NetSPI

Budget-Friendly, Battle-Ready: Cybersecurity for the Everyday Business

Presented by Robert Wagner, Managing Director, NetSPI

11.13.24

Introduction

Robert Wagner

- @ Mr_Minion
- @ Mr_Minion@infosec.exchange
- https://www.linkedin.com/in/robertwagner2/

Advisory CISO / Managing Director

Community:

- Hak4Kidz Co-Founder
- ISSA Chicago Board
- Chicago CISO of the Year
- BurbSec
- BSides312

Feel Free To:

- Take pictures
- Post to social

The Most Trusted Products, Services, and Brands Choose NetSPI

Hewlett Packard Enterprise

Microsoft

CHUBB

GONG

Broadridge

IHG HOTELS & RESORTS

20% of the Fortune 500

9/10 Top U.S. Banks

3/5 Largest Global Healthcare Companies

3/3 Largest Cloud Providers

> ***“NetSPI is exemplary at penetration testing, dynamic application security testing, and breach and attack simulation...”***
>
> Craig Guiliano, Cyber Intelligence Officer, Chubb

Trusted Pentesting

21K engagements*

NetSPI U

20+ years of testing

Security Expertise

4M assets tested*

1.5M vulnerabilities reported*

CREST PEN TEST STAR STAR-FS

CBEST

OFFENSIVE SECURITY OSCE

OFFENSIVE SECURITY OSCP

CISSP

Red Team Ops 1

Recognized by:

Gartner

FORRESTER

GIGAOM

*cumulative as of 2023

I Wrote This Talk Because...

- Many organizations need inexpensive or free solutions that can be implemented now
- Too often perfect is the enemy of good

Progress

~~Perfection~~

Cybersecurity Poverty Line

“The line below which an organization cannot be effectively protected – much less comply with – security regulations.”

Wendy Nather, 2010

Primary Hurdles

Money

Expertise

Capability

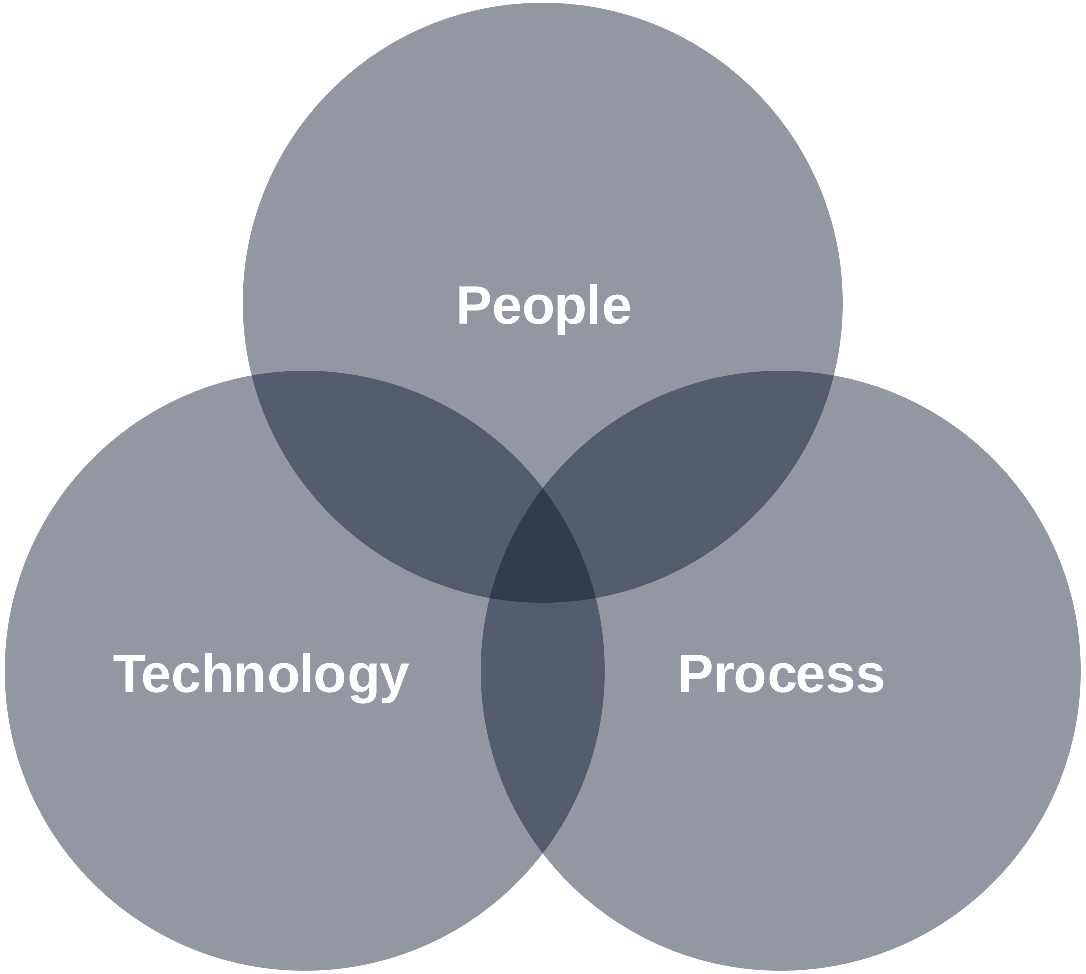
Influence

“There is a better way for everything.

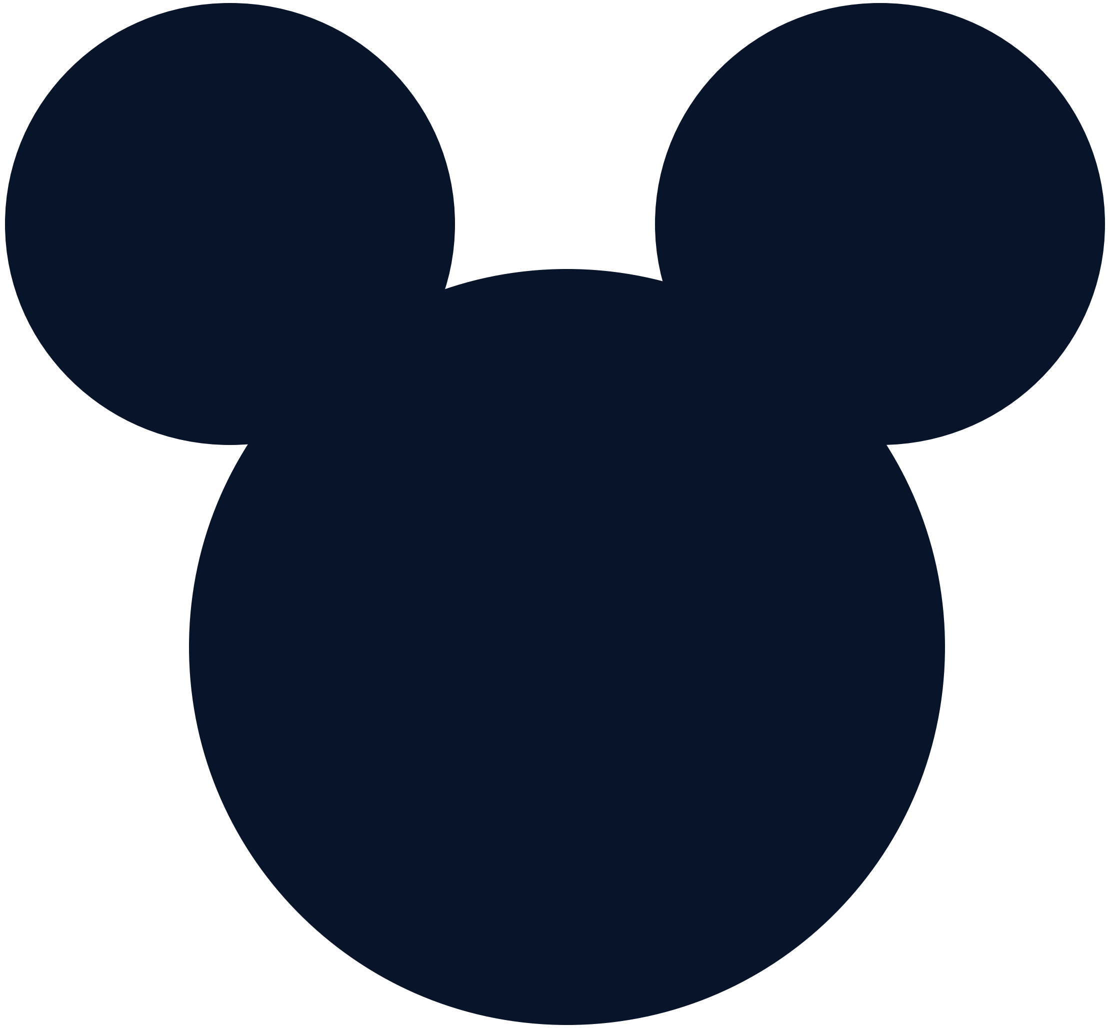
Find it.”

