



# A Theme of Fear: Hacking the Paradigm

# AGENDA

- Introduction
- Fear and Loathing
- The Cost of Fear
- A History of Fear
- The Consequences of Fear
- Changing the Paradigm
- Moving Forward
- Final Thoughts



# Introduction

Me!



A decorative background featuring a circuit board pattern with white lines and circles on a dark teal gradient. The pattern is most prominent on the left and right sides, with lines extending from the corners towards the center.

@INVESTIGATORCHI

Dr. Catherine J. Ullman

- Sr. Information Security Analyst, University at Buffalo
- Staff: BsidessROC, UB GenCyber Camp
- VP: Buffalo-Niagara ISSA Chapter
- Volunteer: Wall of Sheep, Skytalks, BsidessLV
- Speaker: Wall of Sheep, Hacker Halted, Circle City Con
- Certifications: GSEC, CEH, CFCE, MCSE
- M.F.S. (Master of Forensic Science), PhD, Philosophy

# Fear and Loathing





1989

# What Virus?

If you think your data center is immune to viruses because you're running MVS, you're gravely mistaken. Your system could be infected right now.

**CA-UNIPACK/SCA for MVS  
is the best defense you can buy.**

Now CA-UNIPACK™/SCA, the industry's only complete Security, Control and Audit software solution, lets you rapidly detect everything from logic bombs to trap doors, Trojan Horses and, yes, viruses.

With CA-EXAMINE™ CA-ACF2™ or CA-TOP SECRET® and CA-VMAN™ included in CA-UNIPACK/SCA, you'll get extensive MVS auditing capabilities in addition to total access control and enhanced network security.

So don't wait for a security breach to cripple your MVS system. Ensure your data is safe with a total solution from the world's leading security software company, CA-UNIPACK/SCA from Computer Associates.

For more information, call Dana Williams at 800-645-3003 and ask for your free copy of the special **virus** issue of Security & Audit News.



© 1989 Computer Associates International, Inc.,  
711 Stewart Avenue, Garden City, N.Y. 11530-4787

NETWORK WORLD • JULY 17, 1989  
41

Copyrighted material

Your system  
could be  
infected right  
now

2007

## Evolved over billions of years... Protecting your enterprise in one hour.

The immune system has evolved over billions of years. But it takes just one hour to install one in your enterprise.

Using artificial intelligence, Darktrace can tell friend from foe, and catches threats that others miss. Even if they've never been seen before.

From quiet insider threats and zero-day attacks, to hacks of connected devices or industrial networks, our software sees it and responds.

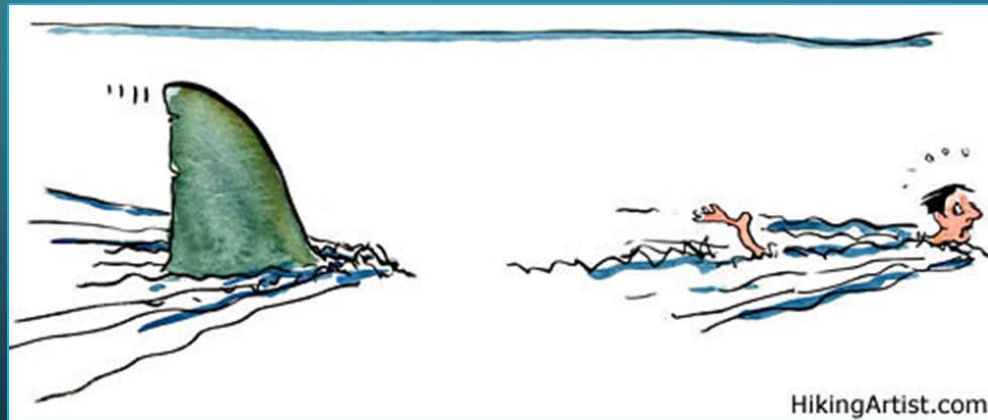
Find out what's lurking inside your systems.  
darktrace.com

Find out  
what's  
lurking inside  
your systems

**DARKTRACE**  
World-Leading Cyber AI

## WHAT WE THINK FEAR CAN DO:

- Motivate a positive change in behavior
- Bolster human behavior change







# The Cost of Fear

## MORE SPENDING = MORE SECURE, RIGHT?

- 2017 - \$86.4 billion worldwide spending on InfoSec
- 2018 - \$114 billion worldwide spending on InfoSec  
(up 12.4%)





Spoiler: It's not working.

# “Blinky Box Syndrome” - Chris Roberts

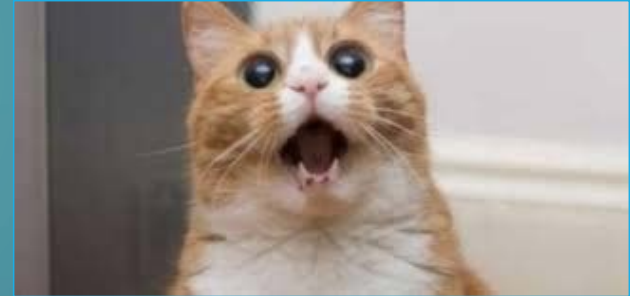


e.g.

