

# IT Risk is Business Risk: Find and Manage Yours

May 5, 2015

The webinar will start at 10:00 am CT



**Ryan Burrus**  
Senior Technology Consultant

# Administration



**If you need HRCI/CPE credit, please participate in all polls throughout the presentation.**

#AGHUwebinars

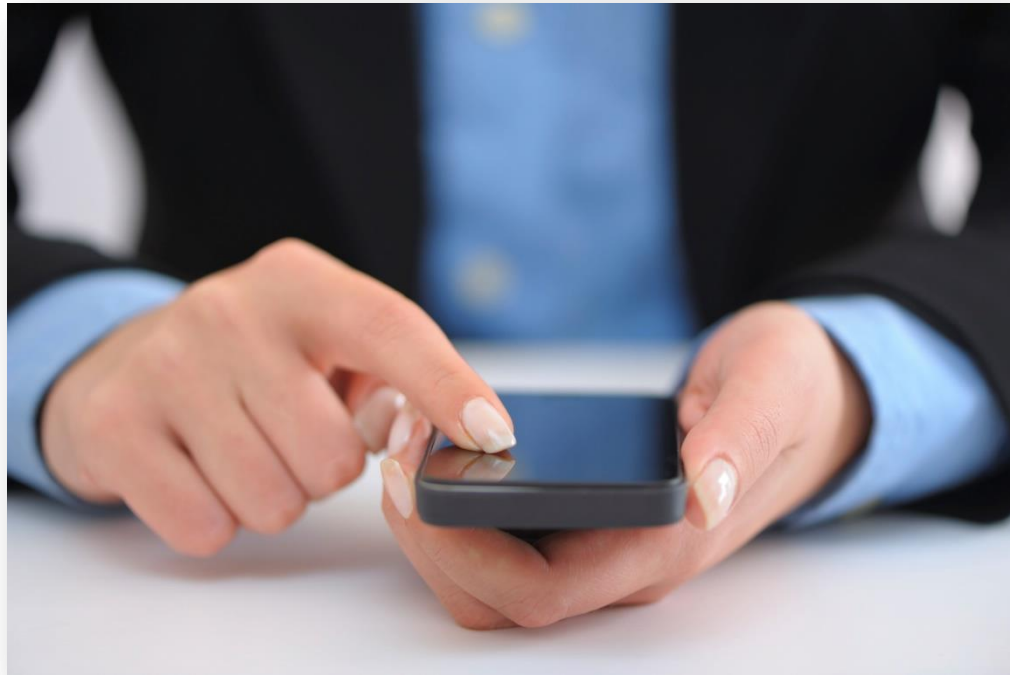
# Administration



**A recording of today's webinar will be emailed for your reference or to share with others.**

**#AGHUwebinars**

# Administration



**For best quality, call in by phone instead of using your computer speakers.**

#AGHUwebinars



# Administration



**To ask questions during the presentation, use the questions box on the right side of your screen.**

#AGHUwebinars

# Administration



**Please provide your feedback at the end of today's presentation.**

# IT Risk Management

**Who owns risk?**





**Sure,  
it's **safe!****









password







# NEWS

## MASSIVE DATA BREACH

Security Breach Affects Thousands

LINDMEYER.



Schülerhändin erschöpft Kasse

Wortspiele:  
Das Münchner  
Literaturfestival





OFFICE OF THE  
**CIO**

601







**“Who owns loss  
owns **risk.**”**

– *Dr. Jack Freund*  
IT Risk Manager,  
TIAA-CREF



**Sorry John,  
but this was **your**  
**responsibility.****

**CEO**



**IT Risk is  
Business Risk**

## AGENDA:

1. Why does this **matter?**
2. What **needs** to **change?**
3. Where do we **start?**





# Polling Question #1

---

## AGENDA:

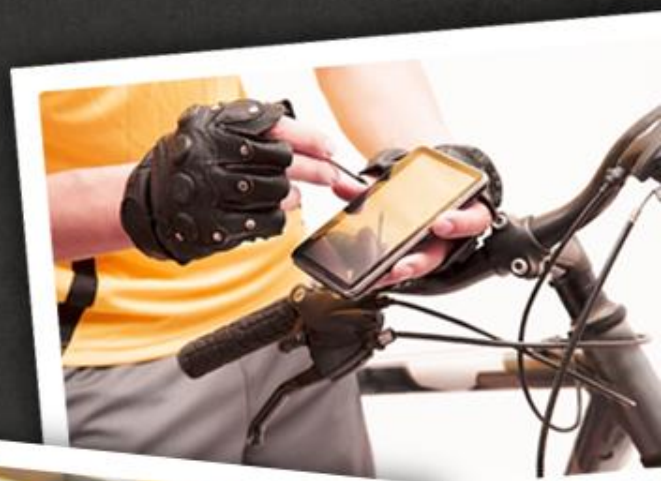
1. Why does this **matter?**
2. What **needs** to **change?**
3. Where do we **start?**

**Why does this  
matter to me?**





Technology is **changing**  
**the way we live,** learn,  
play, and work.



Most organizations **rely on**  
**technology** for their critical  
business processes.







**Technology  
presents  
opportunity.**

**But opportunity  
can have risk.**

# 2.5 Billion



**Exposed records** as a result  
of data breach **from 2009 to 2013.**



# An Additional 904 Million



## In the first three quarters of 2014.



# Records Breached in 2014:

# 1,023,108,267



Records Breached in 2014:  
**1,023,108,267**



Number of  
Breach  
Incidents:  
**1,541**

Records Breached in 2014:  
**1,023,108,267**

**78%**  
Increase in  
Breached Records  
from 2013



Number of  
Breach  
Incidents:  
**1,541**



Data records were  
**lost or stolen** with  
the following frequency:



2,803,036  
**Per Day**

Data records were  
**lost or stolen** with  
the following frequency:



2,803,036  
Per Day



116,793  
Per Hour

Data records were  
**lost or stolen** with  
the following frequency:



2,803,036  
Per Day



116,793  
Per Hour



1,947  
Per Minute



Data records were  
**lost or stolen** with  
the following frequency:



2,803,036  
Per Day



116,793  
Per Hour



1,947  
Per Minute



32  
Per Second

# NUMBER OF **BREACH INCIDENTS** BY SOURCE:

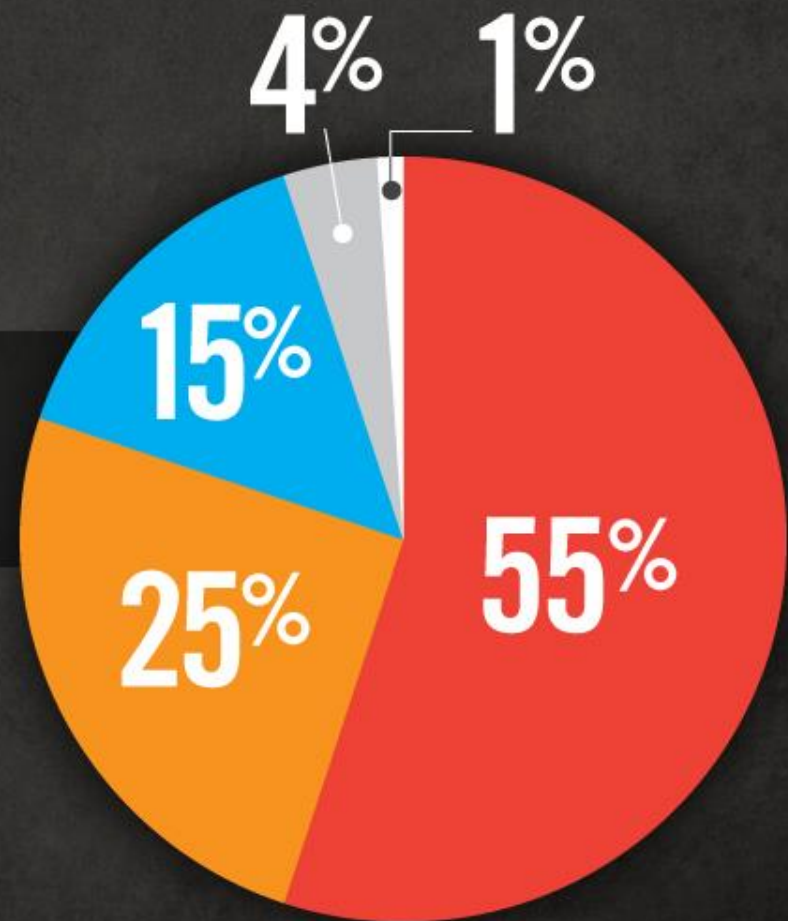
■ MALICIOUS OUTSIDER

■ ACCIDENTAL LOSS


■ MALICIOUS INSIDER

■ STATE SPONSORED

■ HACKTIVIST