Thomas A. Edison

Where Do We Start?



Too Much Focus on Technology



People

Surface Attack Prevention
98%
Vulnerabilities Detected
System Normal
Attack Detected
Attack Blocked
Scan In Progress
All Systems

Talent is hard to find.

Is it really, though?

Consider non-traditional approaches to hiring.

Stop Chasing Unicorns

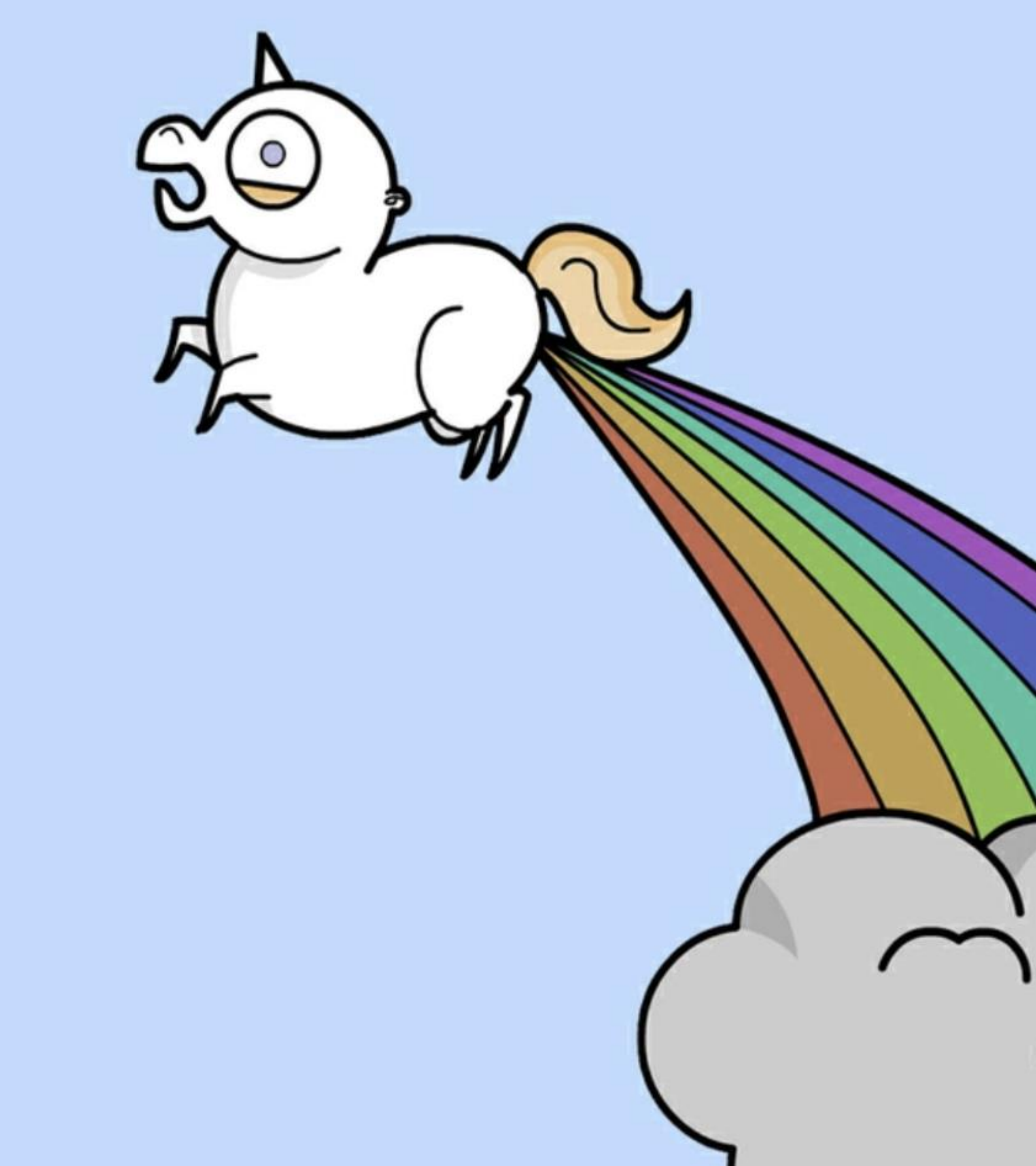
Hire Strategic Leads

- Target of empathy & mentorship
- Run interference for “Business Politics”
- Lead by example

Create a Low-Cost Army

- Interns
- Temp-to-hire
- Entry-level hires

Nurture Talent



How to Nurture Talent – From Within and Without

- Create a culture of mutual mentorship and sharing
- Train them so well that they could leave -- Treat them so well that they stay
- Help justify their training to the business
  - New hires usually don’t know the right language
- Encourage participation in the InfoSec community
- Look for talent in existing employees

Better Job Descriptions = More Candidates

Use Neutral Language

- E.g. "Energetic" can deter older candidates.

New AI for Better Job Descriptions

- Checks your job descriptions for optimal language

Get Rid of “Nice-to-Haves" in Job Descriptions

- Men apply at meeting 60% of the requirements. Women apply if they meet 100%.

Free Security Training to Level Up The Talent You Have

- CISA Cyber Essentials Toolkit
  - Bite-sized actions for IT and C-suite leadership to work toward full implementation of each Cyber Essential.
- Cyber Readiness Institute
  - The Cyber Readiness Program guides small and medium-sized enterprises to become cyber ready.
- SANS Cyber Aces
  - Online course that teaches the core concepts needed to assess and protect information security systems.
- Security BSides & Other Conferences
  - Many offer free (or cheap) training.

Employee Security Awareness Training

- 45% of employees receive NO security training at all from their employer.
- 62% of companies do not provide enough security awareness training to receive ANY benefits.