- AI
- ML
- Next-Gen

## WHAT FEAR ACTUALLY DOES:

- Cause a defensive response
  - Not enough fear = complacency
  - Too much fear = paralysis, controlled by it
- Create negative association w/company or product
- Create overreactive response







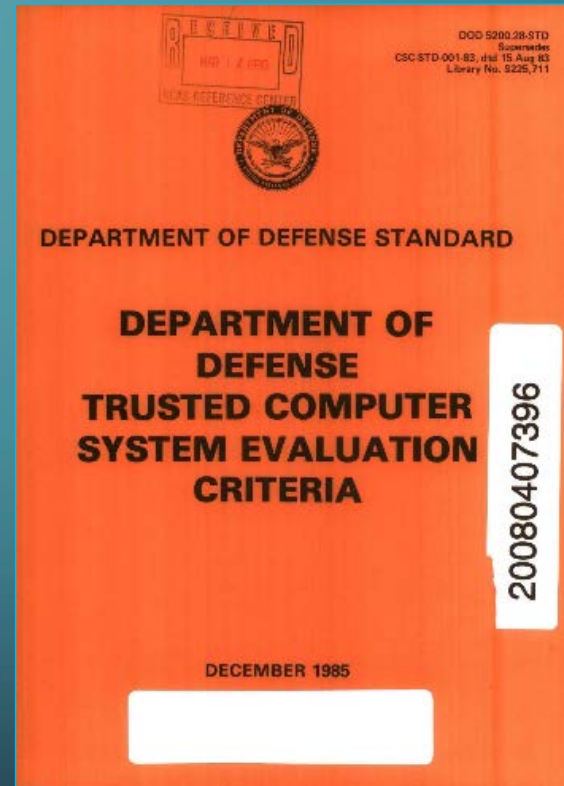
# A History of Fear

# FEAR BY DESIGN



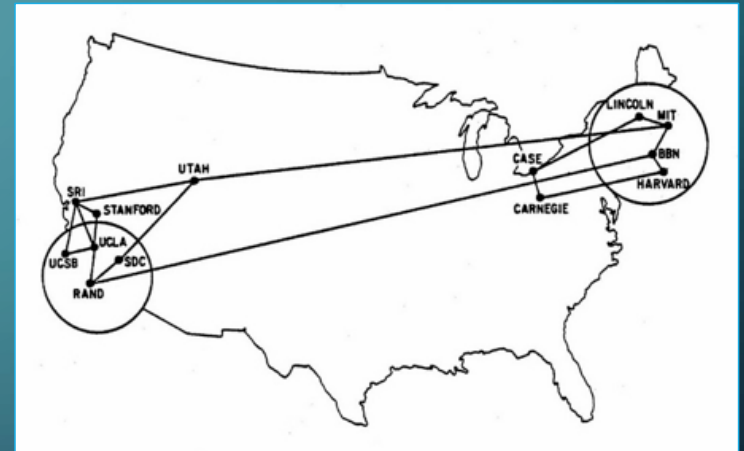
# ORANGE BOOK JOY

- Terms “information security” or “cyber security” do not exist
- Government risk assessment, policy, and controls



# THE INTERNET BEGINS

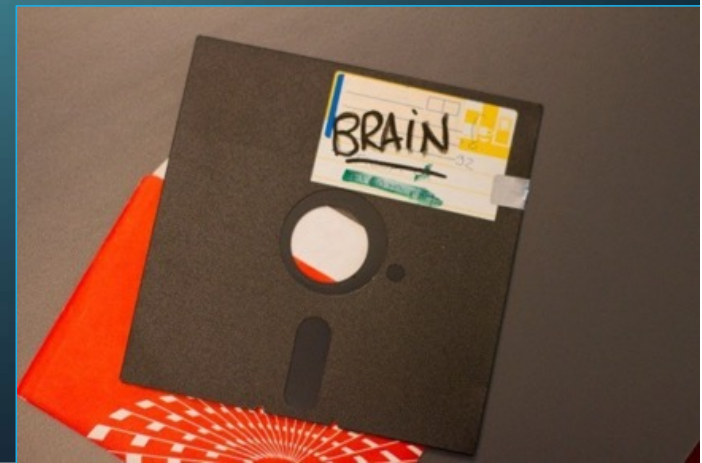
- Mid-1980s
  - ARPANET expanding
    - BITNET!
  - Personal computer boom
  - Companies using “the Internet”



