Why organizations keep getting breached.... *Still, in 2015.*

Kevin Beaver, CISSP
Principle Logic, LLC
www.principlelogic.com
kbeaver@principlelogic.com

Principle Logic
Your Answer to Information Security℠

“There seems to be some perverse human characteristic that likes to make easy things difficult.”

- Warren Buffett

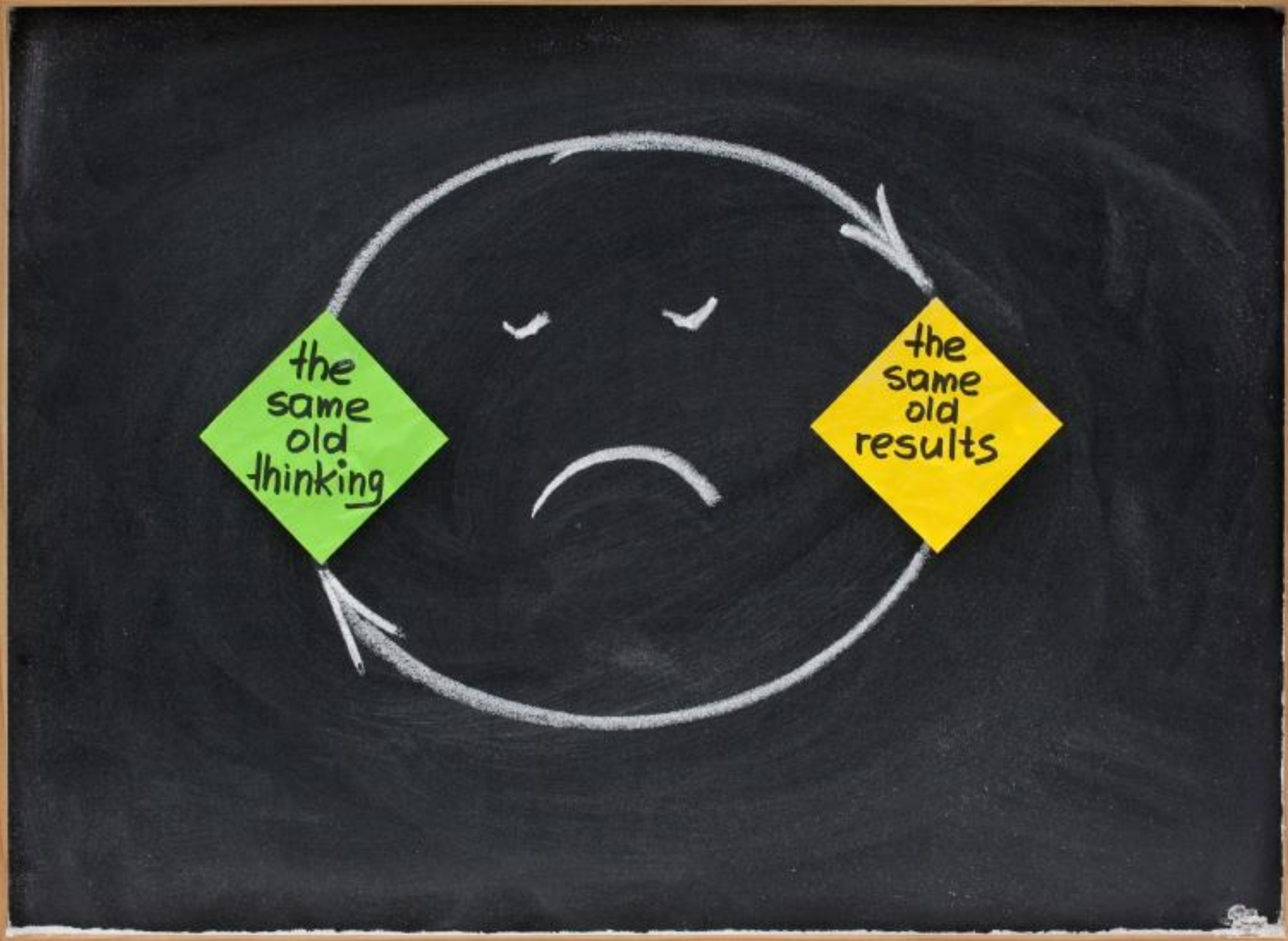
2015 Verizon DBIR

