

# What You Need to Know About InfoSec and Why You Should Care

Paul Gilzow



University of Missouri

# What You Need to Know About InfoSec and Why You Should Care

Submit questions to  
<https://2019.wpcampus.org/?p=734>

Paul Gilzow



University of Missouri

# TL;DR



University of Missouri

TL;DR

# Minimizing Risk



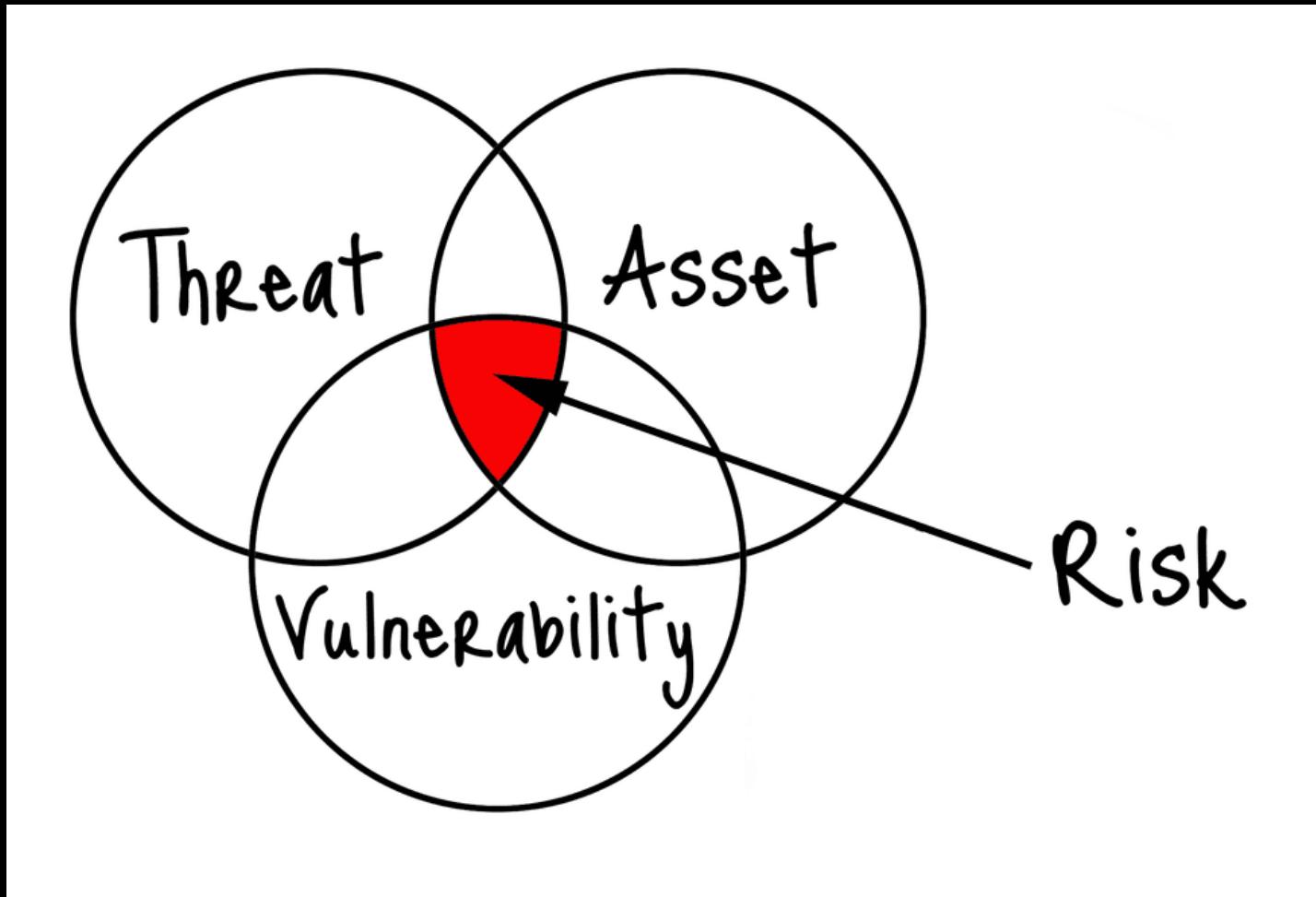
University of Missouri

# What is “Risk”?



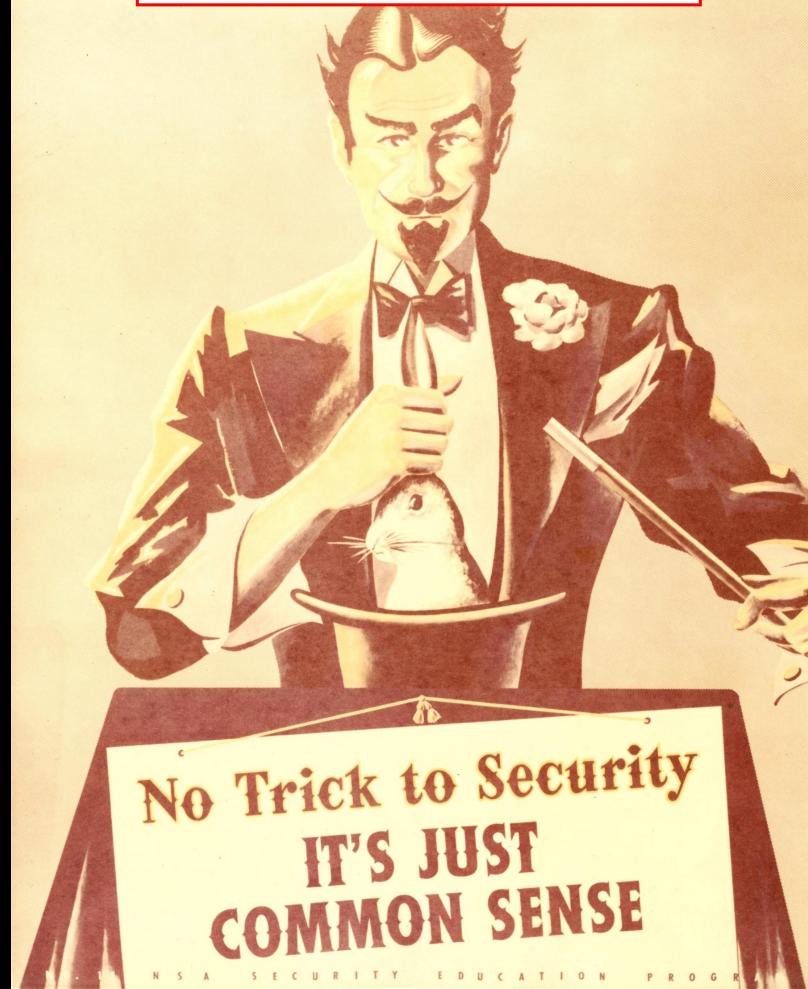
University of Missouri

# What is “Risk”?



# Asset

Approved for Release by NSA on 04-17-2018, FOIA Case # 83661



University of Missouri

# Asset

- An asset is what we are trying to protect



University of Missouri

# Asset

- An asset is what we are trying to protect
- People



University of Missouri

# Asset

- An asset is what we are trying to protect
- People
- Property



University of Missouri

# Asset

- An asset is what we are trying to protect
- People
- Property
- Information/Data



University of Missouri

# Threat



University of Missouri

# Threat

- Anything that represents a potential danger to an asset, whether deliberately or by accident



# Threat

- Anything that represents a potential danger to an asset, whether deliberately or by accident
- A threat is what we're trying to protect against