Free Awareness Training Resources

Because everyone loves awareness training

Amazon Security Awareness Training

https://learnsecurity.amazon.com/en/index.html

Google Course

https://skillshop.exceedlms.com/student/collection/644416-improve-online-security?locale=en-GB

EdApp (Mobile Based)

https://training.safetyculture.com/top-10-cyber-security-training-for-employees/

Backdoors & Breaches – Black Hills Information Society

https://www.blackhillsinfosec.com/projects/backdoorsandbreaches/

NIST

https://www.nist.gov/itl/applied-cybersecurity/nice/resources/online-learning-content

Wizer

https://www.wizer-training.com/

Create Your Own Competition

Create a Healthy Security Culture

- Security awareness training should never be used as a punishment
- Employees receive regular training in identifying risks
- Employees are encouraged to ask for help when unclear about a security issue or policy
- Make training fun and personal
- Everyone is held to the same security standards

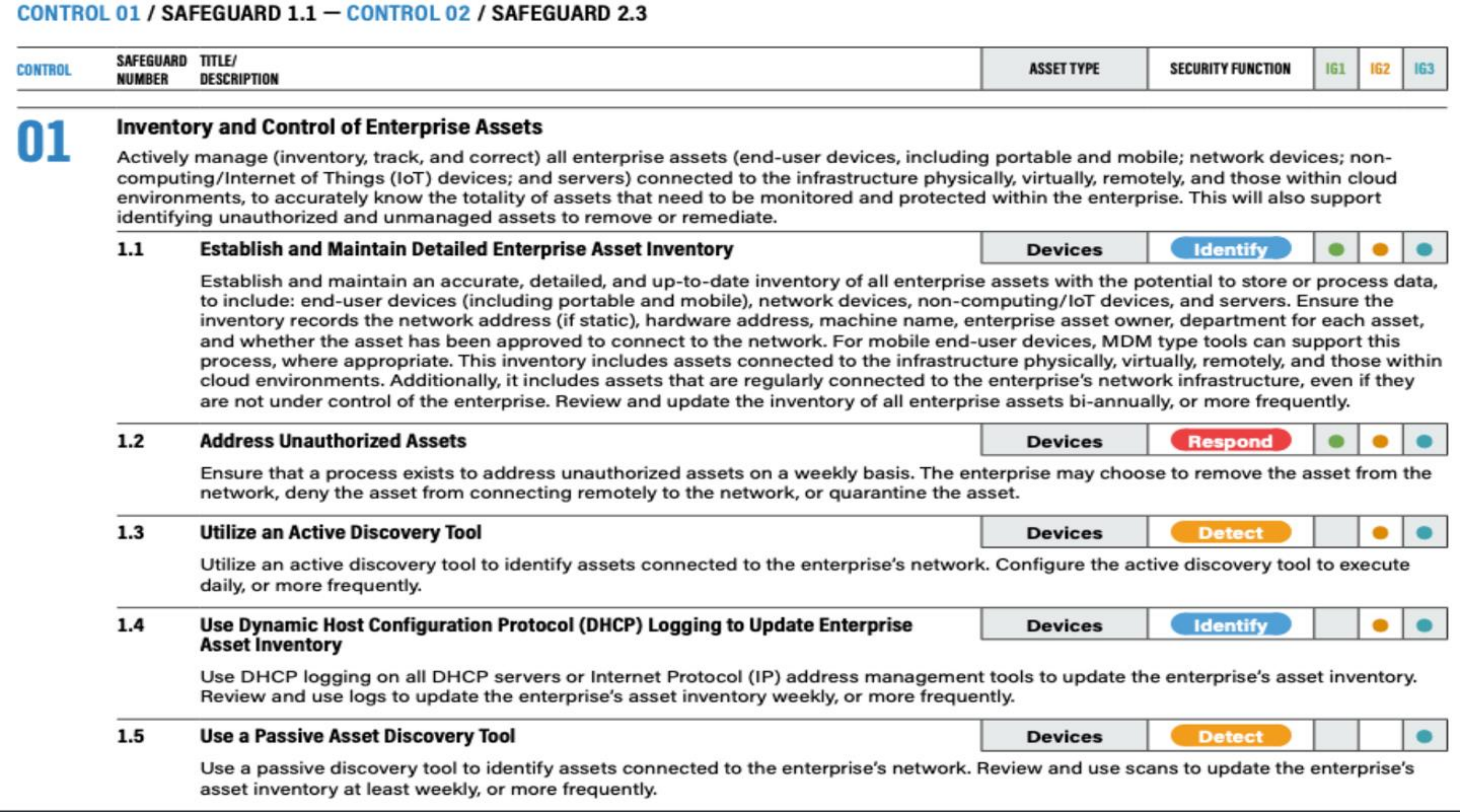
Process

Surface Attack Prevention
98%
Vulnerabilities Detected
System Normal
Attack Detected
Attack Blocked
Scan In Progress
All Systems

CIS 18 Critical Controls

Now with implementation groups!

Implementation Groups (IGs) are the recommended guidance to prioritize implementation of the CIS Critical Security Controls.



CONTROL	SAFEGUARD NUMBER	TITLE/ DESCRIPTION	ASSET TYPE	SECURITY FUNCTION	IG1	IG2	IG3
01		**Inventory and Control of Enterprise Assets** Actively manage (inventory, track, and correct) all enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/Internet of Things (IoT) devices; and servers) connected to the infrastructure physically, virtually, remotely, and those within cloud environments, to accurately know the totality of assets that need to be monitored and protected within the enterprise. This will also support identifying unauthorized and unmanaged assets to remove or remediate.					
	1.1	**Establish and Maintain Detailed Enterprise Asset Inventory** Establish and maintain an accurate, detailed, and up-to-date inventory of all enterprise assets with the potential to store or process data, to include: end-user devices (including portable and mobile), network devices, non-computing/IoT devices, and servers. Ensure the inventory records the network address (if static), hardware address, machine name, enterprise asset owner, department for each asset, and whether the asset has been approved to connect to the network. For mobile end-user devices, MDM type tools can support this process, where appropriate. This inventory includes assets connected to the infrastructure physically, virtually, remotely, and those within cloud environments. Additionally, it includes assets that are regularly connected to the enterprise's network infrastructure, even if they are not under control of the enterprise. Review and update the inventory of all enterprise assets bi-annually, or more frequently.	Devices	Identify	●	●	●
	1.2	**Address Unauthorized Assets** Ensure that a process exists to address unauthorized assets on a weekly basis. The enterprise may choose to remove the asset from the network, deny the asset from connecting remotely to the network, or quarantine the asset.	Devices	Respond	●	●	●
	1.3	**Utilize an Active Discovery Tool** Utilize an active discovery tool to identify assets connected to the enterprise's network. Configure the active discovery tool to execute daily, or more frequently.	Devices	Detect		●	●
	1.4	**Use Dynamic Host Configuration Protocol (DHCP) Logging to Update Enterprise Asset Inventory** Use DHCP logging on all DHCP servers or Internet Protocol (IP) address management tools to update the enterprise's asset inventory. Review and use logs to update the enterprise's asset inventory weekly, or more frequently.	Devices	Identify		●	●
	1.5	**Use a Passive Asset Discovery Tool** Use a passive discovery tool to identify assets connected to the enterprise's network. Review and use scans to update the enterprise's asset inventory at least weekly, or more frequently.	Devices	Detect			●