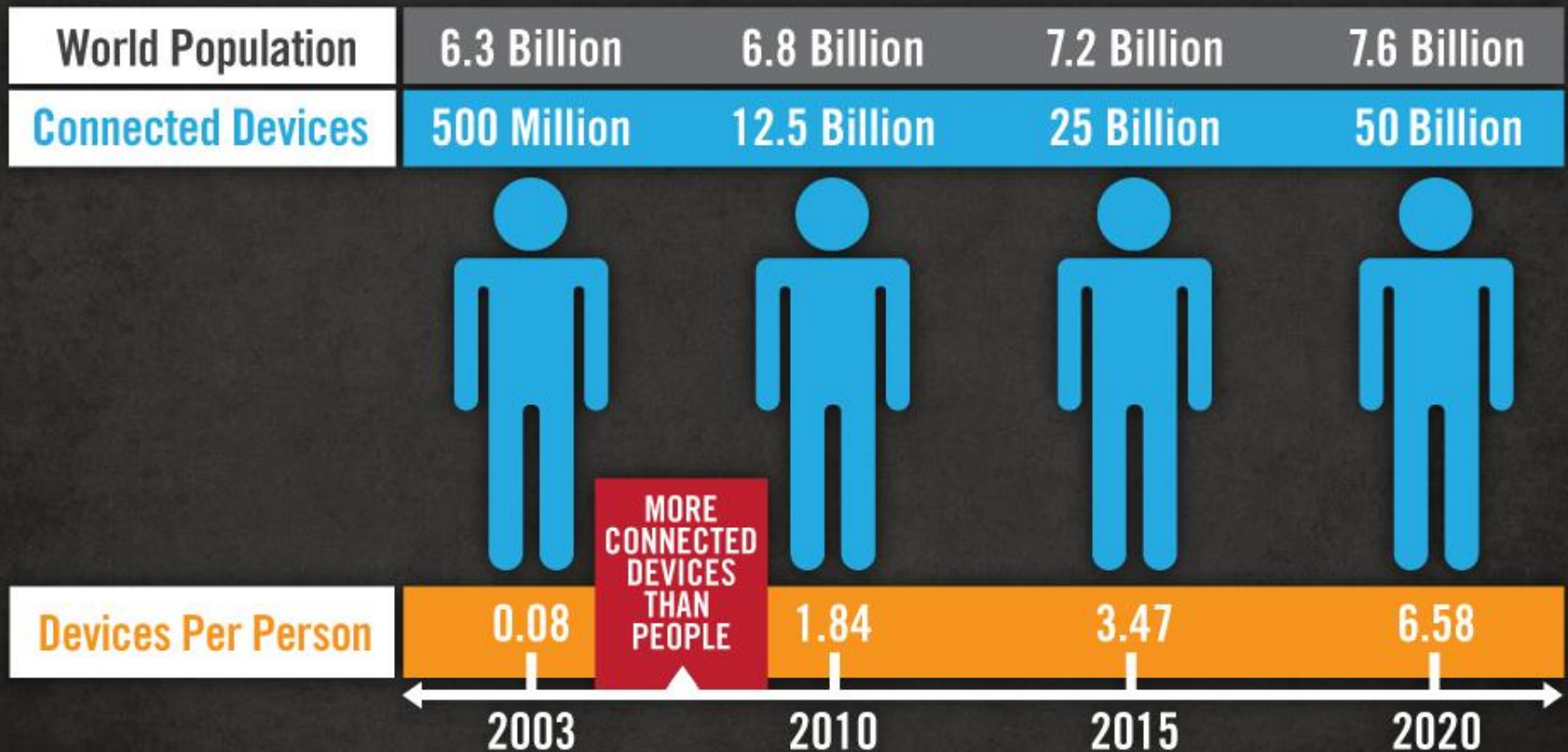




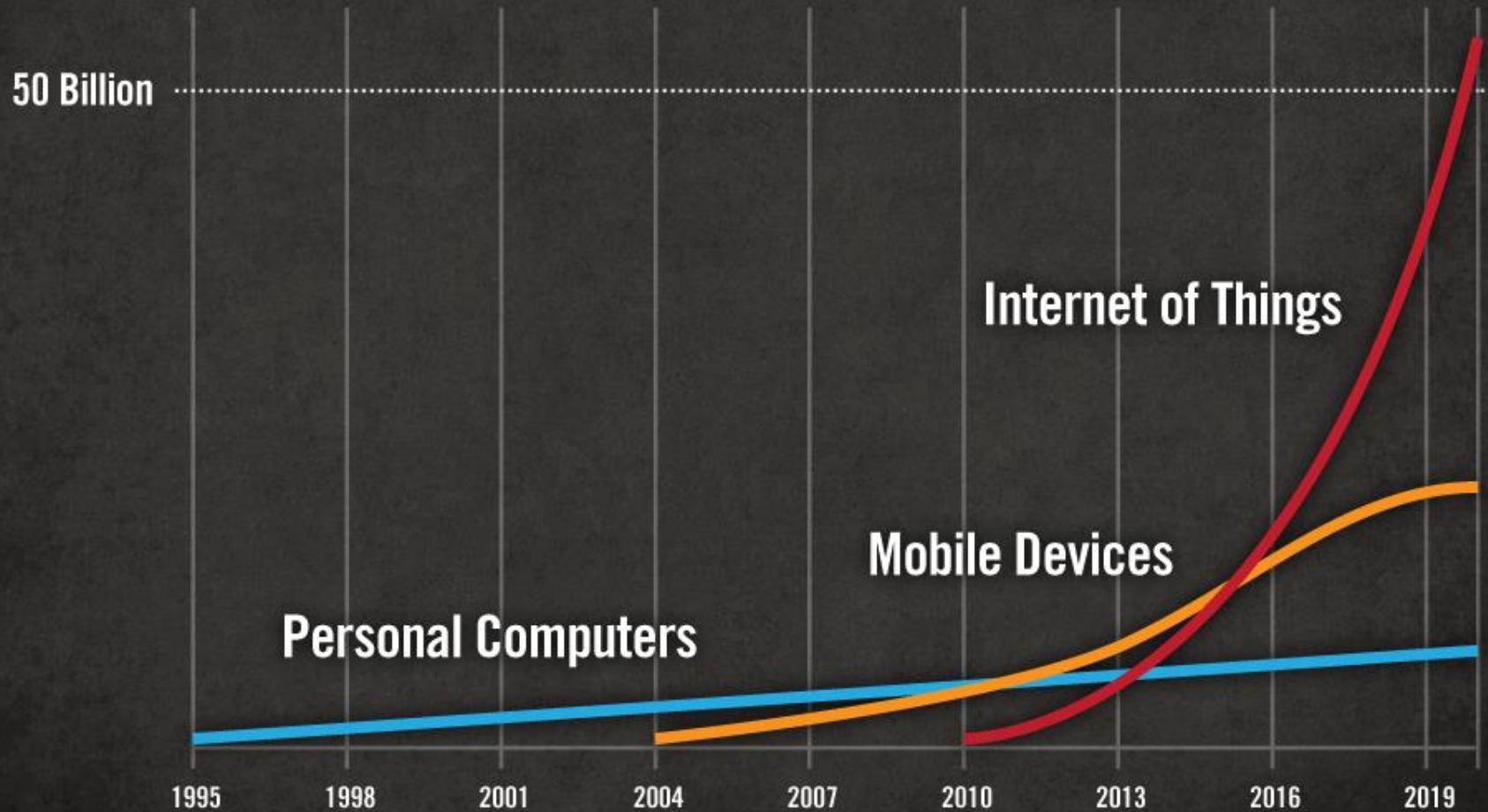
**\$3.06**  
**TRILLION**

**Total**  
**global impact**  
**of cybercrime.**

# The Internet of Things



# Global Internet Connected Devices



Sources: McAfee, based on research by BI Intelligence, IDC, and Intel.





