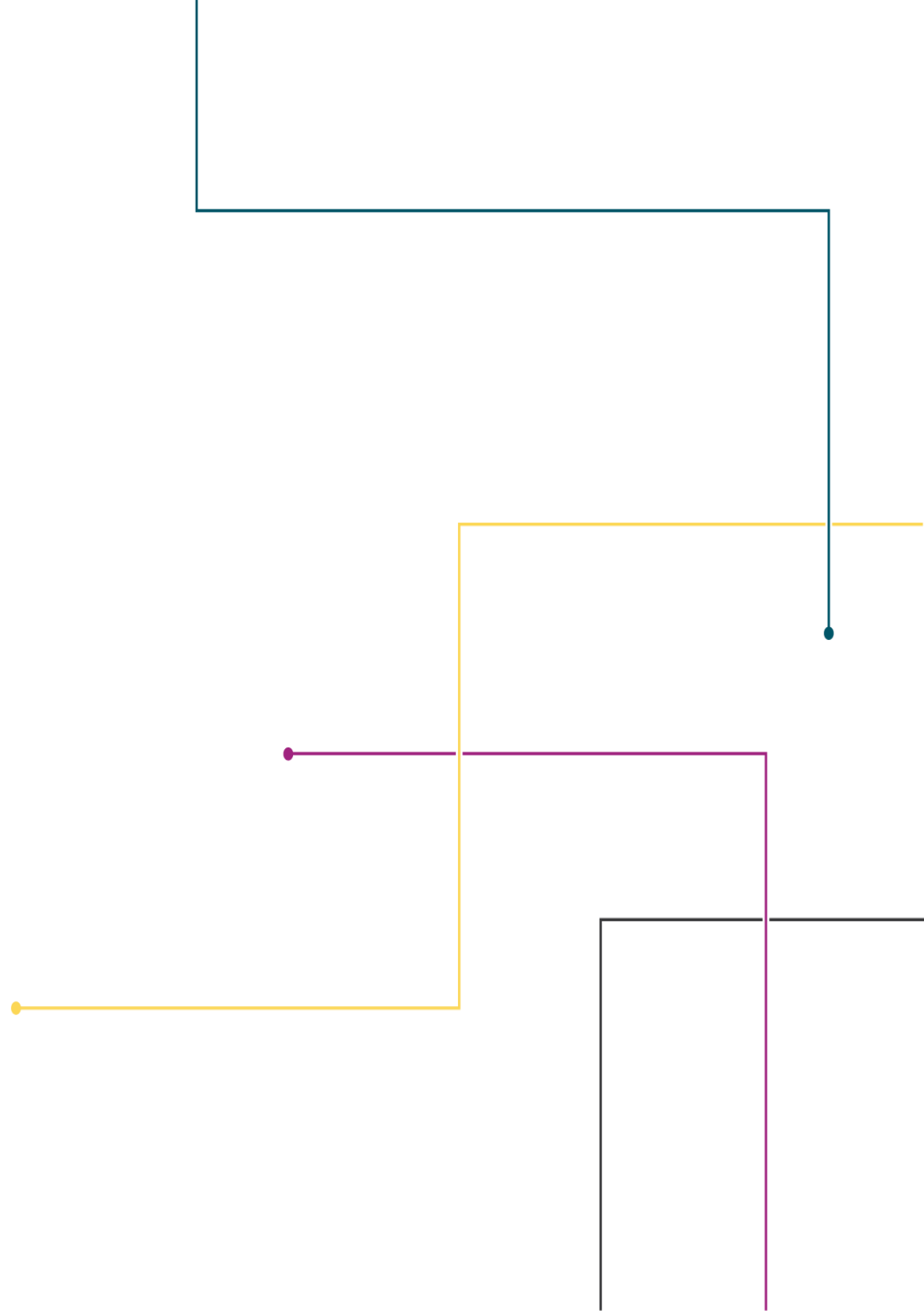
Temporary Access...