It’s OK if you don’t start with Control 01

Start where you’ll be the most effective

04 Secure Configuration of Enterprise Assets and Software

Safeguards — IG1 7/12 — IG2 11/12 — IG3 12/12

CONTROL 05 Account Management

6 Safeguards — IG1 4/6 — IG2 6/6 — IG3 6/6

CONTROL 06 Access Control Management

8 Safeguards — IG1 5/8 — IG2 7/8 — IG3 8/

07 Continuous Vulnerability Management

Safeguards — IG1 4/7 — IG2 7/7 — IG3 7/7

CONTROL 08 Audit Log Management

12 Safeguards — IG1 3/12 — IG2 11/12 — IG3 12/12

CONTROL 09 Email and Web Browser Protections

7 Safeguards — IG1 2/7 — IG2 6/7 — IG3 7/

10 Malware Defenses

Safeguards — IG1 3/7 — IG2 7/7 — IG3 7/7

CONTROL 11 Data Recovery

5 Safeguards — IG1 4/5 — IG2 5/5 — IG3 5/5

CONTROL 12 Network Infrastructure Management

8 Safeguards — IG1 1/8 — IG2 7/8 — IG3 8/

13 Network Monitoring and Defense

Safeguards — IG1 0/11 — IG2 6/11 — IG3 11/11

CONTROL 14 Security Awareness and Skills Training

9 Safeguards — IG1 8/9 — IG2 9/9 — IG3 9/9

CONTROL 15 Service Provider Management

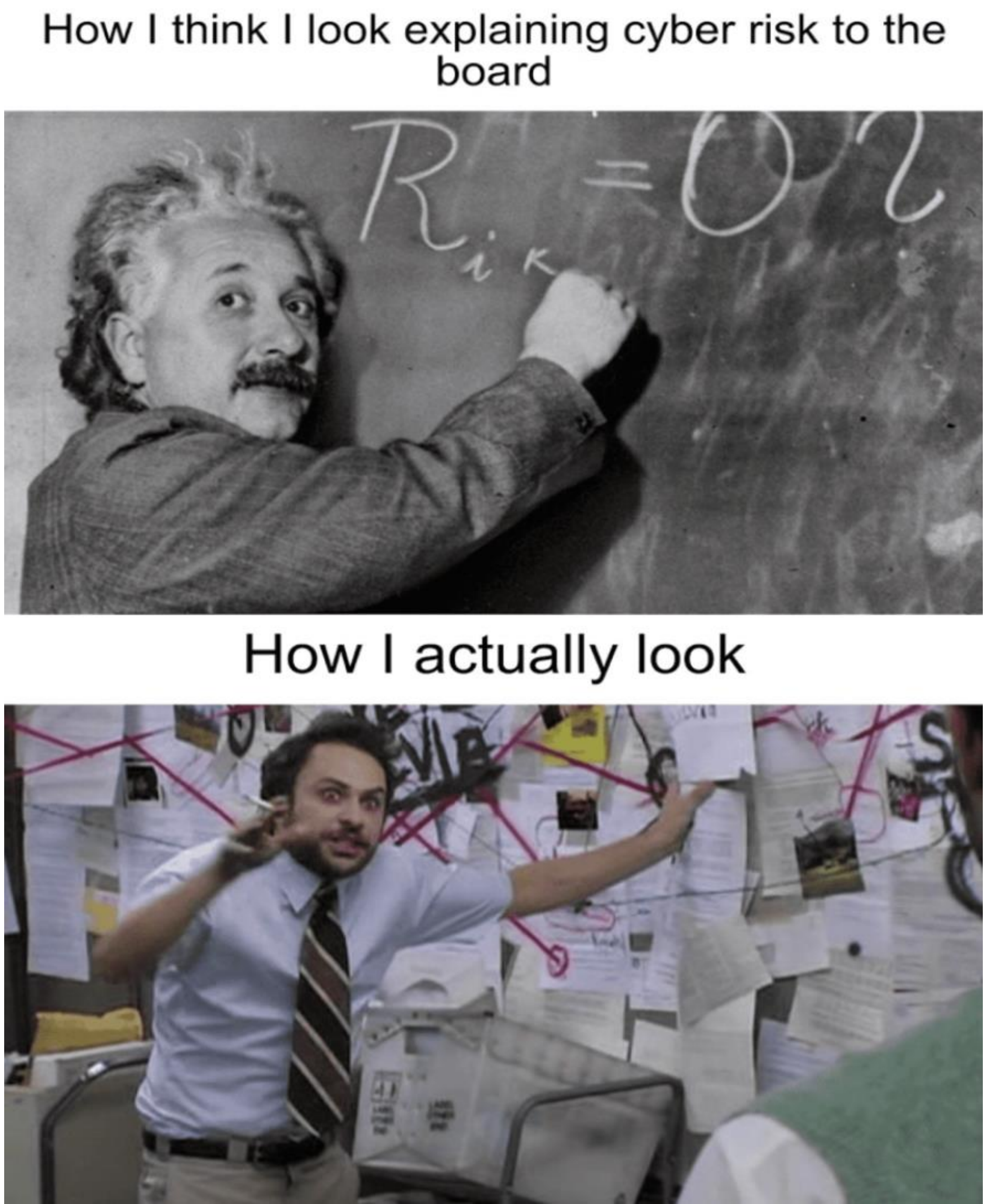
7 Safeguards — IG1 1/7 — IG2 4/7 — IG3 7/

Find Better Ways to Describe Risk

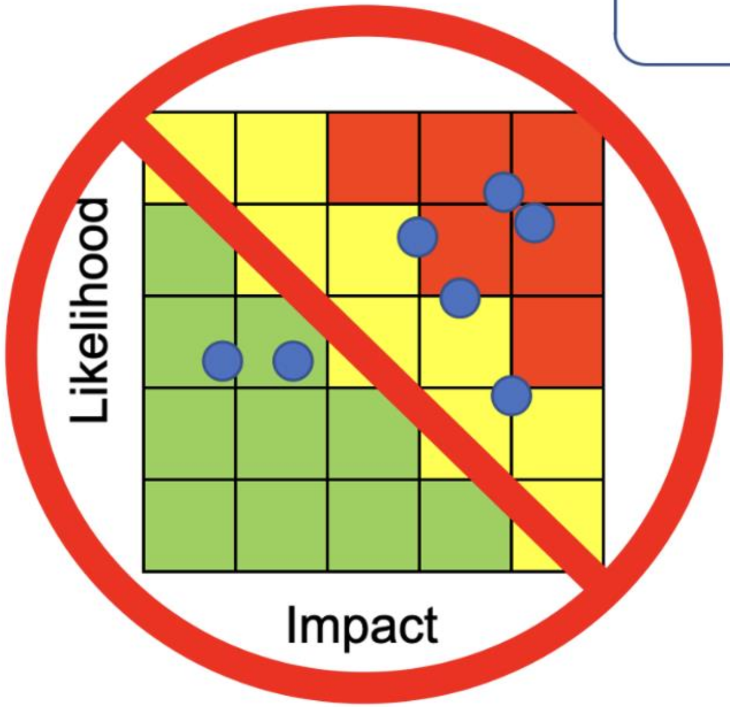
Current methods are not working

40% of global risk and compliance decision makers are improving risk management.