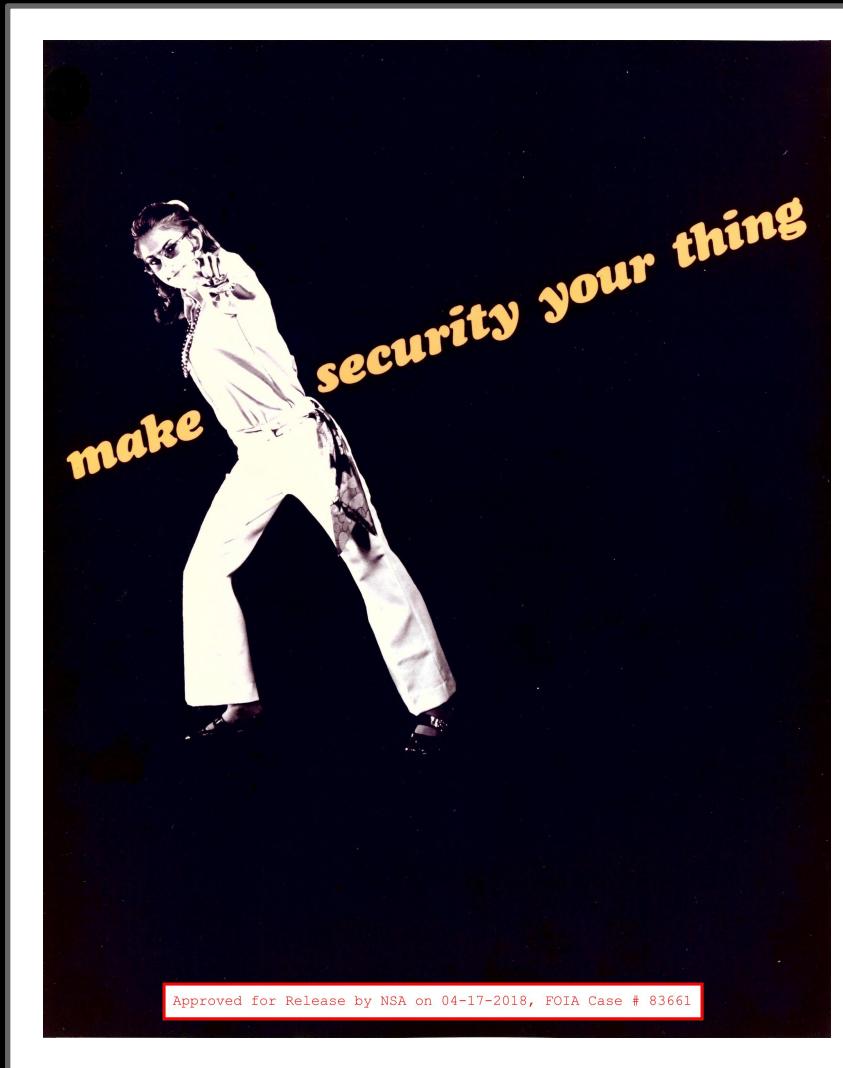


# Threat

- Anything that represents a potential danger to an asset, whether deliberately or by accident
- A threat is what we're trying to protect against
- *Threat Agent* is a group or individual who exploits a vulnerability to manifest or cause a threat to occur