# Polling Question #2

---

## AGENDA:

1. Why does this matter?
2. What **needs** to **change**?
3. Where do we start?



**Okay, I'm  
convinced!**  
**What needs to  
change?**



Adjust your **perspective.**

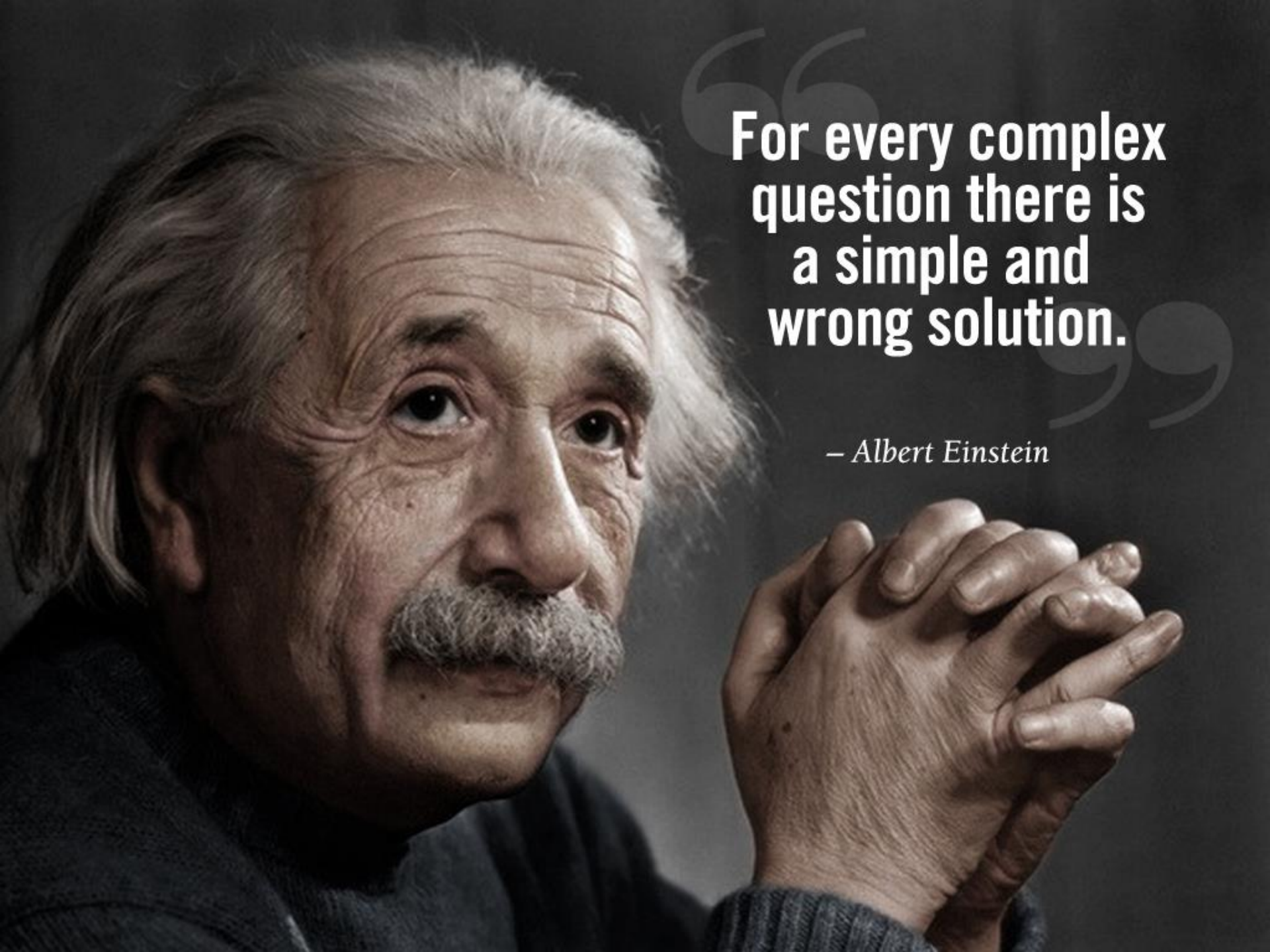






If you think technology can  
solve your security problems,  
then **you don't understand**  
the problems and you don't  
understand the technology.

— Bruce Schneier

A close-up portrait of Albert Einstein, showing his characteristic wild white hair and mustache. He is looking slightly to the right with a thoughtful expression. His hands are clasped together in front of him. The background is dark and out of focus.

**For every complex  
question there is  
a simple and  
wrong solution.**

*– Albert Einstein*



A man in a dark pinstripe suit is seen from the side, holding a wooden baton in his right hand and gesturing with his left. He is positioned in front of a dark, textured background. Overlaid on the background is the text 'PEOPLE PROCESS TECHNOLOGY' in large, bold, sans-serif capital letters. 'PEOPLE' is white, 'PROCESS' is orange, and 'TECHNOLOGY' is light blue. The baton is positioned vertically, passing through the 'P' of 'PEOPLE' and the 'T' of 'TECHNOLOGY'.

**PEOPLE**  
**PROCESS**  
**TECHNOLOGY**

**orchestrate**

*verb*

**To organize or plan  
(something that is complicated)**

# Minimum Table Stakes

## A Few Examples:

- Identity & Access Controls
- Network & Endpoint Protection
- Training & Employee Awareness





**CONFIDENTIAL**

Psst!

Email is like  
a postcard.

Don't tell  
anyone!

**CLASSIFIED**

POST  
CARD



John Doe  
1234 Main Street  
Anytown, USA



Name:  
idk204  
Pass:  
p455wrd

Username



bad

Password



idea\_

Login

Name:  
bigdog3  
Pass:  
Y8~46!2

sderr  
Pass:  
bond55

Name:  
okay55  
Pass:  
Pr3897

Name:  
johnna  
Pass:  
x0532jrt

“Amateurs  
hack **systems.**

Professionals  
hack **people.**”