80% of attacks are external

Discovery times are too long

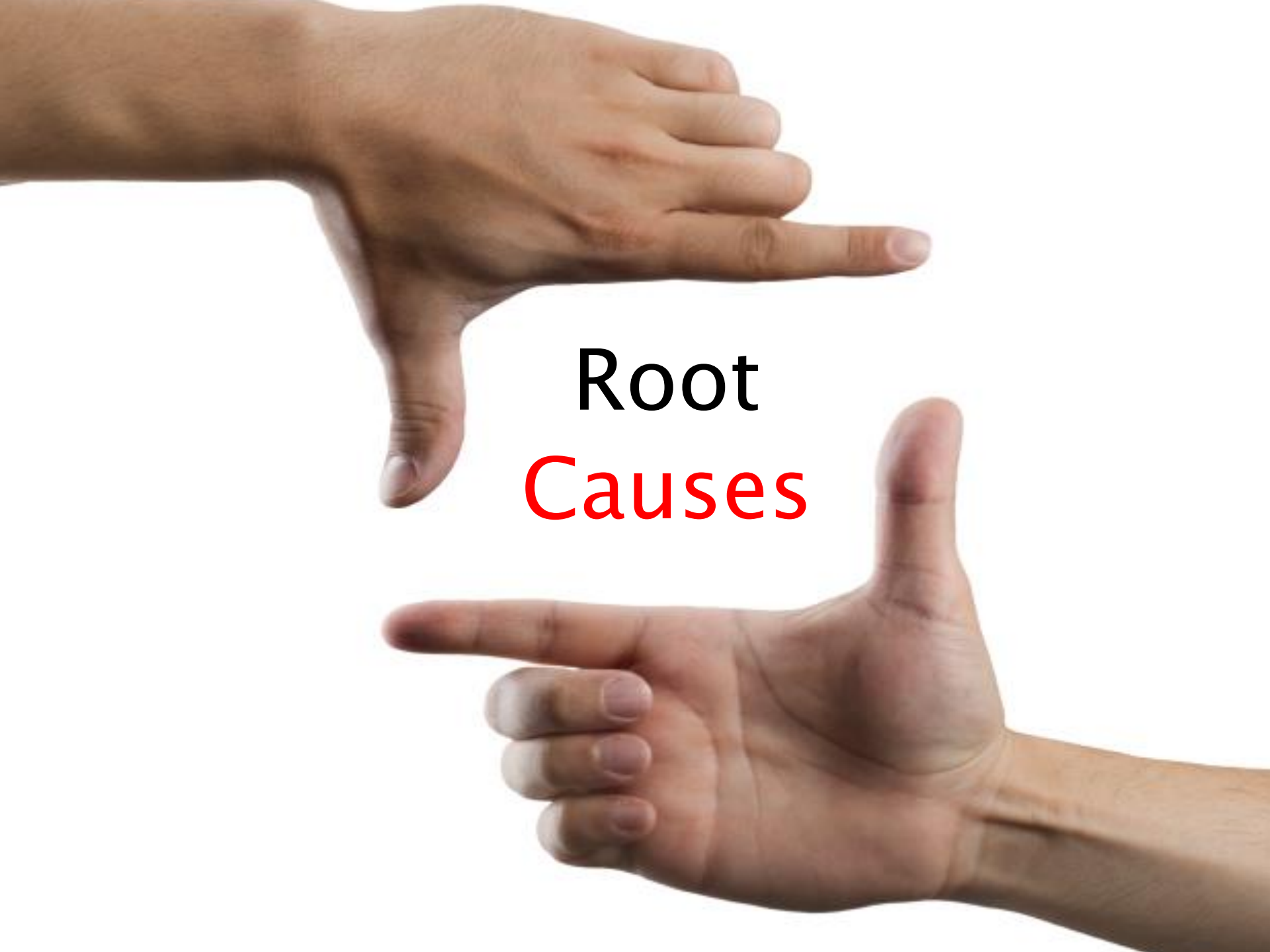
Flaws still not being patched

Phishing more effective

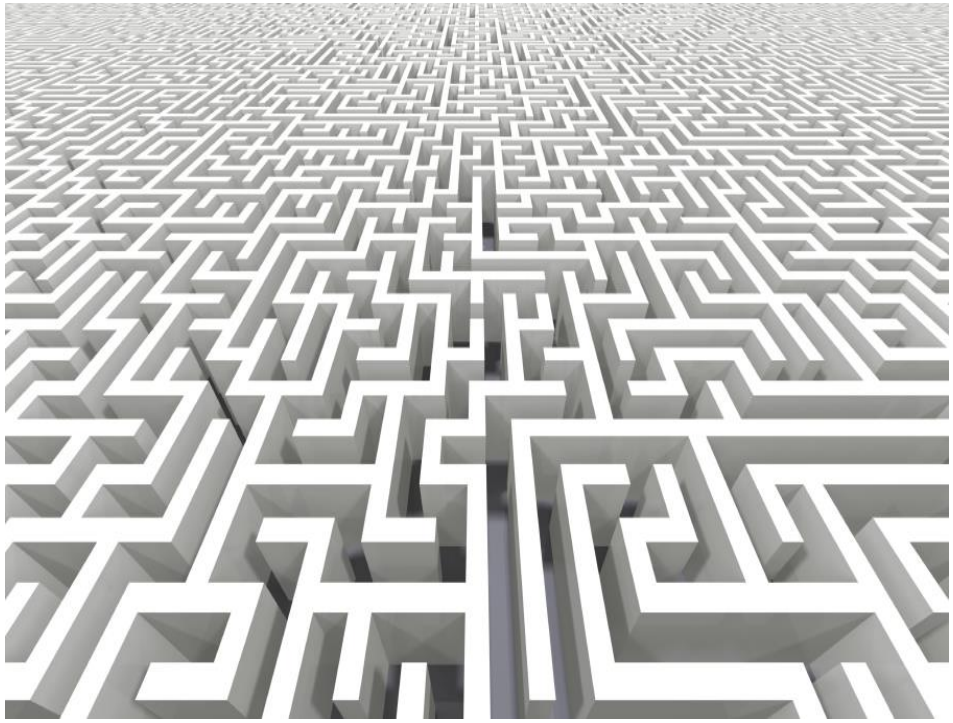

the same old thinking
the same old results

You *cannot* secure
(or respond to)
what you don't
acknowledge
(or know about).

Once the breach occurs…


Root
Causes

Threats are getting bigger and better.