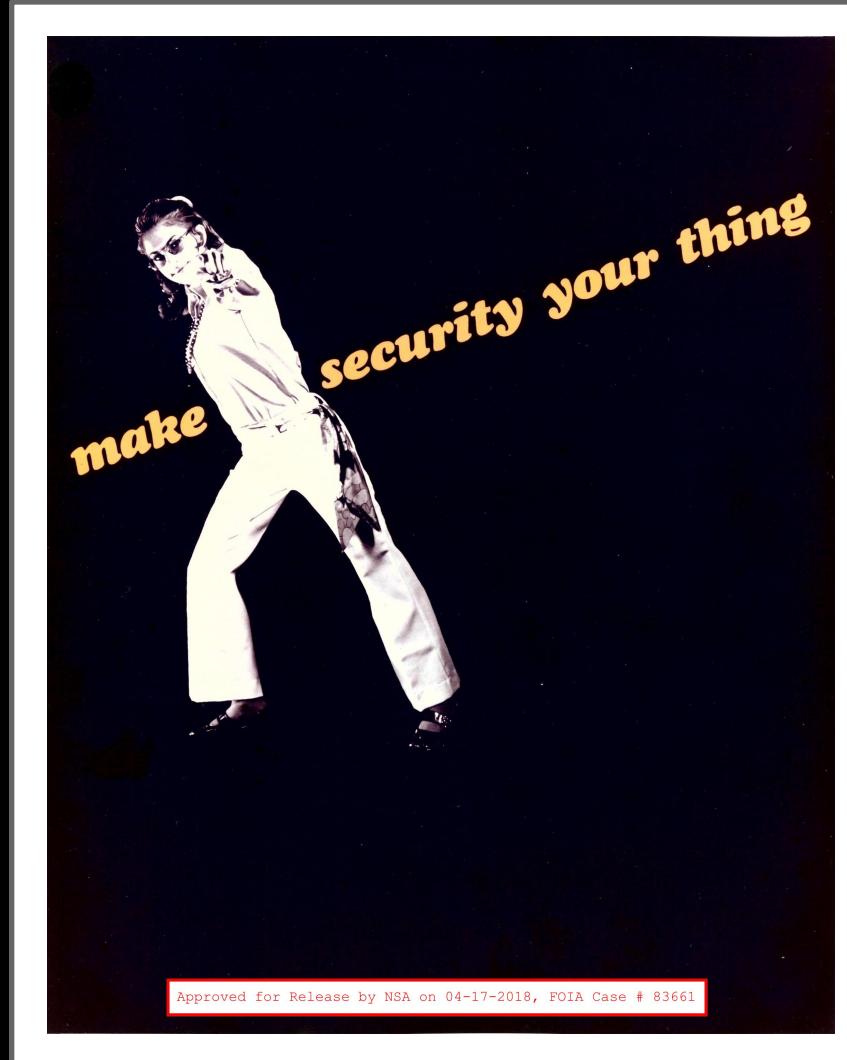
# Vulnerability



University of Missouri

# Vulnerability

- Weakness or holes/ gaps in security procedures or program that can be exploited by a threat to affect assets



Approved for Release by NSA on 04-17-2018, FOIA Case # 83661



University of Missouri

# What is “Risk”?



University of Missouri

# What is “Risk”?

- Asset = You



University of Missouri



University of Missouri

# What is “Risk”?

- Asset = You
- Vulnerability = Hole in your umbrella



University of Missouri

# What is “Risk”?

- Asset = You
- Vulnerability = Hole in your umbrella
- Threat = Getting wet



University of Missouri

# What is “Risk”?

- Asset = You
- Vulnerability = Hole in your umbrella
- Threat = Getting wet
- Risk = Rain



University of Missouri

# What is “Risk”?

The potential for loss, damage or destruction of an asset(s) as a result of a threat exploiting a vulnerability multiplied by the impact of the threat occurring



# Higher Education Assets



# Higher Education Assets

- Network bandwidth and availability



# Higher Education Assets

- Network bandwidth and availability
- Computing power



# Higher Education Assets

- Network bandwidth and availability
- Computing power
- SEO reputation



# Higher Education Assets

- Network bandwidth and availability
- Computing power
- SEO reputation
- Brand and reputation



# Higher Education Assets

- Network bandwidth and availability
- Computing power
- SEO reputation
- Brand and reputation
- Social Media accounts



# Higher Education Assets



# Higher Education Assets

- Personally Identifiable Information (PII) / Sensitive Personal Information (SPI)



# Higher Education Assets

- Personally Identifiable Information (PII) / Sensitive Personal Information (SPI)
- Protected Health Information (PHI)