<input type="checkbox"/>	Name	Type
<input type="checkbox"/>	 A136-DL-Customer Account Managers (VITA)	Group
<input checked="" type="checkbox"/>	 Amberman Timothy zkp27798 (Timothy.Amberman@trs.virginia...)	User
<input type="checkbox"/>	 Andrews Lee yrm78594 (Lee.Andrews@trs.virginia.gov)	User
<input type="checkbox"/>	 Edwards Deborah saj29937 (Deborah.Edwards@trs.virginia.gov)	User
<input type="checkbox"/>	 Kissel John xir34163 (John.Kissel@vita.virginia.gov)	User
<input type="checkbox"/>	 Krafcik Rich hvp42785 (Rich.Krafcik@trs.virginia.gov)	User
<input type="checkbox"/>	 McRae Daniel xsa33749 (Daniel.McRae@itsupplier.virginia.gov)	User



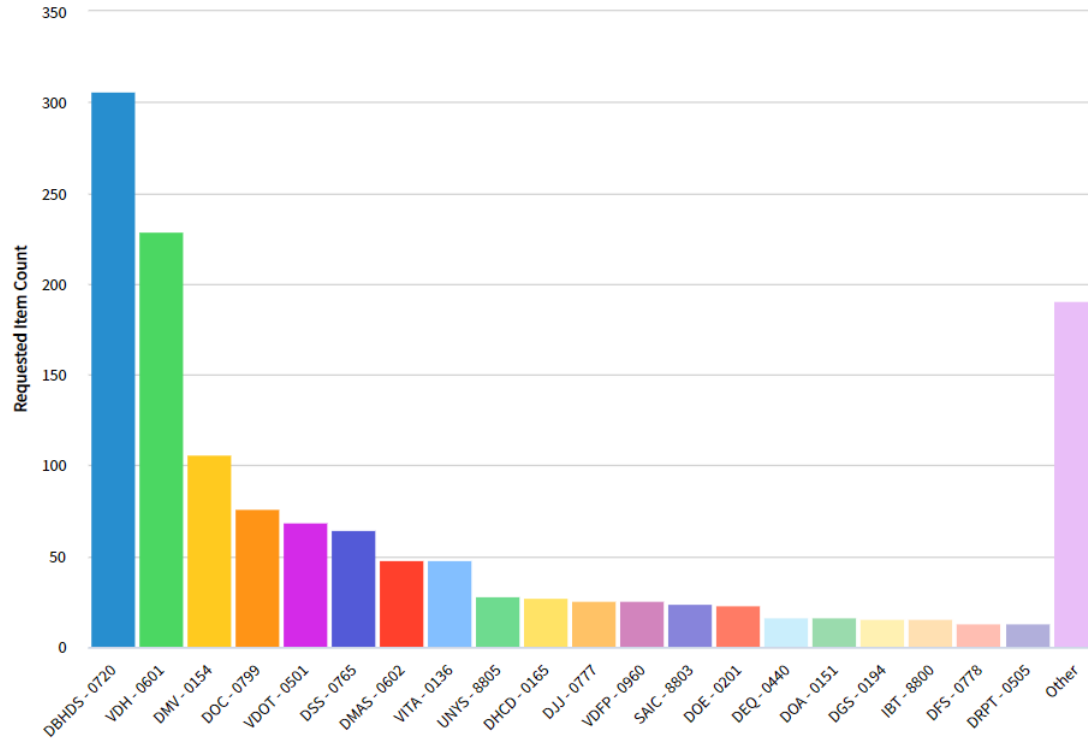
# APPENDIX

ARS SELF SERVICE REQUESTS  
PERFORMED BY VCCC/AAO TEAM



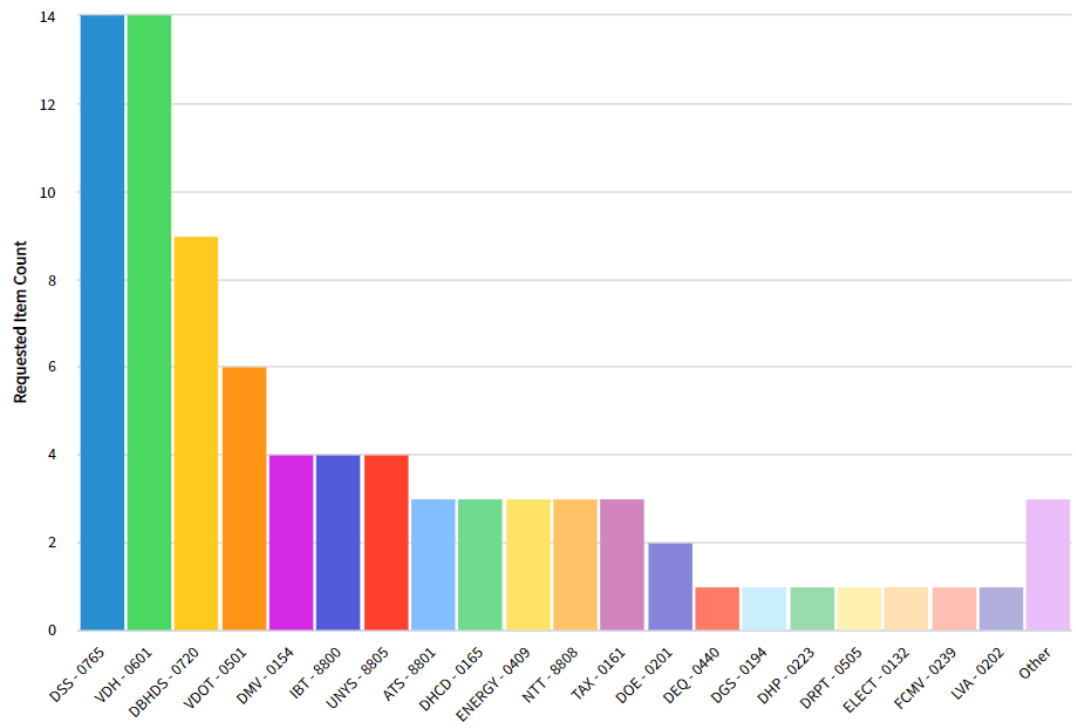


COV Security Group Modify - By Agency (Last 3 Months)



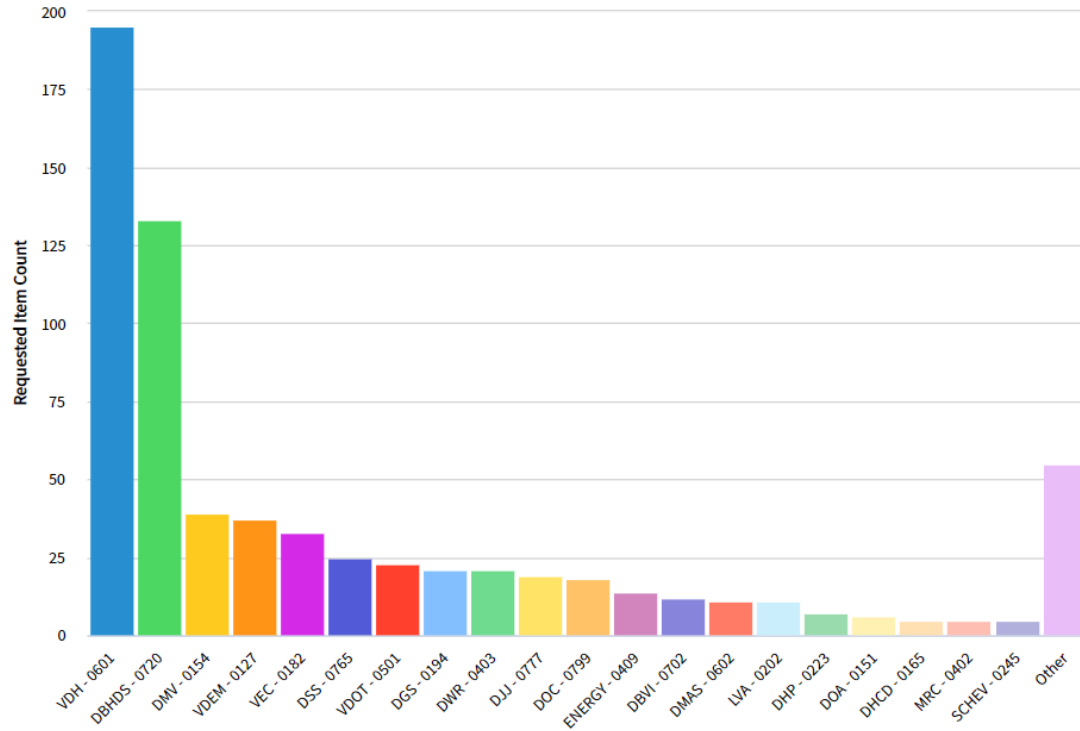


COV Security Group Modify - By Agency (Current)