Forrester

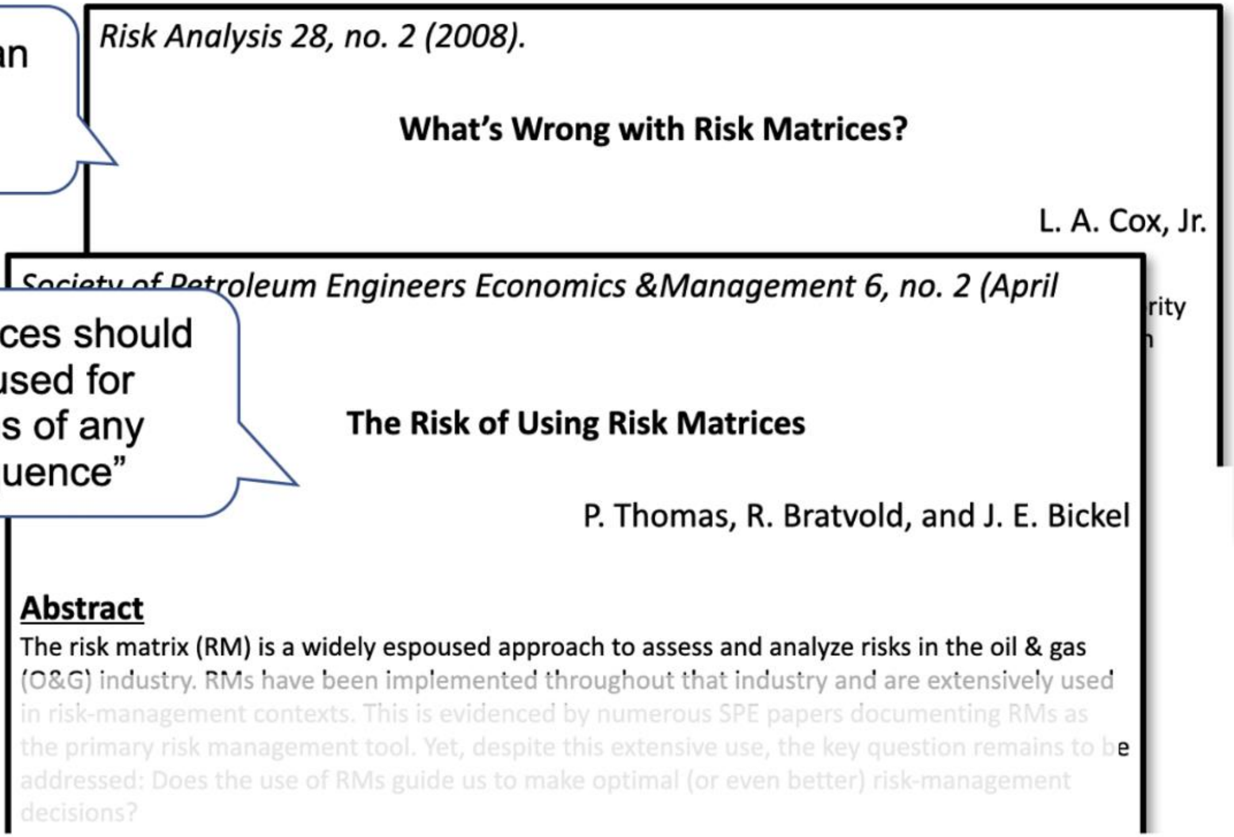


Stop Using Risk Matrices



"[Risk Matrices] can be worse than useless"

"Risk Matrices should not be used for decisions of any consequence"



Risk Analysis 28, no. 2 (2008).

What's Wrong with Risk Matrices?

L. A. Cox, Jr.

Society of Petroleum Engineers Economics &Management 6, no. 2 (April

The Risk of Using Risk Matrices

P. Thomas, R. Bratvold, and J. E. Bickel

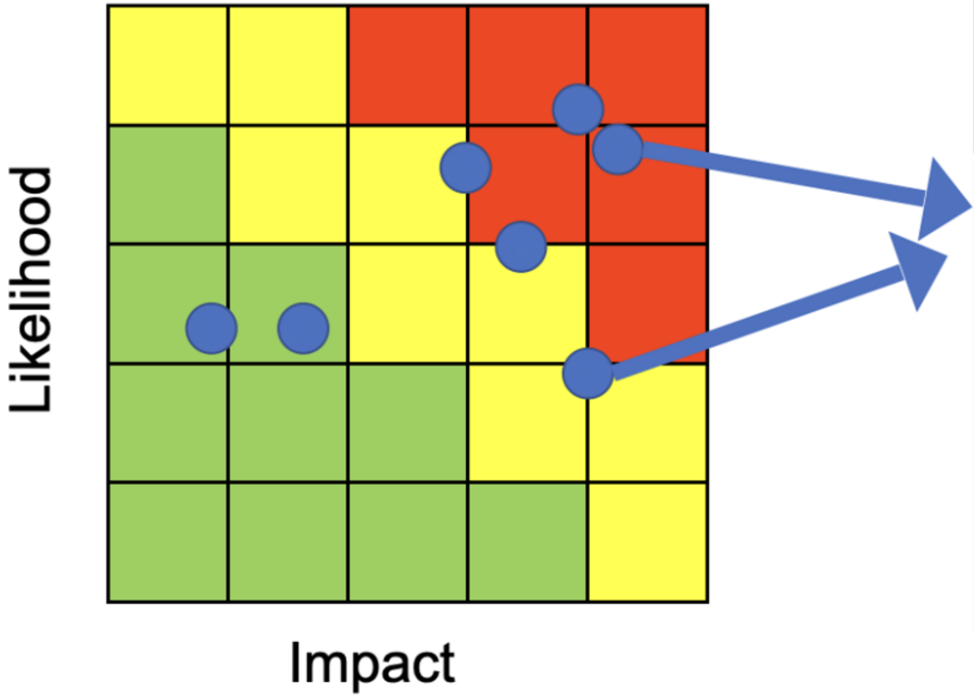
Abstract

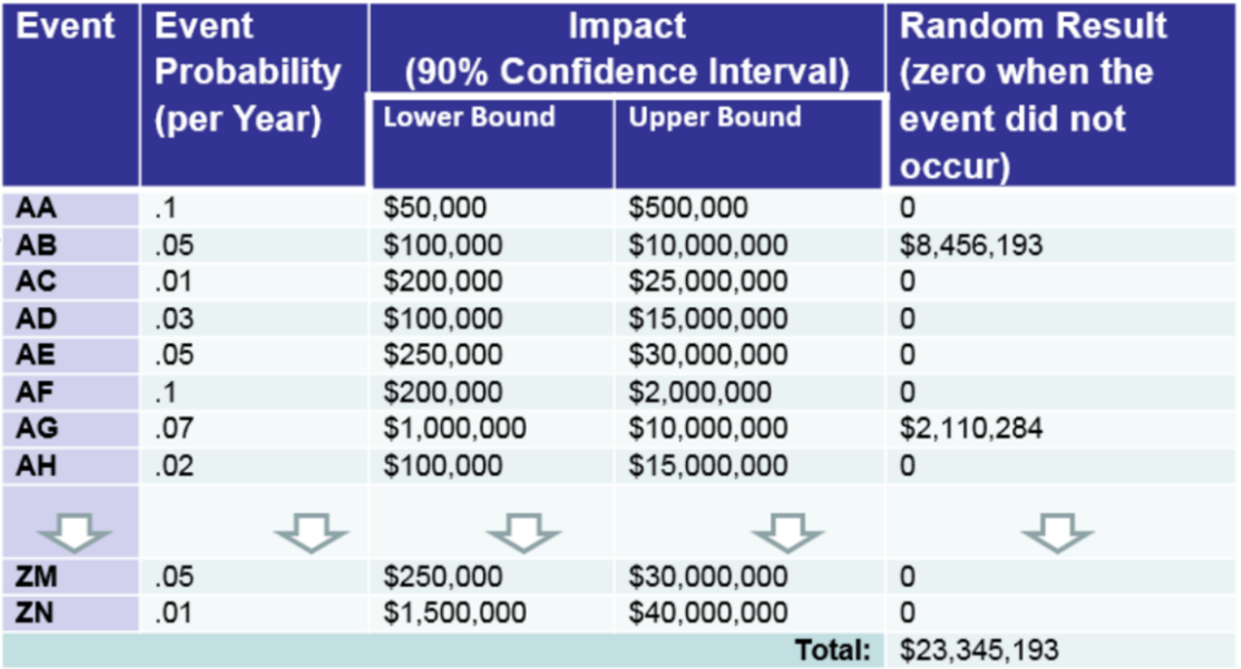
The risk matrix (RM) is a widely espoused approach to assess and analyze risks in the oil & gas (O&G) industry. RMs have been implemented throughout that industry and are extensively used in risk-management contexts. This is evidenced by numerous SPE papers documenting RMs as the primary risk management tool. Yet, despite this extensive use, the key question remains to be addressed: Does the use of RMs guide us to make optimal (or even better) risk-management decisions?