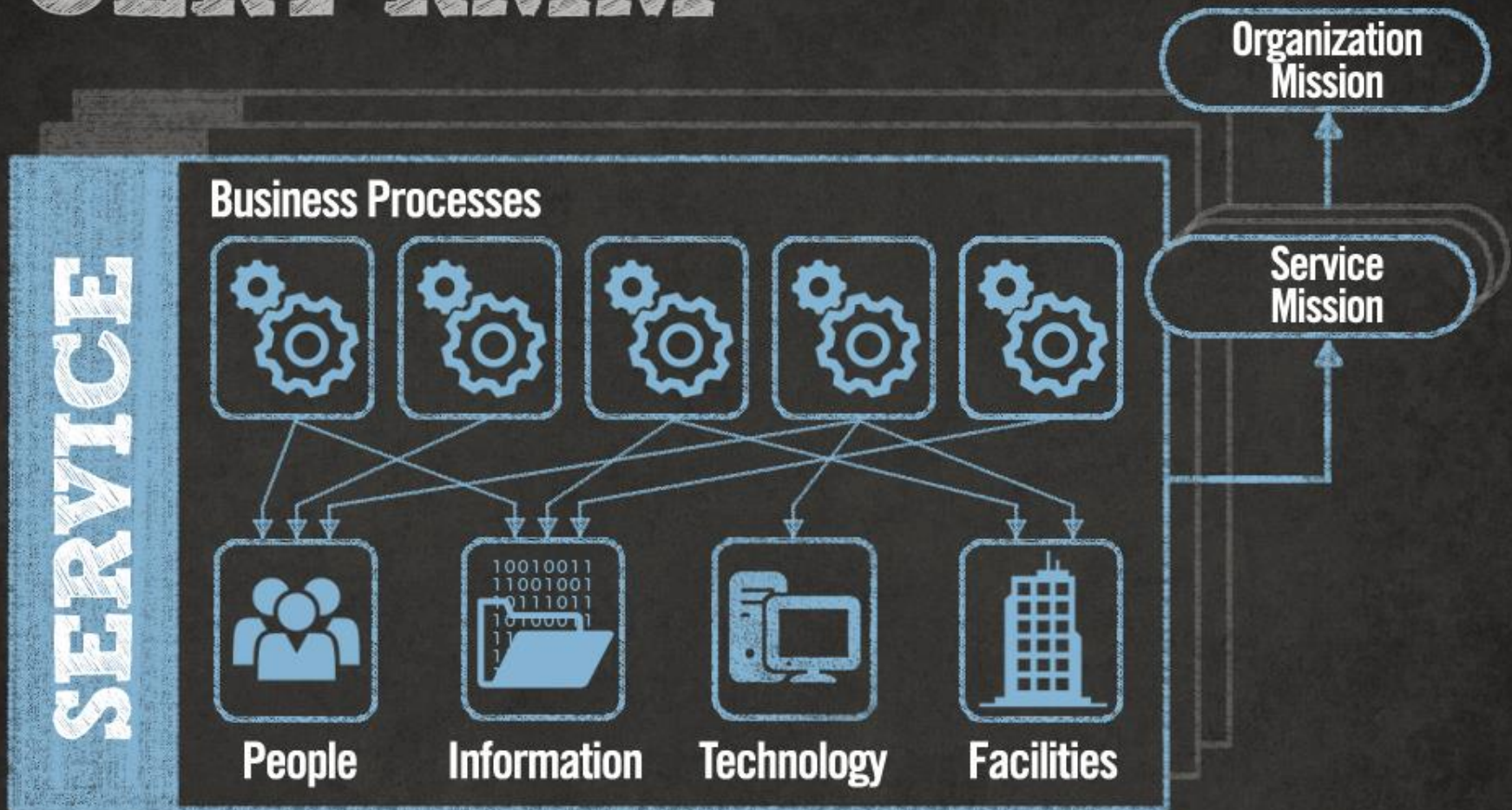
– Bruce Schneier



**Think differently.**

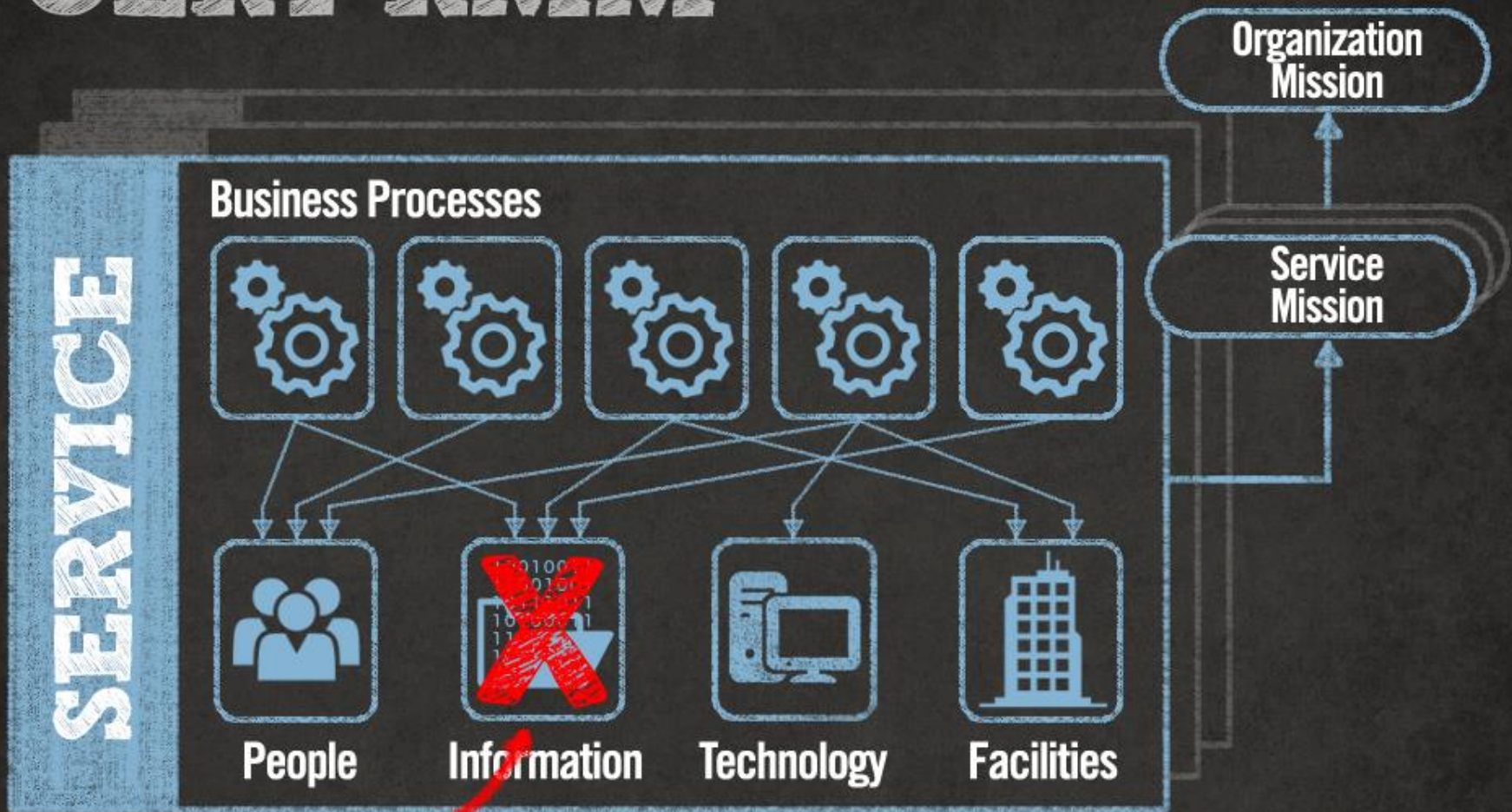


# CERT-RMM





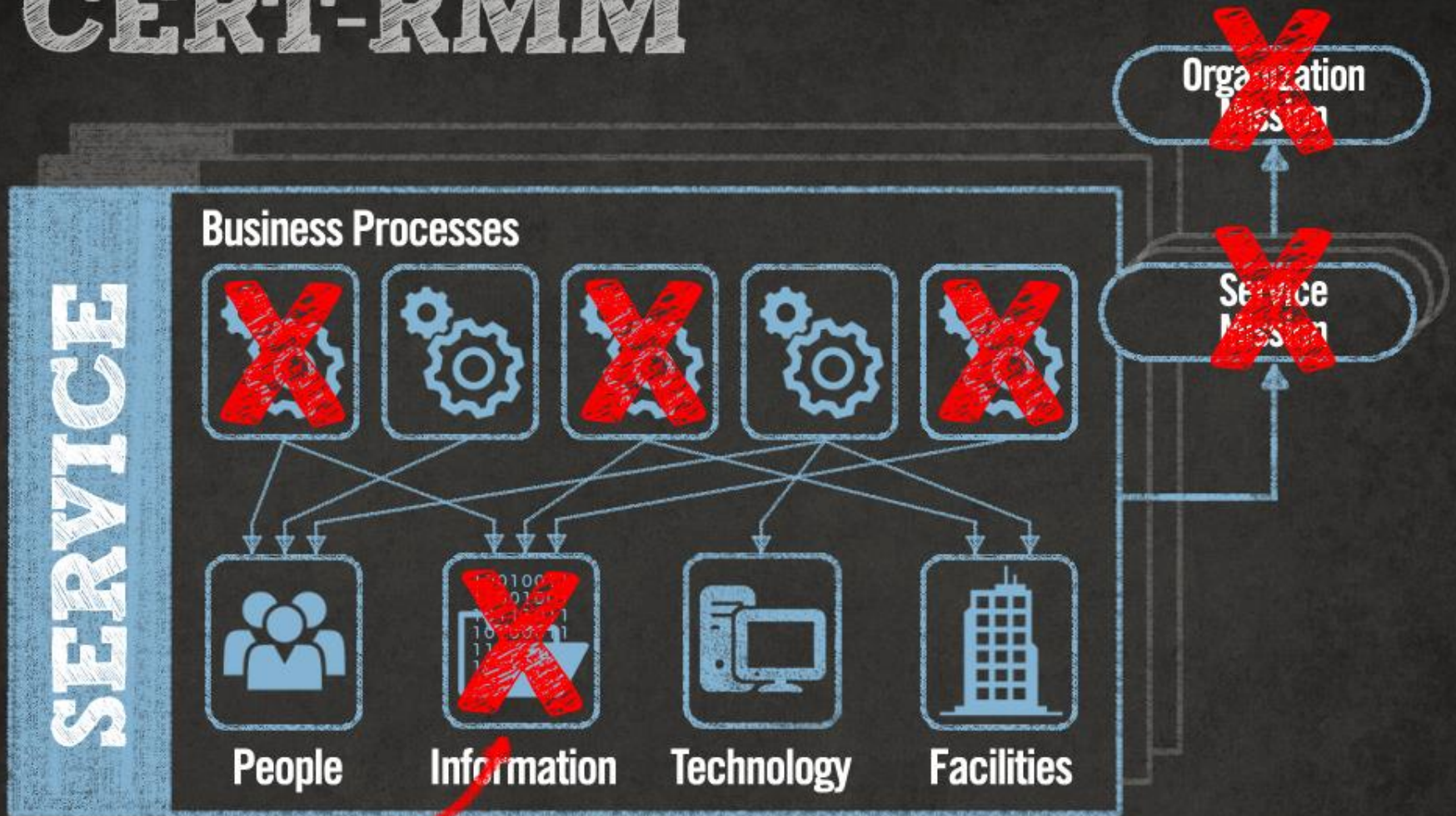
# CERT-RMM



Asset Disruption



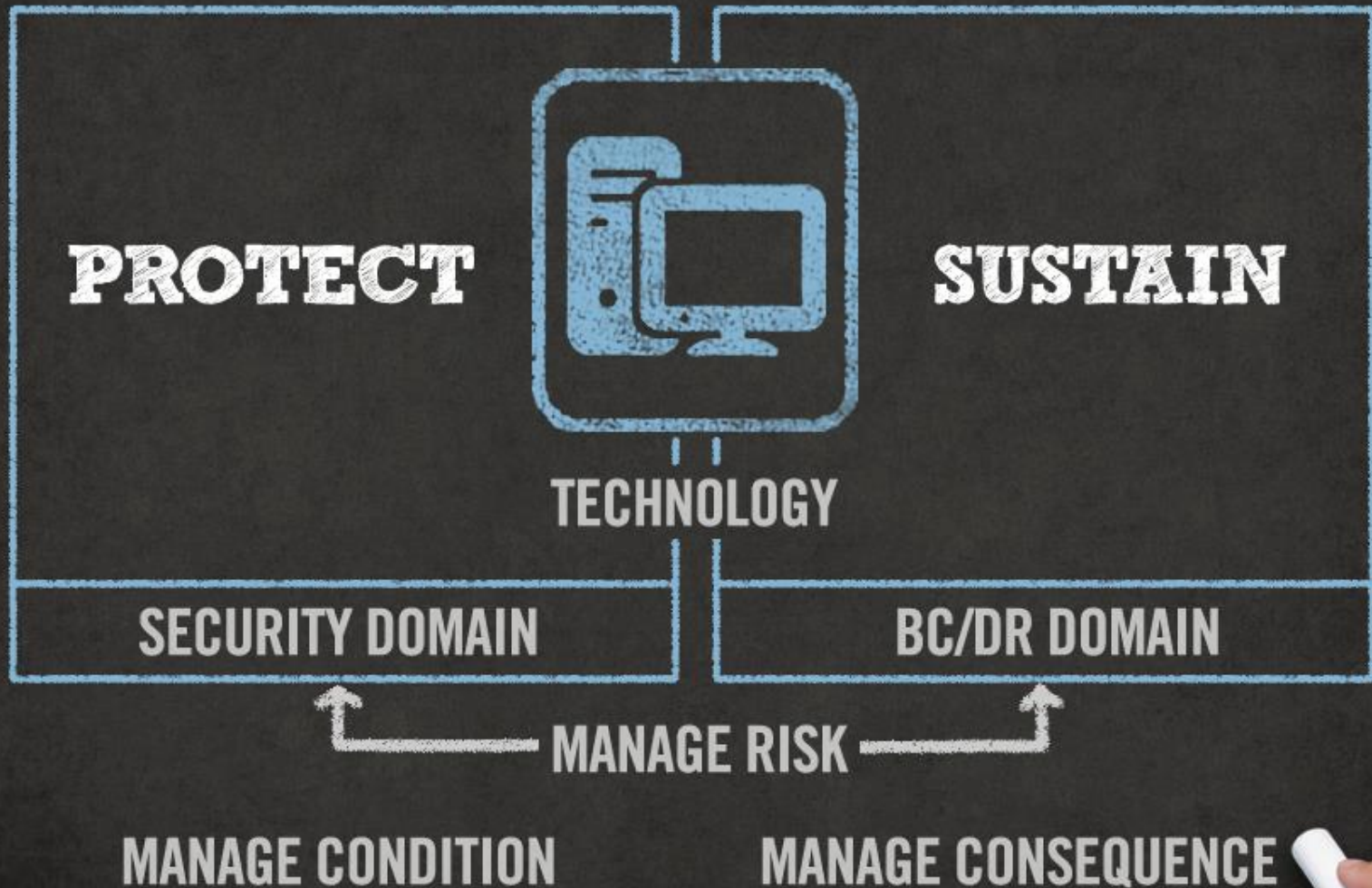
# CERT-RMM



Asset Disruption



# CERT-RMM



*Pro*  
~~Reactive~~



**Being **compliant** isn't  
the same as **being secure.****



**Don't wait** for the event.

**TIME** FOR  
ACTION



Move  
**you** from  
a state of  
**awareness** to  
a state of **action.**





How do you **approach** other  
business **opportunities**?