ARPANET 1970

## EARLY SECURITY DEVELOPMENTS

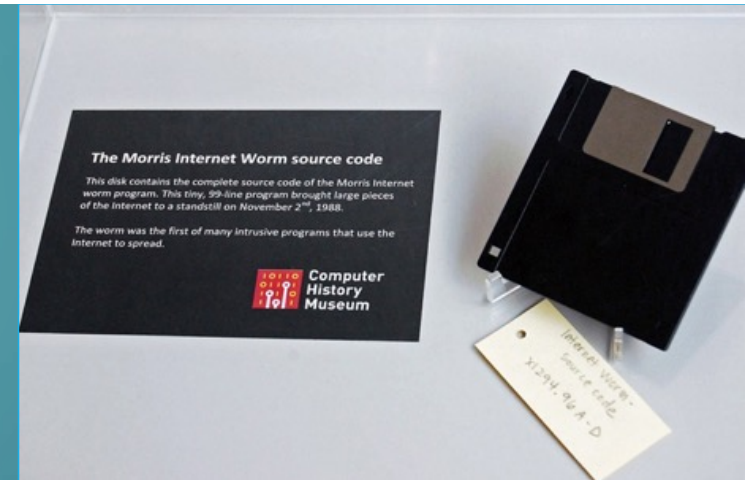
- 1986 – First PC virus “Brain” catalyst for John McAfee
  - Copyright infringement tool “wipes files”
- Late 80s - Symantec and Sophos debut
  - 1989 – More AV vendors than viruses





# GOVERNMENT RESPONSE

- 1986 - Gov't fear of virus infections
  - “potentially devastating weapon”
  - “high technology equivalent of germ warfare”
- 1988 – Morris Worm hits
  - Crashed 1/10 of all computers on the internet
  - First CERT at Carnegie Mellon established



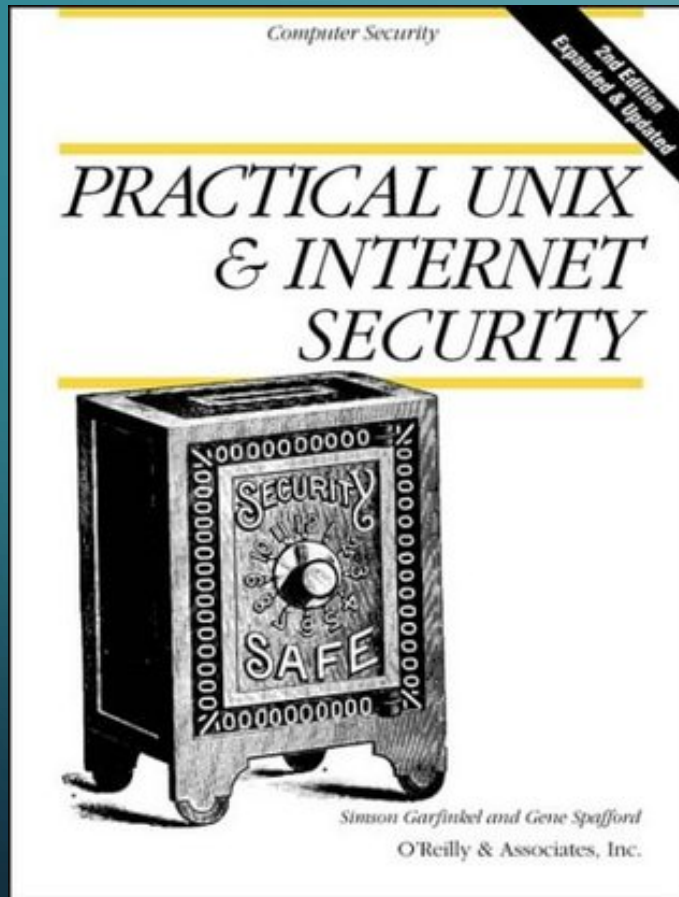
## FEAR OF EXTERNAL ATTACK → SPENDING \$

1990 –

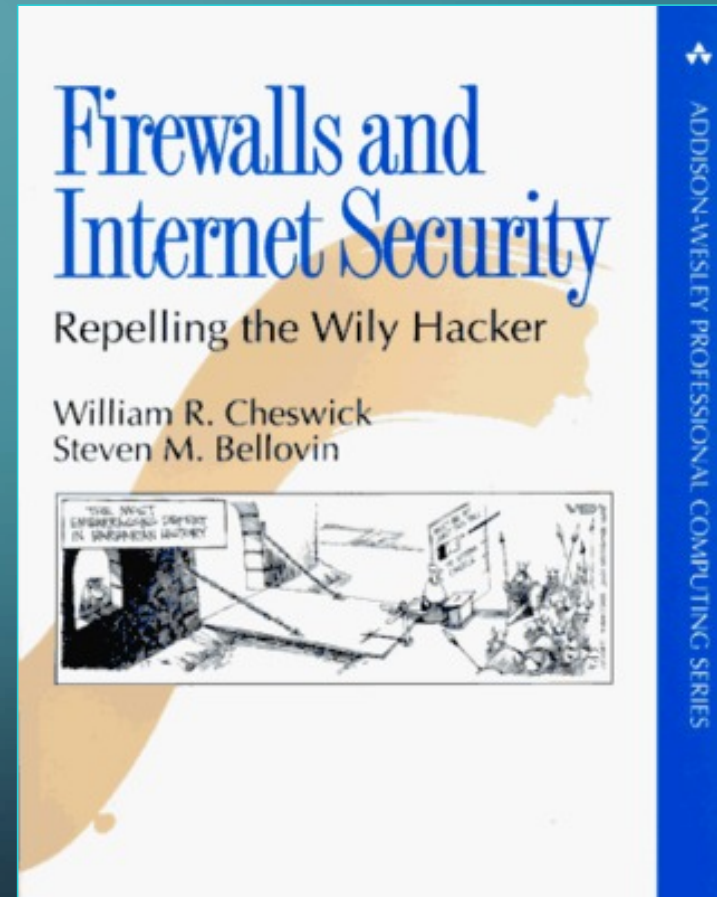
- Annual cost of malware removal: \$1.5 billion worldwide
- Prevention: \$5-10/mo. per PC for AV or 2 salaries  
\$120k-\$150k = now reasonable