Use Monte Carlo Simulations Instead

Each of these examples can be found on

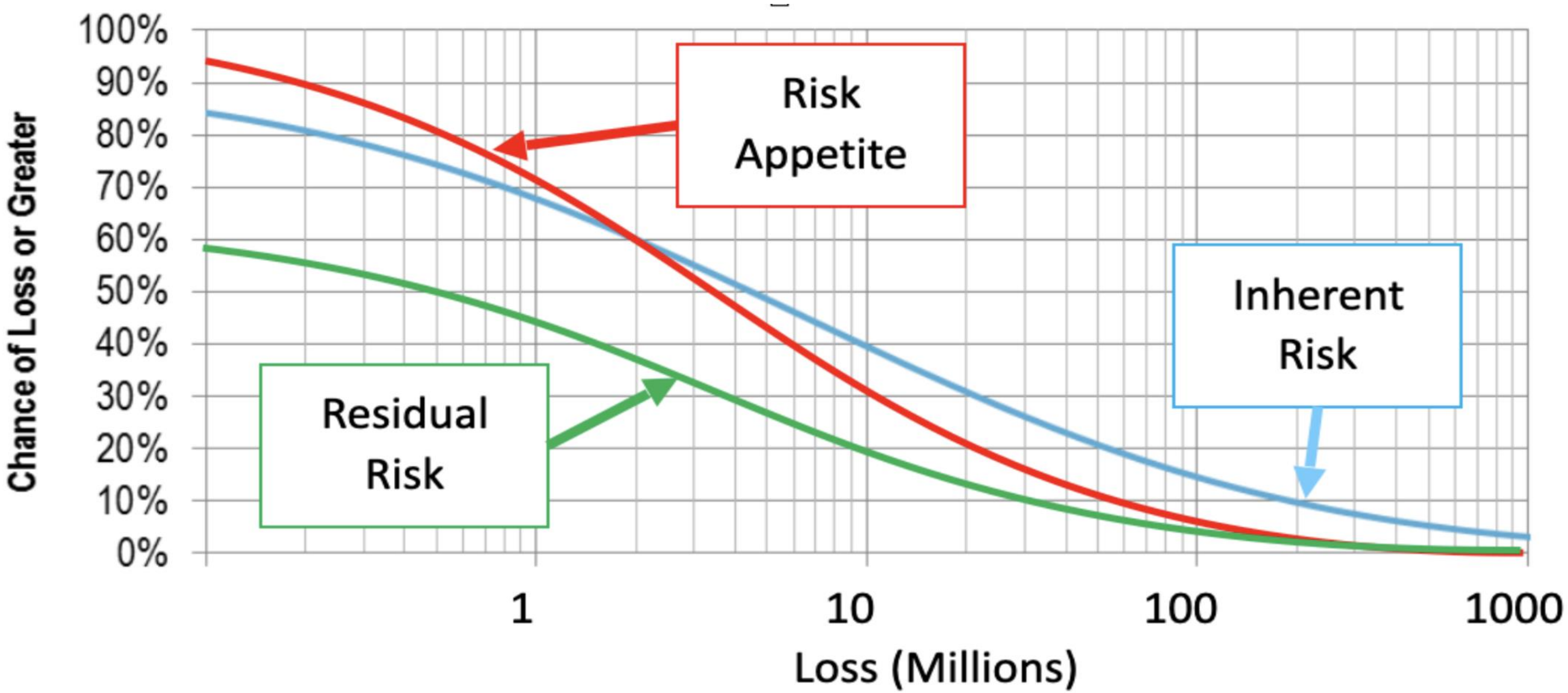
www.howtomeasureanything.com/cybersecurity





Event	Event Probability (per Year)	Impact (90% Confidence Interval)		Random Result (zero when the event did not occur)
		Lower Bound	Upper Bound	
AA	.1	$50,000	$500,000	0
AB	.05	$100,000	$10,000,000	$8,456,193
AC	.01	$200,000	$25,000,000	0
AD	.03	$100,000	$15,000,000	0
AE	.05	$250,000	$30,000,000	0
AF	.1	$200,000	$2,000,000	0
AG	.07	$1,000,000	$10,000,000	$2,110,284
AH	.02	$100,000	$15,000,000	0
⇩	⇩	⇩	⇩	⇩
ZM	.05	$250,000	$30,000,000	0
ZN	.01	$1,500,000	$40,000,000	0
			Total:	$23,345,193

This, Your Board Will Understand



Basic Hygiene

CISA Free Services

- Cyber Hygiene Services
  - Vulnerability Scanning
  - WebApp Scanning
- Incident Management Review Training
- Cyber Resilience Review

Smart Assessments & Audits

They can be your best leverage when done right

- Risk or Threat Assessments 1st
    - These should always precede a security assessment
- Tailor Audits & Assessments
    - They should support YOUR security goals and budget needs whenever possible
- Every Assessment Should be a Purple Team Exercise
- Create Highly Detailed Scoping Docs
    - If you don’t scope assessments properly, most consulting firms will simply have their interns scan you with Nessus
- Insist on Quality Output
    - A paid assessment should result in actionable recommendations and remediation plans

Pick the Right "Box"

Get the best value from assessments

"Black Box" is a poor choice

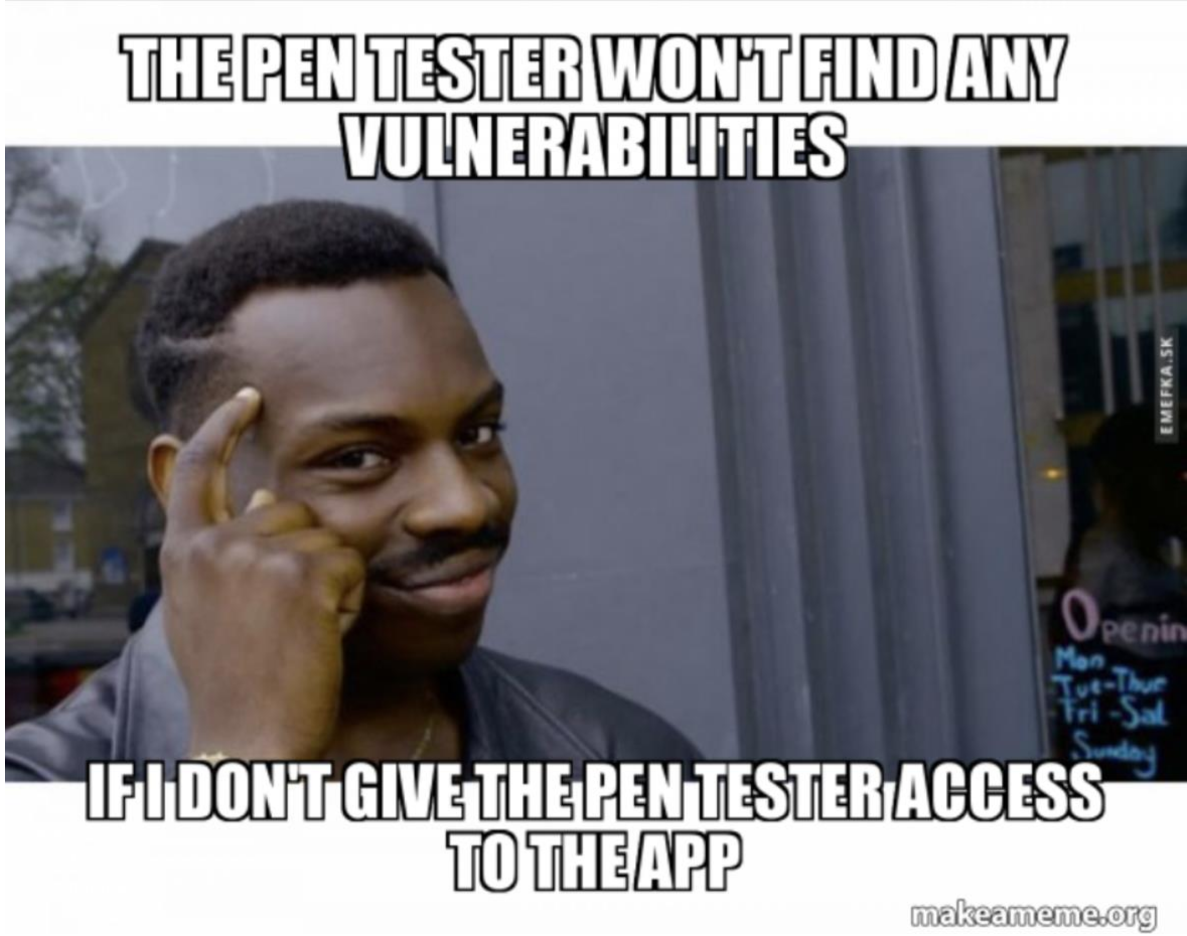
- These assessments require the tester to "break in" on their own. They waste too much time on a result you know is going to happen. They will eventually phish their way in. These primarily just "test the tester."