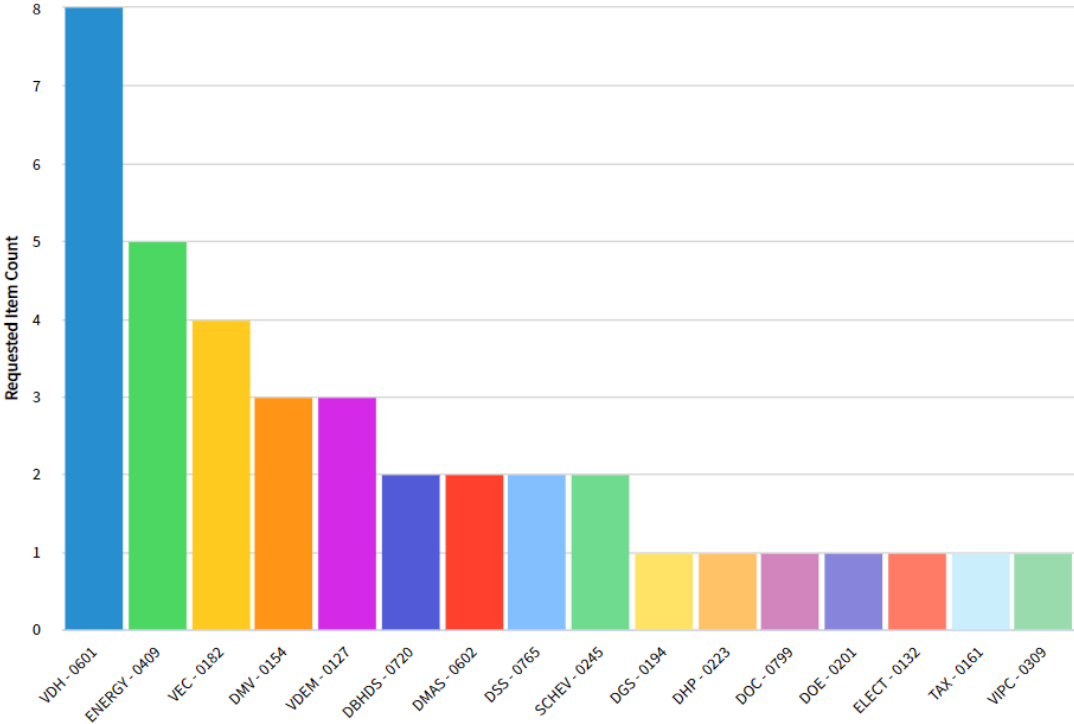
Google Group Request Modify - By Agency (Last 3 Months)







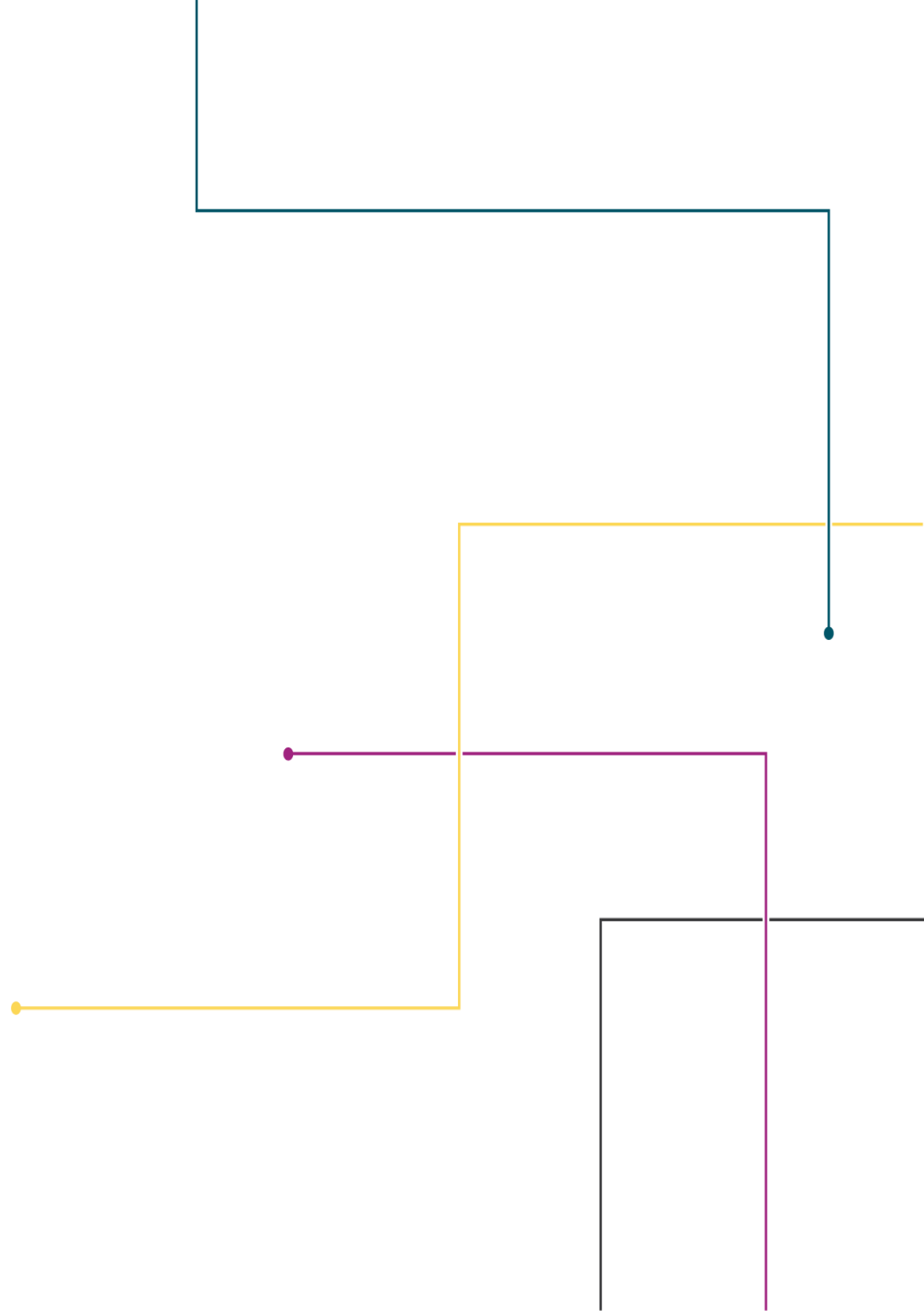
Google Group Request Modify - By Agency (Current)