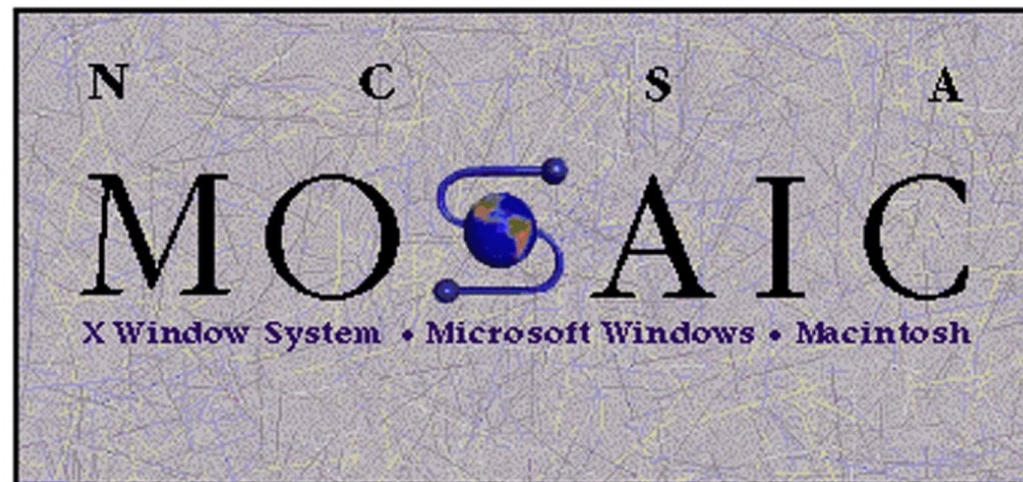
1991



1994



# JANUARY 23, 1993 - MOSAIC INITIAL RELEASE (AND THE WORLD CHANGED)



Welcome to NCSA Mosaic, an Internet information browser and [World Wide Web](#) client



“AFTER ALL, VIRUS PROTECTION IS A MATTER OF TRUST”

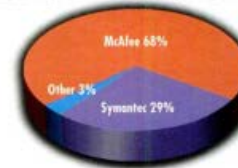
## THE MOST COMPLETE PRODUCT LINE.



## THE BEST VIRUS PROTECTION.



## THE NUMBER ONE CHOICE WORLDWIDE.



Worldwide Standalone  
200 and Windows  
Shipments - IDC, 3/94

## JUST SOMETHING TO THINK ABOUT BEFORE TRUSTING SYMANTEC.

### “Symantec’s little fib” – Information Week, 9/11/95

A lot of people disagree with Symantec’s claim that they have the best virus protection. Even some Symantec people.

Vice President of Desktop Utilities, Ellen Taylor, said “we...regret any misconception...” that resulted from Symantec overstating its detection rate. *Information Week* described it as “Symantec’s Little Fib.”

*The San Jose Mercury News* added that “Symantec, with NCSA’s urging, has acknowledged that it may have exaggerated a bit.”

Another Symantec ad misleads readers by comparing their desktop anti-virus product with McAfee’s VirusScan for the Internet.

Advertising aside, just how good is Symantec virus protection? VSUM tests over the past year show that Symantec detected less than 88% of all viruses while McAfee VirusScan caught over 97%.



### “Norton’s chicken soup not as foolproof as advertised” – San Jose Mercury News, 9/15/95

Maybe that’s why McAfee virus protection is trusted by over 10 million users. More than all others. And maybe that’s why 80 of the Fortune 100 trust McAfee’s products.

To find out for yourself, just download any fully-functioning McAfee product. There are no encryptions or time bombs. We trust you to pay us if you decide to keep it. After all, virus protection is a matter of trust.

And now that you have all the facts, we trust you’ll decide on McAfee.

For more information on McAfee products, including our on-line technical support, call 1-888-VIRUS NO toll free.



Download McAfee: WWW: <http://www.mcafee.com> Internet FTP: <ftp://ftp.mcafee.com> BBS: 14081988-4804 America Online: McAfee! CompuServe: GO McAfee! The Microsoft Network: McAfee!