# Higher Education Assets

- Personally Identifiable Information (PII) / Sensitive Personal Information (SPI)
- Protected Health Information (PHI)
- Confidential Intellectual Property



# Higher Education Assets

- Personally Identifiable Information (PII) / Sensitive Personal Information (SPI)
- Protected Health Information (PHI)
- Confidential Intellectual Property
- Export Controlled Data



# Higher Education Assets

- Personally Identifiable Information (PII) / Sensitive Personal Information (SPI)
- Protected Health Information (PHI)
- Confidential Intellectual Property
- Export Controlled Data
- National Security Interest (NSI)



# Know Your Assets



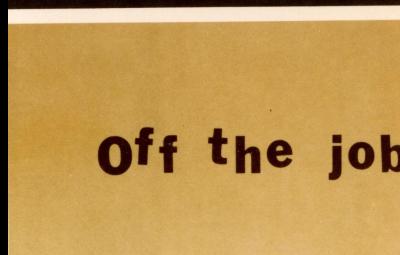
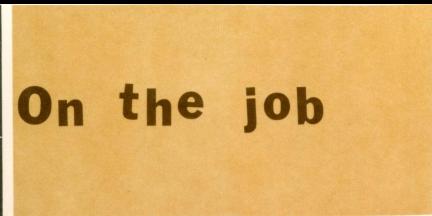
**Off the job**

**SECURITY is up to you**

Approved for Release by NSA on 04-17-2018, FOIA Case # 83661

# Know Your Assets

- You can't protect what you don't know you have

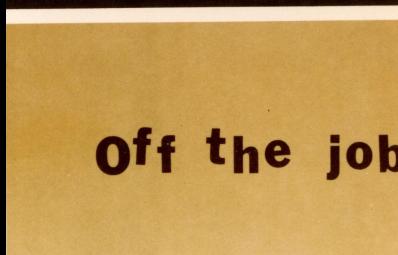
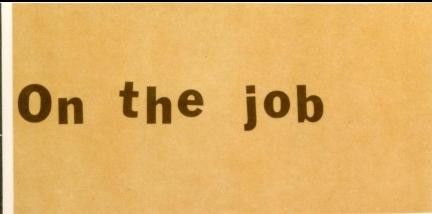
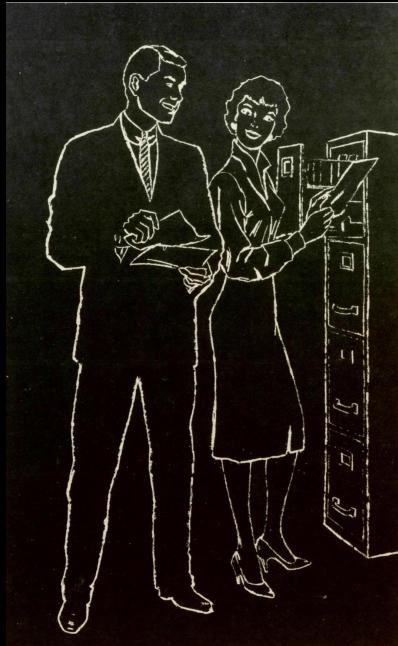


**SECURITY is up to you**

Approved for Release by NSA on 04-17-2018, FOIA Case # 83661

# Know Your Assets

- You can't protect what you don't know you have
- Know your assets intimately



**SECURITY is up to you**

Approved for Release by NSA on 04-17-2018, FOIA Case # 83661

# Defense-in-Depth



# Defense-in-Depth

- Strategy of protection using a series of defensive mechanisms such that if one mechanism fails, another will already be in place to thwart an attack.