"Transparent Box" is a Better Option

- Assumes the tester will get in anyway. So just give them access and details of the org. See how far they can get. Saves time, reduces cost. Allows for testing of more vectors.

"Translucent Box" - Next Step Up

- Limited info is shared with the tester. Typically just login creds. Simulates a real-world scenario.


THE PEN TESTER WON'T FIND ANY VULNERABILITIES
IF I DON'T GIVE THE PEN TESTER ACCESS TO THE APP
makeameme.org
EMEFKA.SK

Guerilla Zero Trust – Zero Trust is a Process, not a TOOL

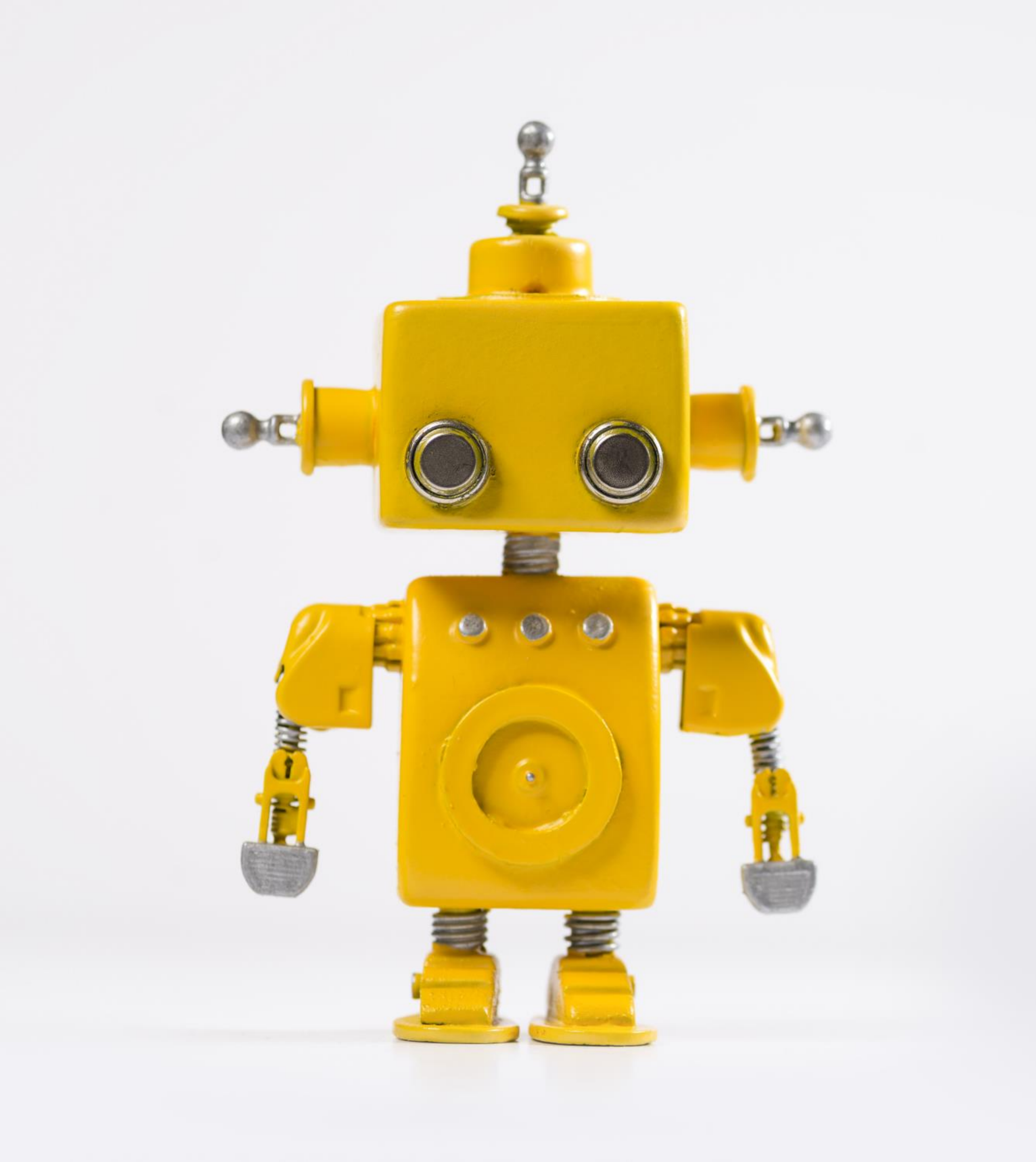
- Implement MFA for EVERYONE
  - Users, Admins, Contractors, Executives (even when they complain), Partners, Third-Party Vendors, ANYONE who touches your systems
- Log and Monitor All Privileged Credential Activity and Sessions
  - Google, Microsoft, TextPower SnapID, Authy
- Implement Security Remote Access
  - Put shared accounts/passwords in a vault or Firecall

- Use Jump Boxes or Security Admin Workstations (SAW) for Privileged Tasks)
  - This is the quickest way to isolate these tasks
- Log and Monitor All Privileged Credential Activity and Sessions
  - For compliance and forensic review, Include session metadata
- Audit Priv Access Creds to Network Devices
  - Most vuln scanners can check for default pwd