# APPENDIX

ARS SELF SERVICE KB ARTICLE



## ARS SELF SERVICE KB ARTICLE - KB0018627

How to search ARS and modify Security Groups and Distribution Lists

This article provides instructions on how to search for and modify security groups and distributions lists in ARS.

### Add Users

1. Log into ARS with your COV Account. You must be on the COV network to get to ARS. ARS address: <https://ars.vita.virginia.gov/ARS/>
2. Use the magnifying glass on the left hand side or the search field in the top right of page
3. Search for the security group by name (ex. A100-AC-Server-Folder Access RW) or the Distribution List by email address (ex. test\_users@test.com) or Group Name (ex. A100-DL-Test Users)
4. Select the check box to the left of the security group and a menu will appear on the right hand side. Select Members.
5. In the new screen you can now click the +Add... button and search for the users you wish to add.
  - You can search for users by Email address, Alias, and Last, First.
  - If you wish to search for multiple users, you can separate the users with a semicolon.
6. Select each user you want added and then click the Ok button.
7. The users are now added to the group and show in the Members window.

### Remove Users

1. Log into ARS with your COV Account. You must be on the COV network to get to ARS. ARS address: <https://ars.vita.virginia.gov/ARS/>
2. Use the magnifying glass on the left hand side or the search field in the top right of page
3. Search for the security group by name (ex. A100-AC-Server-Folder Access RW) or the Distribution List by email address (ex. test\_users@test.com) or Group Name (ex. A100-DL-Test Users)
4. Select the check box to the left of the security group and a menu will appear on the right hand side. Select Members.
5. Once in the members sections, select the box next to the user you want removed and select the Remove button above.
6. Click Yes.

# Questions

???

# MDR Dashboard

Darrell Raymond & Eric Tompkins/ATOS



**VITA's managed security services provider, ATOS, is replacing McAfee security incident and event management (SIEM) with the Alsaac managed detection and response (MDR) platform by end of March '22. The new MDR platform is fully integrated with the CrowdStrike Falcon platform.**

**Security logs from servers, firewalls and network gear are being forwarded to the Alsaac platform. These activities are being done in the background and do not impact the functioning of the agency or service delivered by the supplier.**

**In addition, a MDR platform dashboard will be available to each agency. The dashboard will provide agencies with a self-service portal that allows agencies to see an abstract view of the security information, particularly security events, pertaining to them.**

## **Rollout schedule**

**The Alsaac MDR platform is live and is being validated by the Commonwealth security and risk management (CSRM) team. It will be available for agencies in the week of March 28.**

**Details needed for access requests and training will be forthcoming in the week of March 14.**

**If you have any questions, please contact your business relationship manager (BRM).**

# Upcoming events



THE COMMONWEALTH OF VIRGINIA SECURITY CONFERENCE WILL BE HELD ON  
AUG. 18, 2022, VIRTUALLY.