\*Data includes only for February 1996. Telephone 14081988-8822 Fax 14081970-9717 © McAfee Associates, Inc., 1996. All rights reserved. All brands and products are trademarks of their respective holders.

Copyrighted material



# BLINKY BOXES?



# BLINKY BOX BEGINNINGS

- 1990s: Network firewalls commercially available
  - DEC SEAL - Marcus Ranum
  - Secure gateway - unwanted traffic prevented
  - “virtually fail-safe protection”
- 1995: Mitnick hacks San Diego SCC
  - Spoofing address/sequence prediction attack



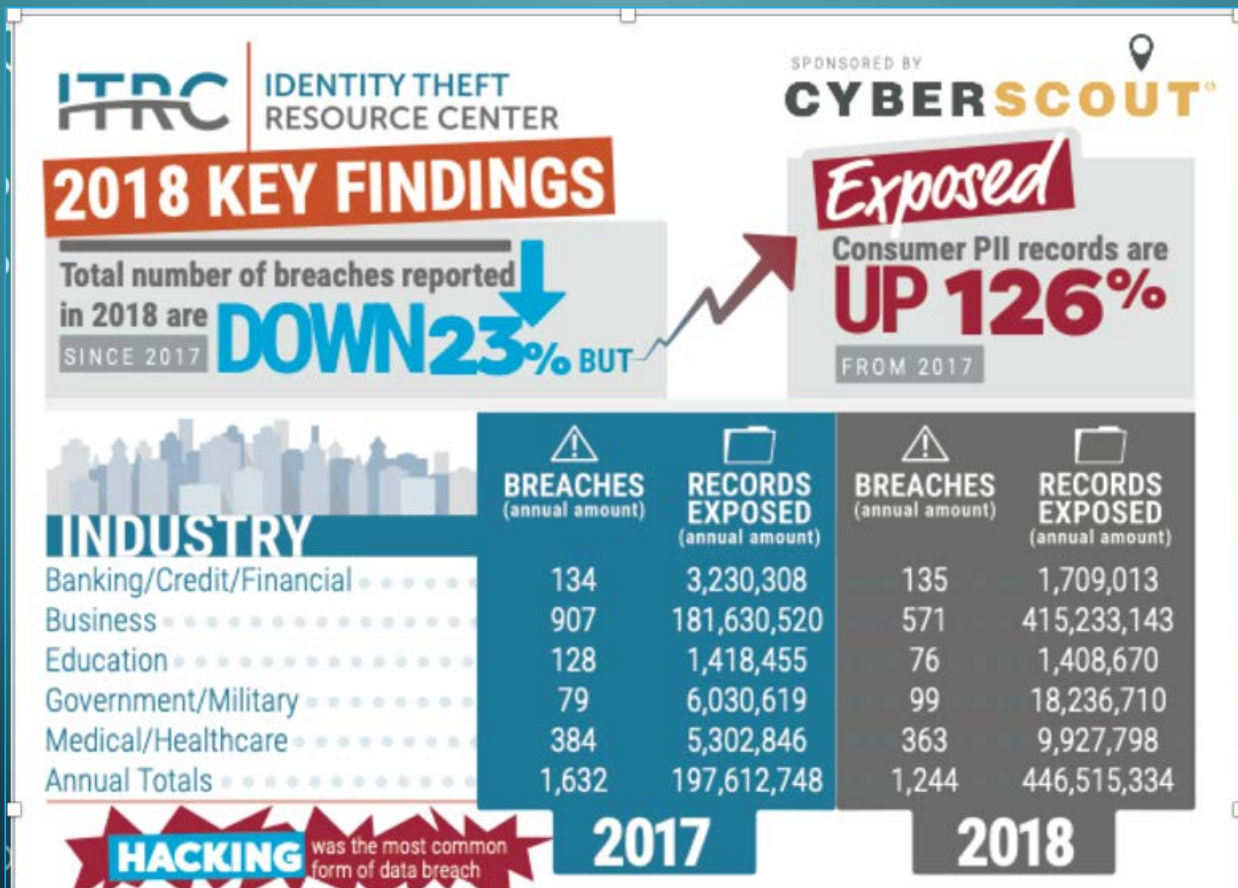


And today? Now that we have  
all the money for all the  
things?





NAH...







# The Consequences of Fear



# FUD – FEAR UNCERTAINTY AND DOUBT

- Fear-based marketing strategy
  - Involves spreading product misinformation
  - Discouraging purchase of competitors product
  - IBM vs. Gene Amdahl

“The security industry generates FUD in order to sell hope.”

-Rich Smith, Duo Security

## 7. Create FUD about competitors

I think I'll stick with EMC. They showed me that moving to a consolidation solution is dangerous and expensive.

I'm not surprised they told you that since they can't help you consolidate, and wouldn't, even they could – after all, they couldn't sell you as many new disks! You might want to ask them why they think 30% storage utilization is okay for you.