# Minimize the Attack Surface



University of Missouri

# Minimize the Attack Surface

- The sum of all paths for data/commands into and out of the application



# Minimize the Attack Surface

- The sum of all paths for data/commands into and out of the application
- Plus all of the code that protects those paths



# Minimize the Attack Surface

- The sum of all paths for data/commands into and out of the application
- Plus all of the code that protects those paths
- Plus all of the data used in the application



# Minimize the Attack Surface

- The sum of all paths for data/commands into and out of the application
- Plus all of the code that protects those paths
- Plus all of the data used in the application
- Plus all of the code that protects this data



# What is “Attack Surface”?



University of Missouri

# Principle of Least Privilege

# Principle of Least Privilege

- Grant necessary permissions required to perform the intended activities

# Principle of Least Privilege

- Grant necessary permissions required to perform the intended activities
- For a limited time

# Principle of Least Privilege

- Grant necessary permissions required to perform the intended activities
- For a limited time
- But with the *minimum* rights required for the task(s)

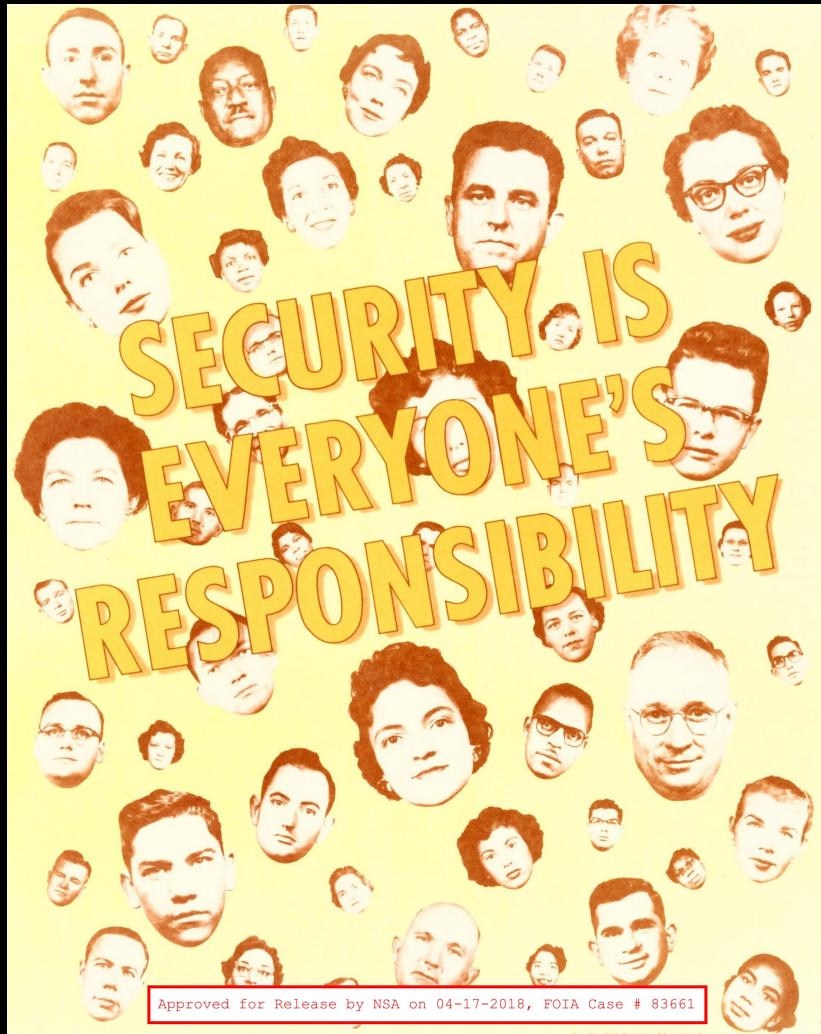
# Principle of Least Privilege

- Grant necessary permissions required to perform the intended activities
- For a limited time
- But with the *minimum* rights required for the task(s)
- Removing permissions when no longer needed