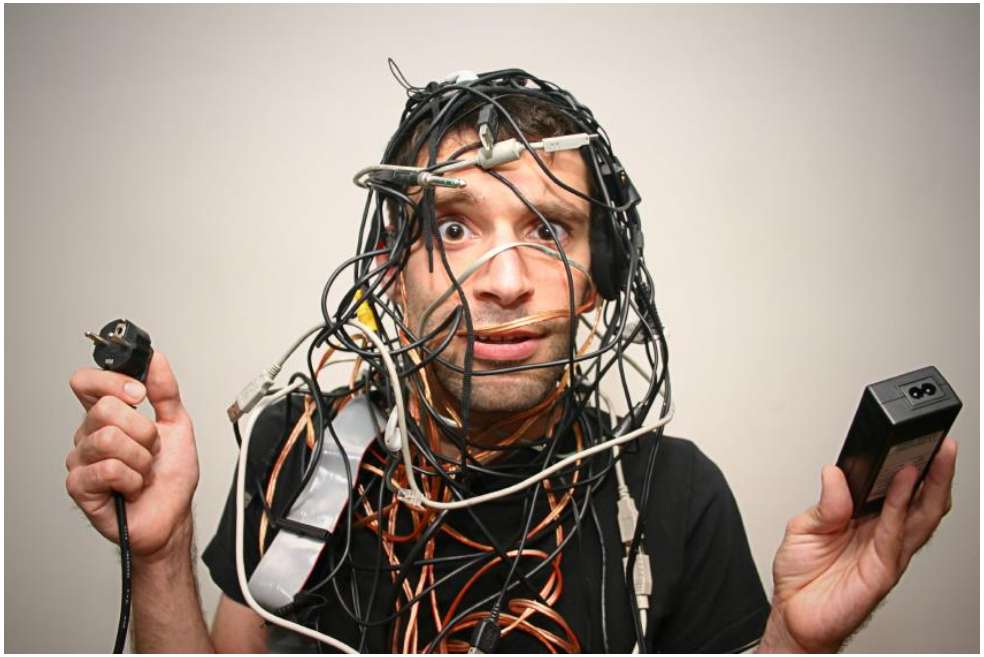


Attack surfaces are growing.

Bad (or no) information.

Lack of situational awareness.

Improperly set expectations.



Response is becoming more difficult.

Indecisiveness – no goals, no direction.

The 3 Steps You Have to Take.

Step #1

Know what you've got.

First Things First

What are your specific requirements?

What's expected of you?