MORE DETAILS WILL BE FORTHCOMING.



**April 6, 2022, from 1 to 4 p.m.**

**Presenters:**

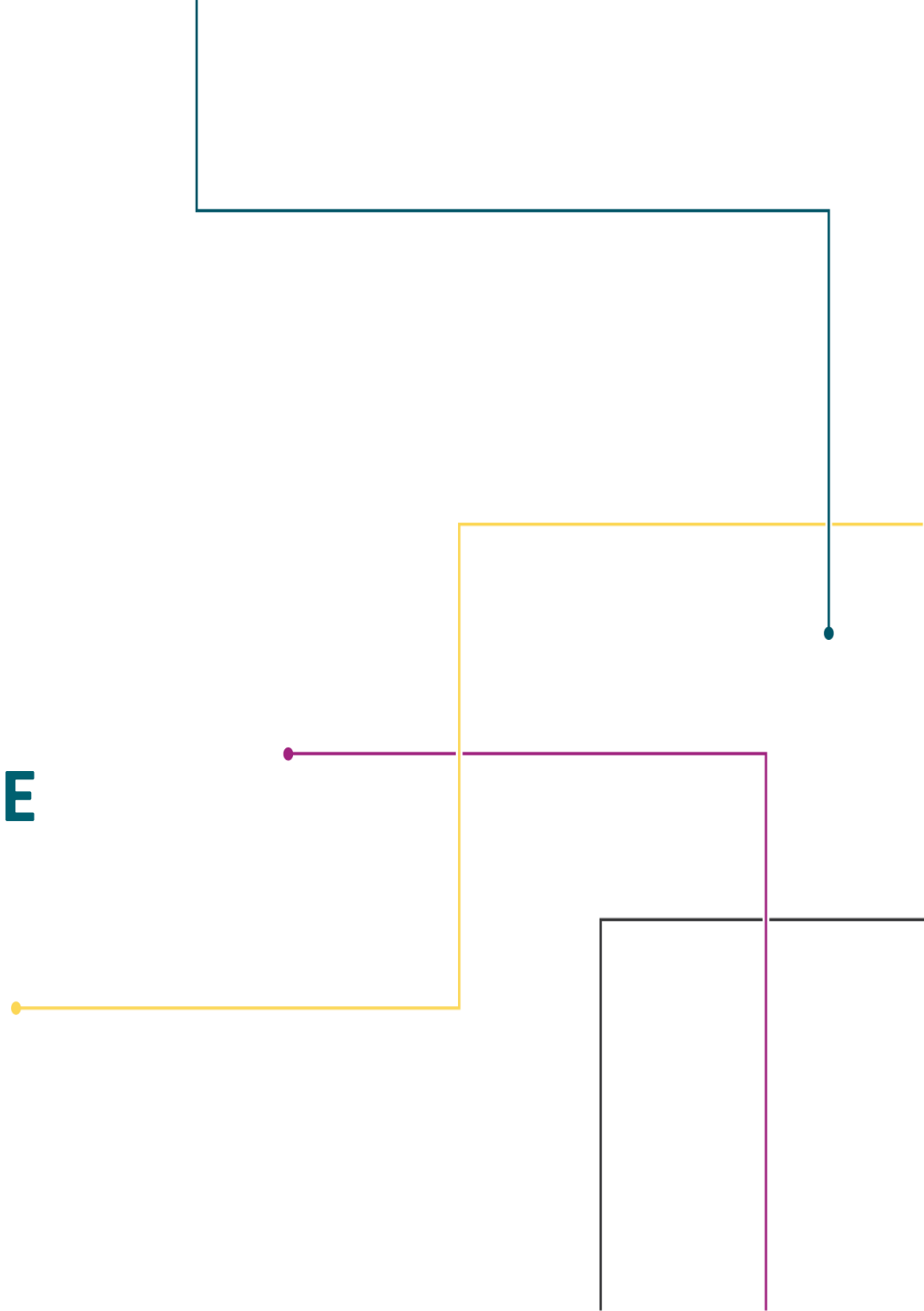
**John Singleton/VSP**

**Arlyn Elise /Virginia Edu**

**Melissa Goldate, Jon Ford & Steve Elovitz/Manidant**



**IS ORIENTATION  
MARCH 30, 2022  
1:00 PM  
HOSTED BY MARLON COLE**







**THANK YOU FOR  
ATTENDING!**