# Polling Question #3

---

## AGENDA:

1. Why does this **matter?**
2. What **needs** to **change?**
3. Where do we **start?**

**That sounds**  
**reasonable!**  
**But where do**  
**we start?**







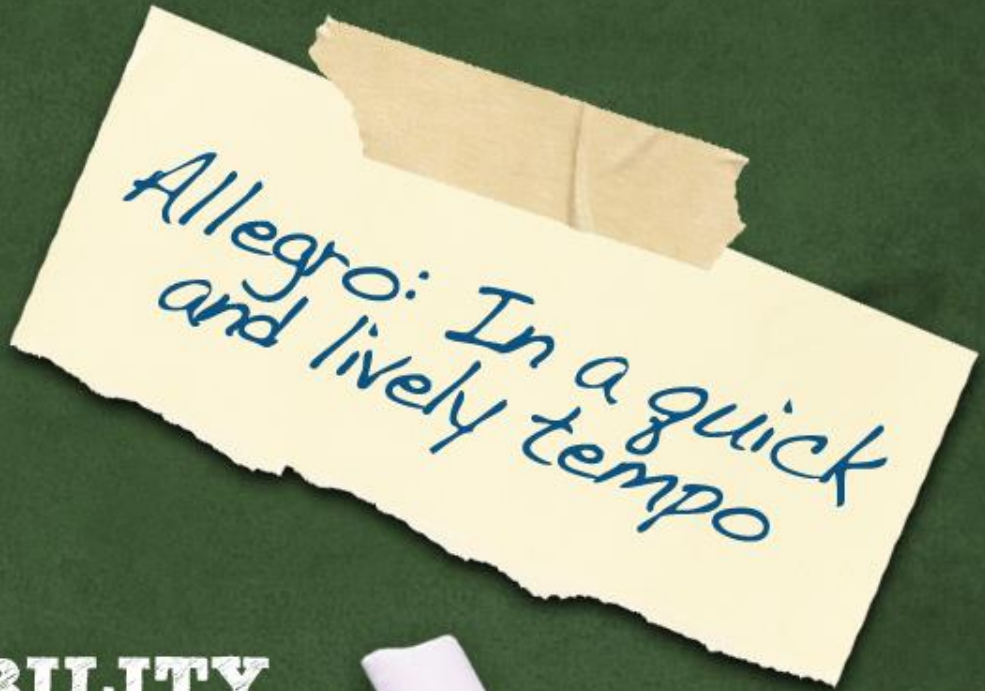
**Risk Assessments  
are the cornerstone  
of any risk  
management system.**







# OPERATIONALLY CRITICAL THREAT ASSET VULNERABILITY EVALUATION



## ESTABLISH DRIVERS

1

Establish Risk Measurement Criteria

## PROFILE ASSETS

2

Develop Information Asset Profile

3

Identify Information Asset Containers

## IDENTIFY THREATS

4

Identify Areas of Concern

5

Identify Threat Scenarios

## IDENTIFY & MITIGATE RISKS

6

Identify Risks

7

Analyze Risks

8

Select Mitigation Approach

OCTAVE  
allegro



## ESTABLISH DRIVERS

1

Establish Risk Measurement Criteria

## PROFILE ASSETS

2

Develop Information Asset Profile



3

Identify Information Asset Containers

## IDENTIFY THREATS

4

Identify Areas of Concern



5

Identify Threat Scenarios

## IDENTIFY & MITIGATE RISKS

6

Identify Risks



7

Analyze Risks



8

Select Mitigation Approach

OCTAVE  
allegro

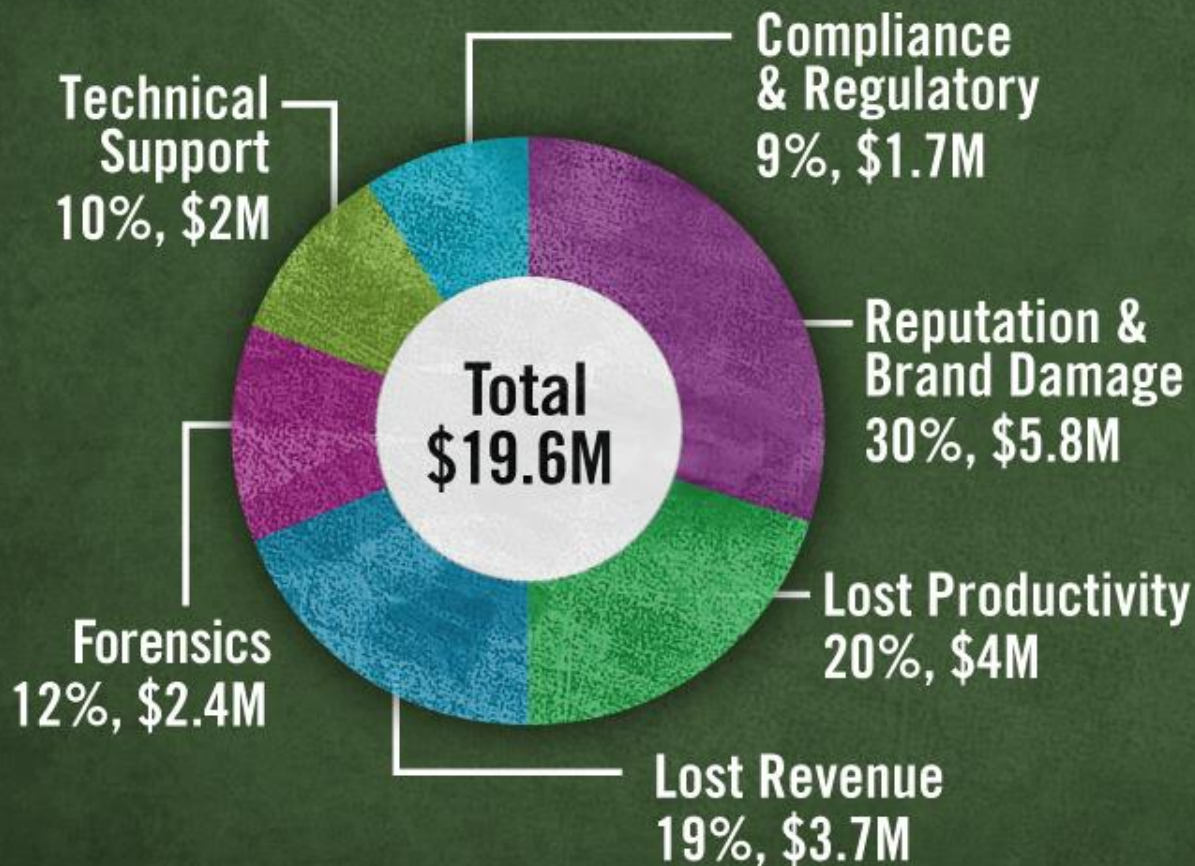


# Where would it **hurt** most?

What **high-impact event** could  
put you out of business?

- Reputation & Brand Image
- Lost Productivity
- Lost Revenue
- Compliance & Regulatory
- Safety, Life & Health

# Financial Impact by Cost Category



Business costs  
make up  
more than

**75%**

of the financial  
consequences  
of business  
continuity and  
IT security  
failures.