# Be Paranoid

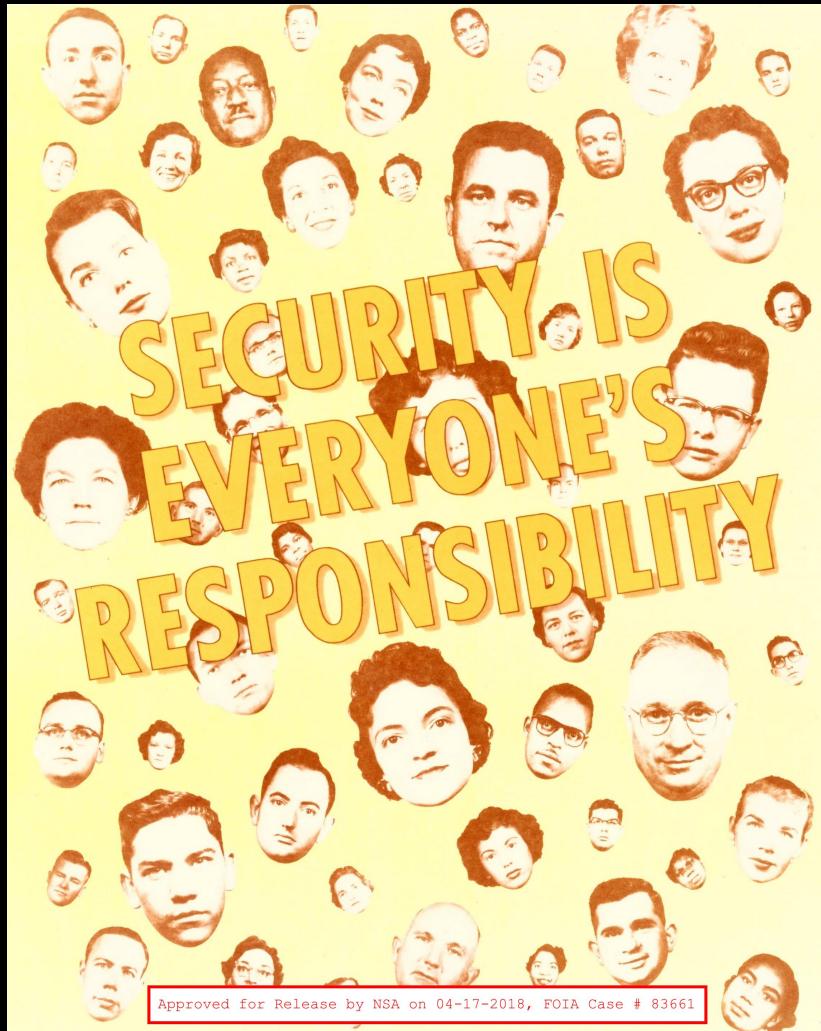


# Ok, How About: “Be Skeptical”



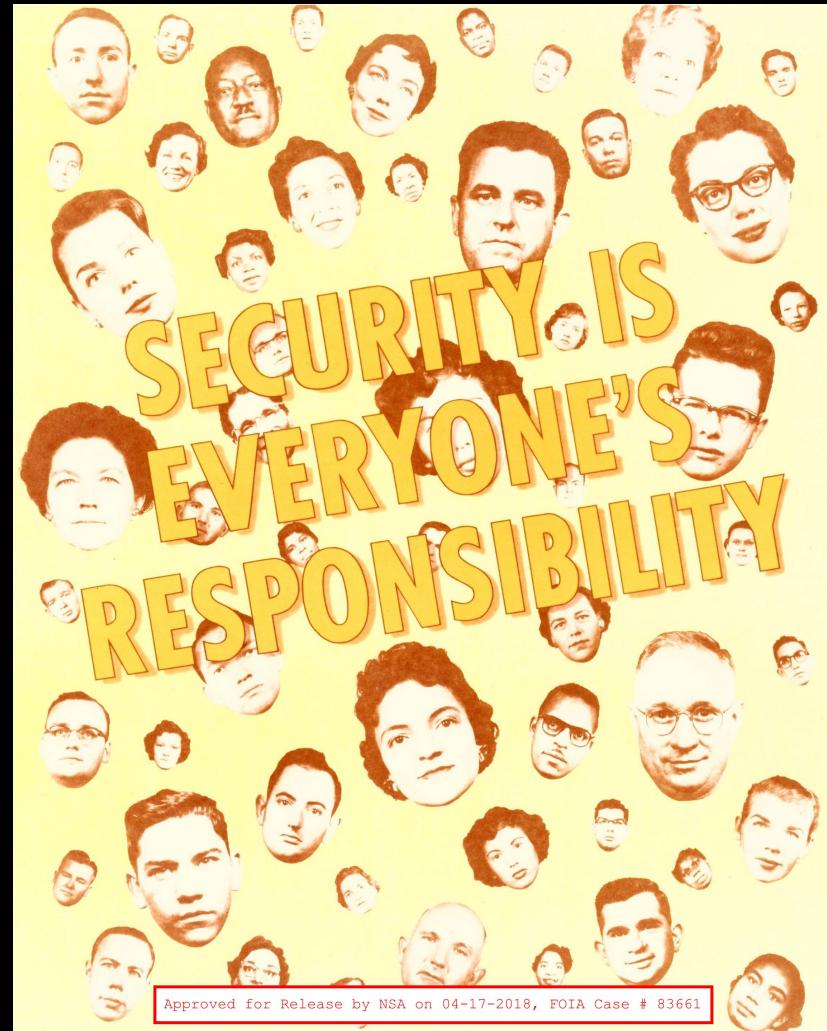
# Ok, How About: “Be Skeptical”

- *Treat all third party code/  
data as tainted and hostile*



# Ok, How About: “Be Skeptical”

- *Treat all third party code/ data as tainted and hostile*
- Humans remain the weakest link in the InfoSec armor



Security is a continual process;  
you're never “finished”

# Your Challenge

Always be thinking in terms of  
how you can reduce risk

**Any way you look at it...**



**SECURITY**

**IS**

**YOUR**

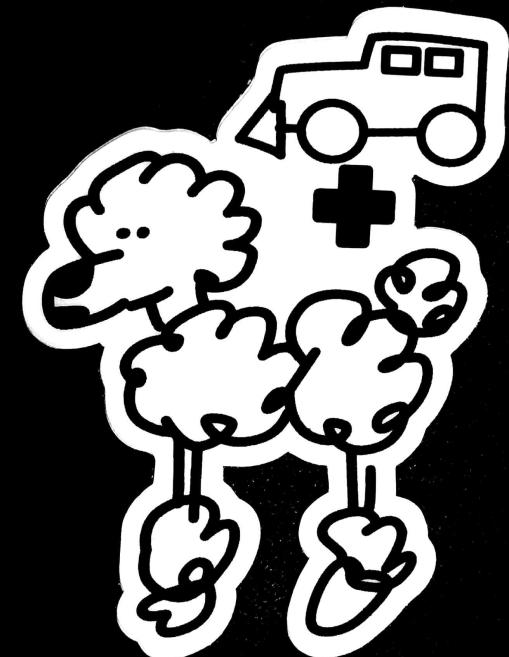
**RESPONSIBILITY**

Approved for Release by NSA on 04-17-2018, FOIA Case # 83661

NSA SECURITY EDUCATION PROGRAM 35

# Paul Gilzow

- Programmer/Analyst / Security Analyst at the University of Missouri
- Contact
  - [gilzow@missouri.edu](mailto:gilzow@missouri.edu)
  - @gilzow on twitter
  - <https://fb.me/gilzow>
  - <https://profiles.wordpress.org/gilzow>
  - <https://github.com/gilzow/>



# Submit Session Feedback!

You'll win points towards the conference game and you'll be entered for a door prize!

<https://2019.wpcampus.org/?p=734>