## FEAR DRIVEN IMAGE PROBLEM

“In large part due to mainstream media, the idea of security often becomes entangled with fictional concepts of who the people in the world of security are and what the data battlefield looks like.”

--Hafsah Mijinyawa, Duo Security

We fear what we do not understand

# FAMILIAR MARKETING IMAGERY





# SOMEONE WITH MALICIOUS INTENT != HACKER

“Hacking is the art of understanding how computers work, rather than how you are told they ought to work.”

-Rich Smith, Duo Security

Is this your idea of what  
a hacker is?



## FEAR IN THE DEV WORLD



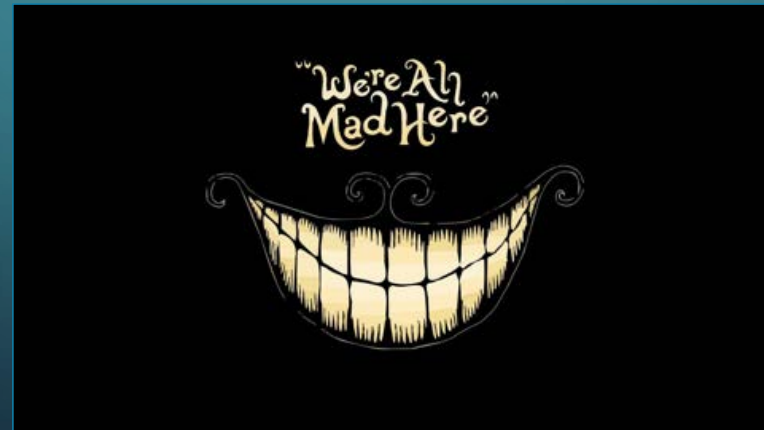
- Potential shame/embarrassment if code → breach
- Demand for complex/large quantity code in short time
- Security not foundational in CS programs
- Additional time/effort required for secure code review

## CONSISTENCY AS A FLAW

CONSIST  
ENCY

- Security as a business afterthought
- Blinky boxes purchased as an “easy button”
- Working against/despite users
- Minimal/no security training for CS students

The definition of insanity is doing the same thing over and over again expecting different results.



## WHERE FEAR AND HATE COLLIDE



***Fear** is the path to the dark side. Fear leads to **anger**. Anger leads to **hate**. Hate leads to **suffering**.*

*- Yoda*

Goalcast



# EVERYONE HATES CYBERSECURITY PROFESSIONALS



[NOTE: BASED ON THYCOTIC REPORT: [HTTPS://THYCOTIC.COM/RESOURCES/CYBER-SECURITY-EXECUTIVES-SURVEY-REPORT-EUROPE/](https://thycotic.com/resources/cyber-security-executives-survey-report-europe/) ]

66%

“doom mongers”

“necessary evil”



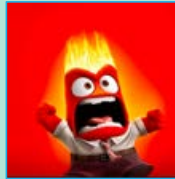
Security teams  
are massively  
misunderstood

38%

“Policemen”



74%



Experience  
indifference/negativity  
implementing new rules

50%



InfoSec purpose → lights  
on/systems working

67%



Infosec is reactive/cost  
center, not asset

## TOP DEFINITION

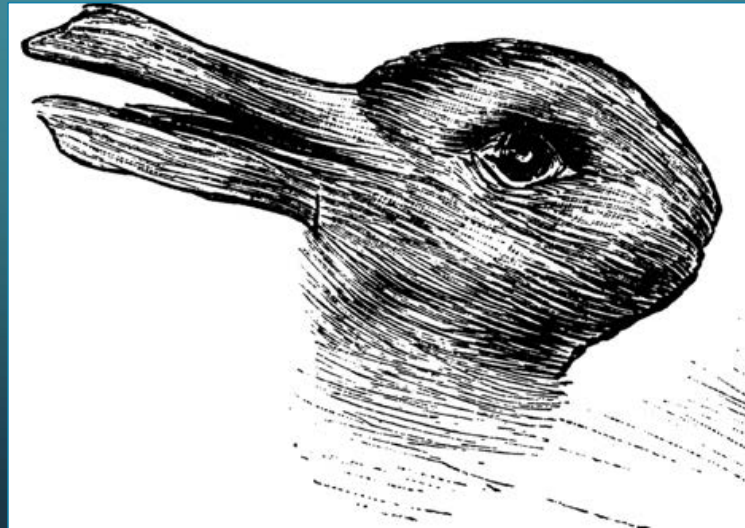


# Infosec

A profession that turns normal people into whiskey drinking, swearing, paranoid, disheartened curmudgeons with no hope for the future of computers or humanity.