Find Ways to Automate EVERYTHING

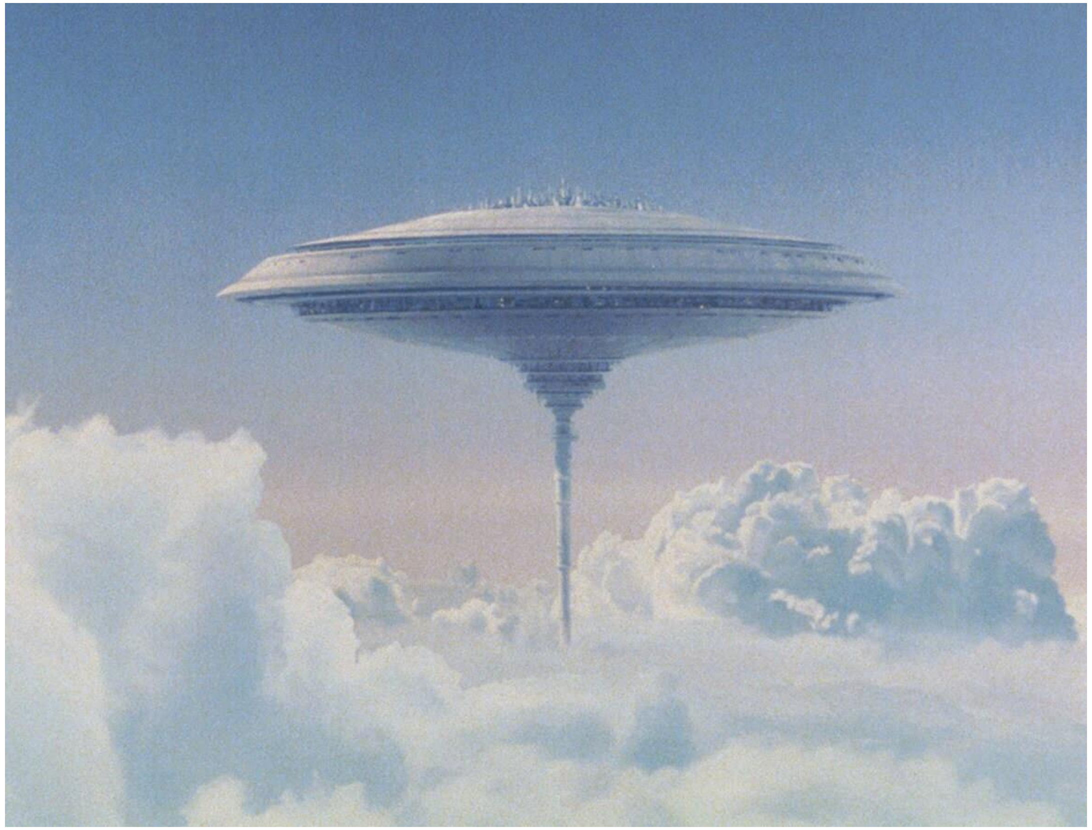
Consider Hiring an Automation Engineer

- If you do a task more than once, it should be automated



Technology

Surface Attack Prevention
98%
Vulnerabilities Detected
System Normal
Attack Detected
Attack Blocked
Scan In Progress
All Systems



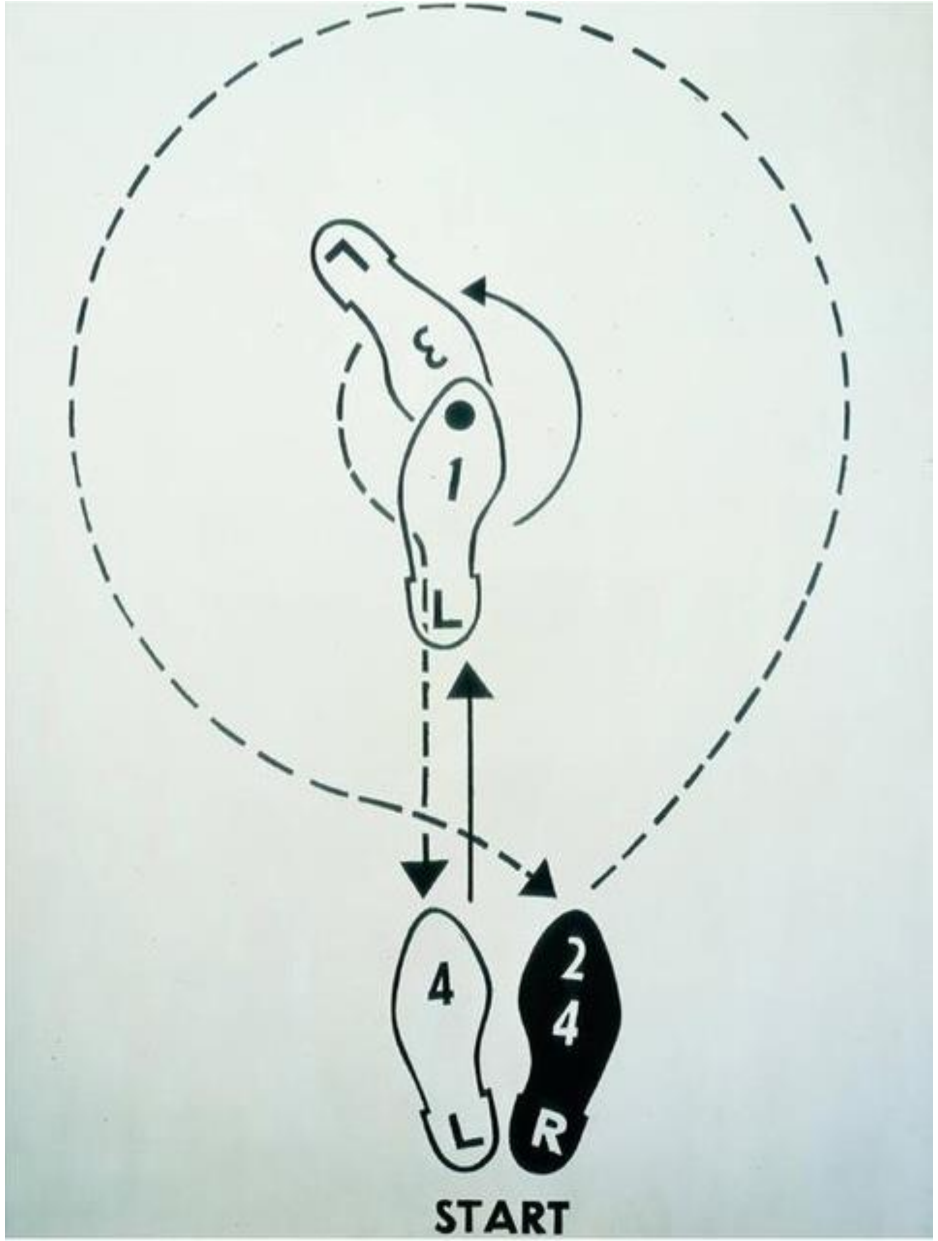
Leverage those “Other” Cloud Services

- Easy, robust, frequent, immutable backups, put the PW in Firecall
- Use available cloud-based security services, AWS-WAF, Google Cloud Armor
- Clean images, regularly reloaded
- Chaos engineering

Limit Your Exposure in Two Easy Steps

- Switch Users to Chromebooks
- Get Rid of Active Directory
  - Use Identity Mgmt Tools
  - Okta, Ping Identity, etc.

Special thanks to @Lintile & @AccidentalCISO



Deception Tactics

Your leverage for more budget and influence

Honey Files

- Files with names like “Password List”
- Alert on Access

Honey Accounts

- DomainAdmin_x
- Put fake “password” in the description
- Add to admins group
- Logon hours=0

Honey Database / Honey Table

- Call it something juicy

Honey Tokens in Memory

- Use CreateProcessWithLogonW
- Free Tool: Invoke-Runas.ps1
- Loads fake admin acct & creds into memory

Honey People

- LinkedIn
- HR
- Accts Payable

NetSPI Proactive Security Solutions

PTaaS

Pentesting programs from Appsec to AI

- Expert delivered pentesting via SaaS platform
- Real-time in-platform reporting
- Decrease detection and remediation time
- Easily integrate with ticketing systems
- Meet compliance needs

BAS

Security control validation

- Validate security detection control efficacy
- Simulate real-world attacker behaviors
- Fine-tune security controls and optimize security stack
- Strengthen ransomware prevention defenses
- Track progress and demonstrate ROI

ASM

Attack Surface Management

EASM

- Always-on external asset discovery and monitoring
- Eliminate noise with validation, prioritization
- Deep context with potential attack path scenarios

CAASM

- Total internal asset visibility and contextualization
- Real-time, centralized risk and vulnerability mapping
- Visualize impact with blast radius

We bring together dedicated security experts, intelligent process, advanced technology to contextualize the priorities that will have the biggest impact on your business

Thank You!

Helpful Links

- https://www.linkedin.com/in/robertwagner2/
- https://www.chicagocisooftheyear.com/
- https://burbsec.com/
- https://www.hak4kidz.com/
- https://www.netspi.com/open-source-tools/