ESTABLISH  
DRIVERS

1

Establish Risk  
Measurement  
Criteria

PROFILE  
ASSETS

2

Develop  
Information  
Asset Profile



3

Identify  
Information  
Asset Containers

IDENTIFY  
THREATS

4

Identify  
Areas  
of Concern



5

Identify  
Threat  
Scenarios

IDENTIFY &  
MITIGATE RISKS

6

Identify  
Risks



7

Analyze  
Risks



8

Select  
Mitigation  
Approach

OCTAVE  
allegro







**Hey Joe,**  
**Susan said you could**  
**explain the X73**  
**process to me...**  
**Joe?**





ESTABLISH  
DRIVERS

1

Establish Risk  
Measurement  
Criteria

PROFILE  
ASSETS

2

Develop  
Information  
Asset Profile



3

Identify  
Information  
Asset Containers

IDENTIFY  
THREATS

4

Identify  
Areas  
of Concern



5

Identify  
Threat  
Scenarios

IDENTIFY &  
MITIGATE RISKS

6

Identify  
Risks



7

Analyze  
Risks



8

Select  
Mitigation  
Approach

OCTAVE  
allegro





**Ahhh,**  
**No boss...no cellphone...**  
**no X73. Just sun, water**  
**and drinks with little**  
**umbrellas.**





**If we don't  
complete the X73  
process by 3:00, we'll  
start losing orders!**  
**Where's Joe?!**



ESTABLISH  
DRIVERS

1

Establish Risk  
Measurement  
Criteria

PROFILE  
ASSETS

2

Develop  
Information  
Asset Profile



3

Identify  
Information  
Asset Containers

IDENTIFY  
THREATS

4

Identify  
Areas  
of Concern



5

Identify  
Threat  
Scenarios

IDENTIFY &  
MITIGATE RISKS

6

Identify  
Risks



7

Analyze  
Risks



8

Select  
Mitigation  
Approach

OCTAVE  
allegro









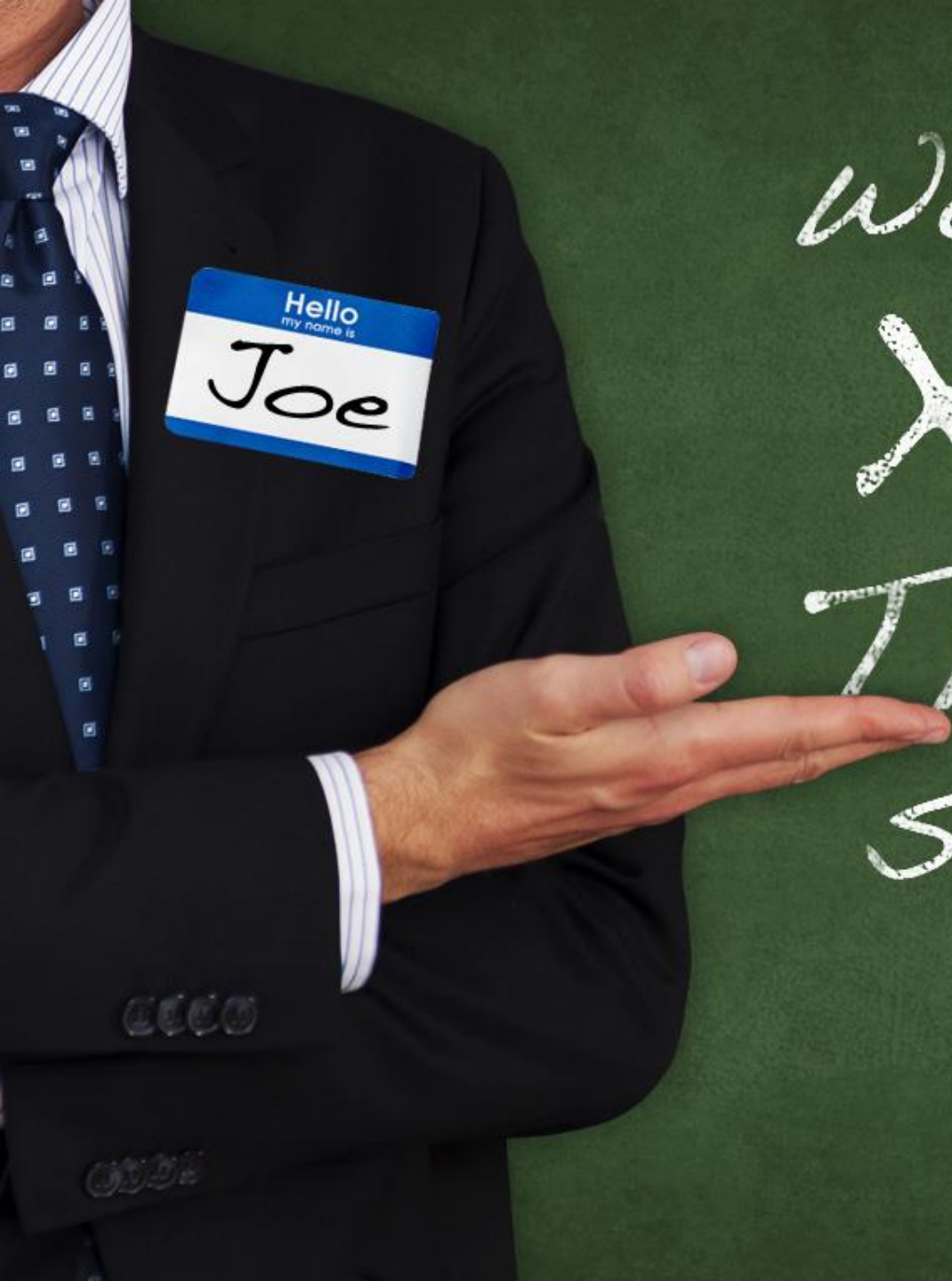












Welcome!

X73

Training  
session  
today





**Okay Sally,**  
**in order to take  
over my old job, here  
are some things you  
might need to know...**

## ESTABLISH DRIVERS

1

Establish Risk Measurement Criteria

## PROFILE ASSETS

2

Develop Information Asset Profile

3

Identify Information Asset Containers

## IDENTIFY THREATS

4

Identify Areas of Concern

5

Identify Threat Scenarios

## IDENTIFY & MITIGATE RISKS

6

Identify Risks

7

Analyze Risks

8

Select Mitigation Approach

OCTAVE  
allegro







**Simplicity** is  
the ultimate  
sophistication.

– Leonardo DaVinci



## AGENDA:

1. Why does this **matter?**
2. What **needs** to **change?**
3. Where do we **start?**

**IT Risk is  
Business Risk**





# Polling Question #4

---



YOU ARE HERE

**Something to consider...**



“Wired people should  
**know something**  
about wires.”

– Neal Stephenson

# Thank you!

## Ryan Burrus

Senior Technology Consultant



[ryan.burrus@aghlc.com](mailto:ryan.burrus@aghlc.com)



[Ryan's LinkedIn Account](#)



316.291.4168



Questions **NOT** related to today's content?

[mike.ditch@aghlc.com](mailto:mike.ditch@aghlc.com)

Check out our other webinars!

[AGHUniversity.com](http://AGHUniversity.com)

#AGHUwebinars