*Hi, I work in Infosec. Please pass the whiskey.  
No, I won't fix your computer.*

# Changing the Paradigm





# OVERCOMING FEAR

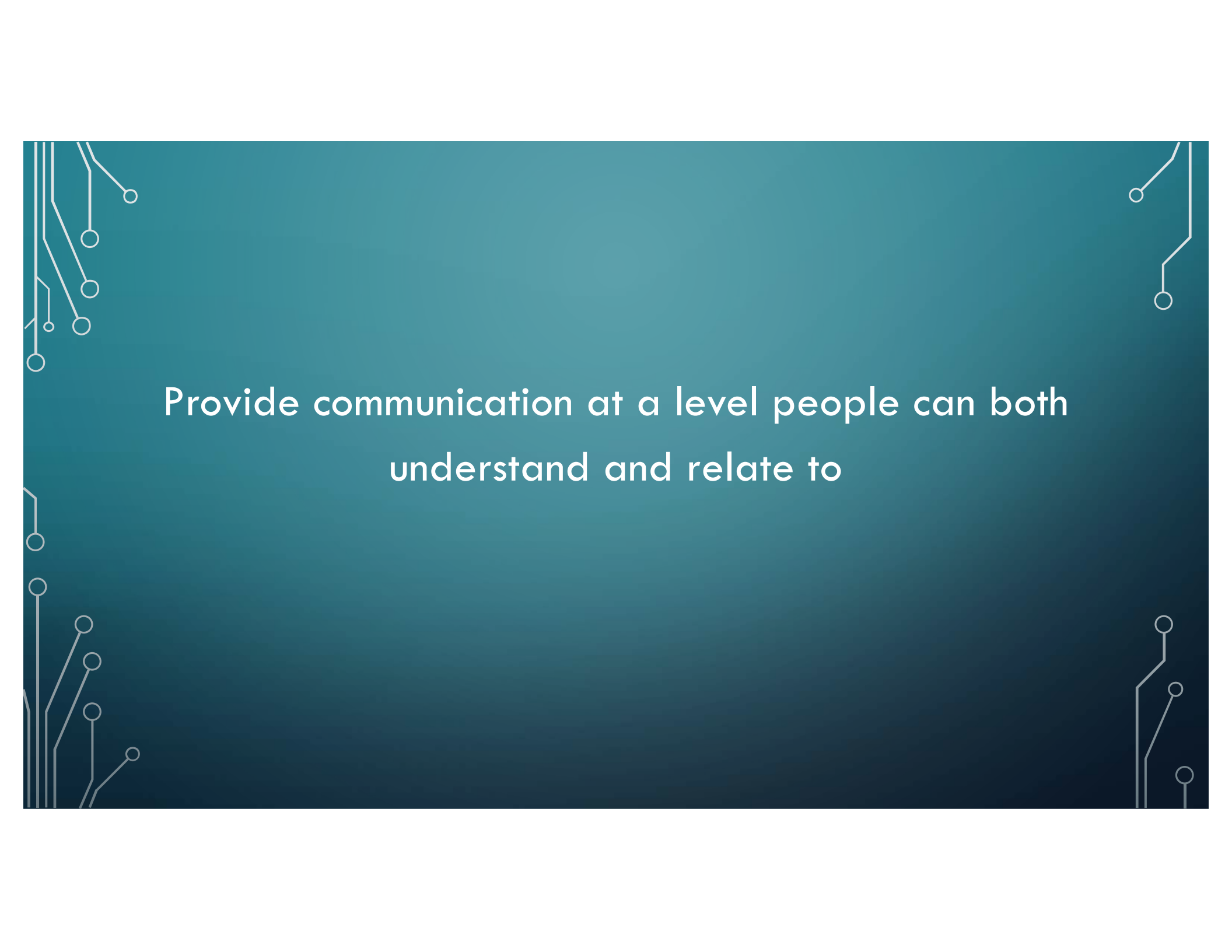
- Honest, yet discerning communication about risk
  - Sometimes less is more
- Empower others
  - Positive messaging
- Be an advocate
  - Actively encourage best practices

“It’s Scary...It’s Confusing...It’s Dull”: How Cybersecurity Advocates Overcome Negative Perceptions of Security – 14<sup>th</sup> Symposium on Usability Privacy and Security

## “US” VS. “THEM” MUST STOP

- Listen to concerns (perception = reality)
- Avoid condescension
- Be patient
- Honest responses/follow through
- Illuminate to build community of trust





Provide communication at a level people can both  
understand and relate to

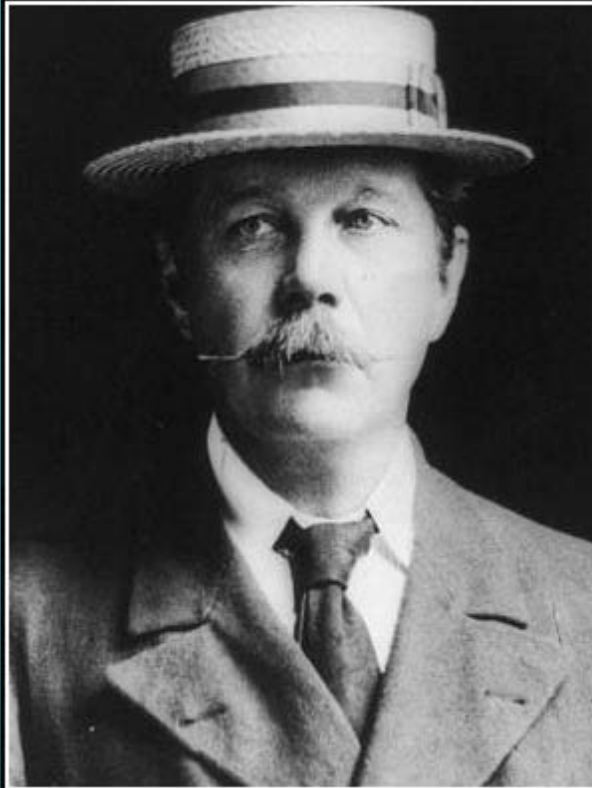


# REPLACE PLAIN FEAR WITH HEALTHY SKEPTICISM

Healthy skepticism: thinking critically when engaging with new content, ideas, or perspectives

- Question everything
- Play devil's advocate
- Requires additional evidence before accepting someone's claims as true/legitimate





Healthy scepticism is the basis of all  
accurate observation.

— *Arthur Conan Doyle* —

AZ QUOTES

# HEALTHY SKEPTICISM OUTSIDE OF INFOSEC

- Question material on web sites
- Question legitimacy of email
- Awareness of daily online risks
  - Training provided regularly, not just annually



## HEALTHY SKEPTICISM INSIDE INFOSEC

- Skepticism of fear-based marketing materials
- Speaking out against the negative hacker image
- Avoid relying on scary-sounding lingo e.g. "advanced persistent threat"



## NUANCED LEARNING REPLACES PLAIN FEAR

Nuanced learning: Involves a subtle or slight degree of difference, as in meaning, feeling, or tone; a gradation

- E.g. “Partner” in online safety vs. “catching” users’ mistakes
- Use language people understand and relate to vs. lingo
- Remove “us vs. them” perception
  - Who DIDN’T click the link?

## BACK TO BASICS – OPERATIONS

- Sensitive data
  - Who uses it?
  - Where does it live?
  - Asset location(s)?
- Remove easy ways into the network (why, hello RDP!)
- Log monitoring
- Fix simple things (XSS, SQL injection, etc.)







Don't let the goal of perfection become the  
enemy of good!

## BACK TO BASICS - EDUCATION

- Integrate security into CS/IT curriculum
  - Security foundation in all topics/courses
  - Prioritize security in CS/IT courses
- Goals:
  - Self-evaluate designs
  - Communicate security issues
  - Recognize need for further expertise

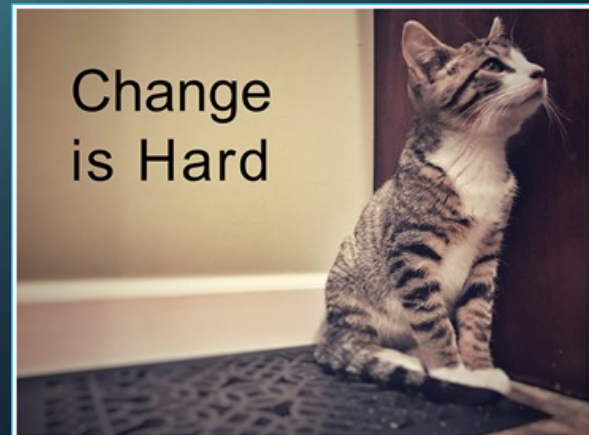




# Moving Forward

## AFFECTING CHANGE IS HARD

- “We’re so hopelessly broken” , “InfoSec is a disaster”
- No “eureka” moments yet...why?
- We’re trying to change people
  - Non-trivial to accomplish
    - E.g. healthy eating, exercise, quit smoking
  - Creatures of habit





“When change works...people who change have clear direction, ample motivation, and a supportive environment.”

“Small changes tend to snowball. But this is not the same thing as saying that change is easy.”

-Chip and Dan Heath, from Switch



# A DIFFERENT KIND OF CHANGE - PARTICIPATION

- Move away from the IT/InfoSec silo
  - Partner with the global community outside of IT/InfoSec
    - “Neighborhood watch”
  - Partner with the next generation
    - Less set in their ways
    - Already computer literate
    - Easier to teach, eager to learn



# HOW TO HAND OVER THE BATON

- Ways to partner with younger folks:
  - Bsides
  - CoderDojo
  - cyber camps
  - Odyssey of the Mind
  - Hak4Kidz
  - Mentoring



A decorative graphic on the left side of the slide, consisting of white lines and circles on a dark teal background, resembling a circuit board or a network diagram.

# Final Thoughts

## JUDGEMENT FREE ZONE

- Our #1 job is to educate
- Remember: *educate*, don't adjudicate
- Learn what they know; trade back your knowledge



QUESTIONS?





**BE THE  
CHANGE  
YOU WISH  
TO SEE IN THE WORLD**



@investigatorchi