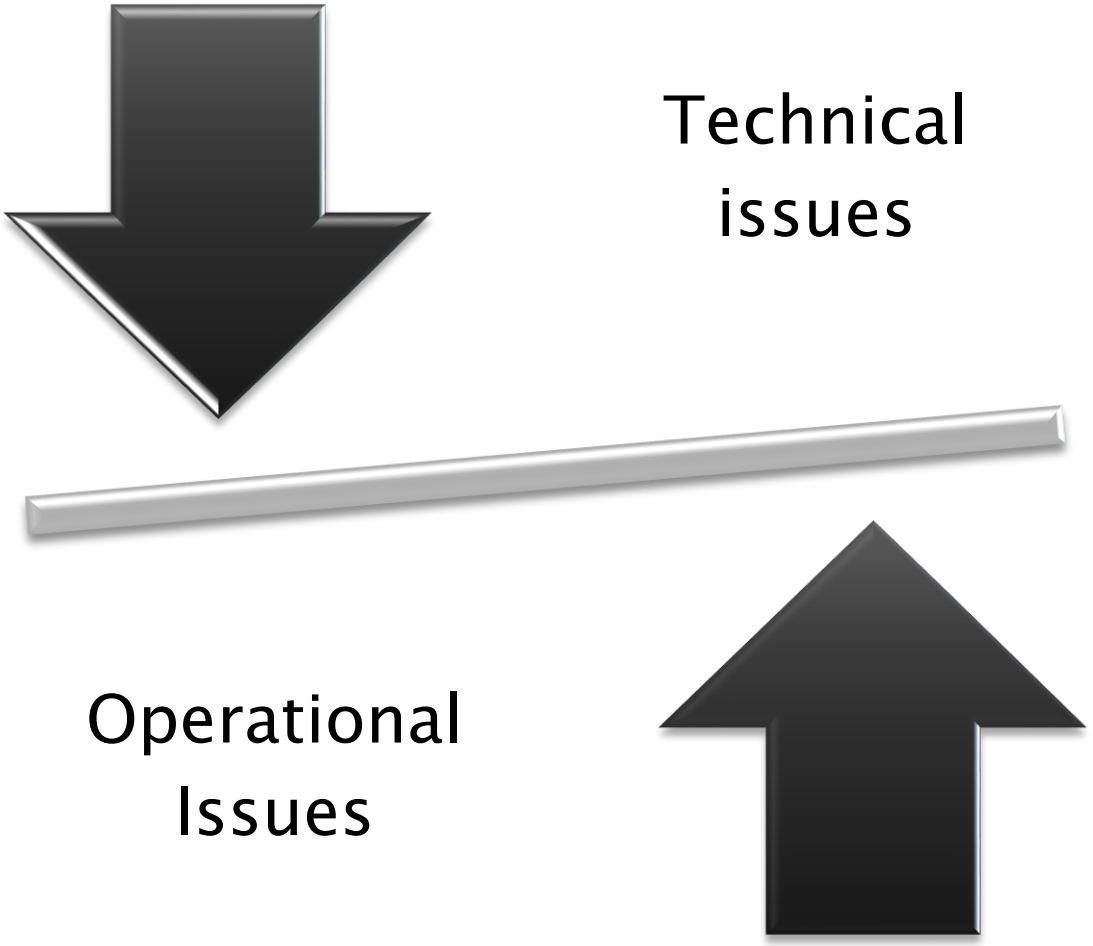
What information are you collecting?

Where are critical assets located?

Information & Systems to Protect

- Customer Information
- Employee Information
- Intellectual Property
- Applications
- Network Systems
- Vendor Connections

Look at Both Sides



Step #2

Understand how it's at risk.

All's well in IT…

Right?

The Givens

Passwords	Encryption	Patches
Malware Protection	Wireless	Web Applications
Physical Security	Unstructured Information	Phishing

Most urgent flaws.

on your

Most important systems.

"Avoidance is the best short-term strategy to escape conflict and the best long-term strategy to ensure suffering."

-Brendon Bruchard

Step #3

Do something

about it.

- ✓ Where does management stand?
- ✓ Are your policies documented?
- ✓ Are your policies reasonable?
- ✓ Are you actually following AND enforcing your policies?

Technology enforces policies.

Or does it…?

"underimplemented"

Who do you have on your side?

What's the worst that could happen?

(minimax regret analysis)

Two modes:

1) Reactive
2) Responsive

Response-ability

What is normal?

Has something gone wrong?

What has actually happened?

How did it happen?

What was impacted?

Who was involved?

What are the next steps?

"Divide each difficulty into as many parts as is feasible and necessary to resolve it.“ -Rene Descartes

Your Plan of Action

Step 1: Understand what's at stake.

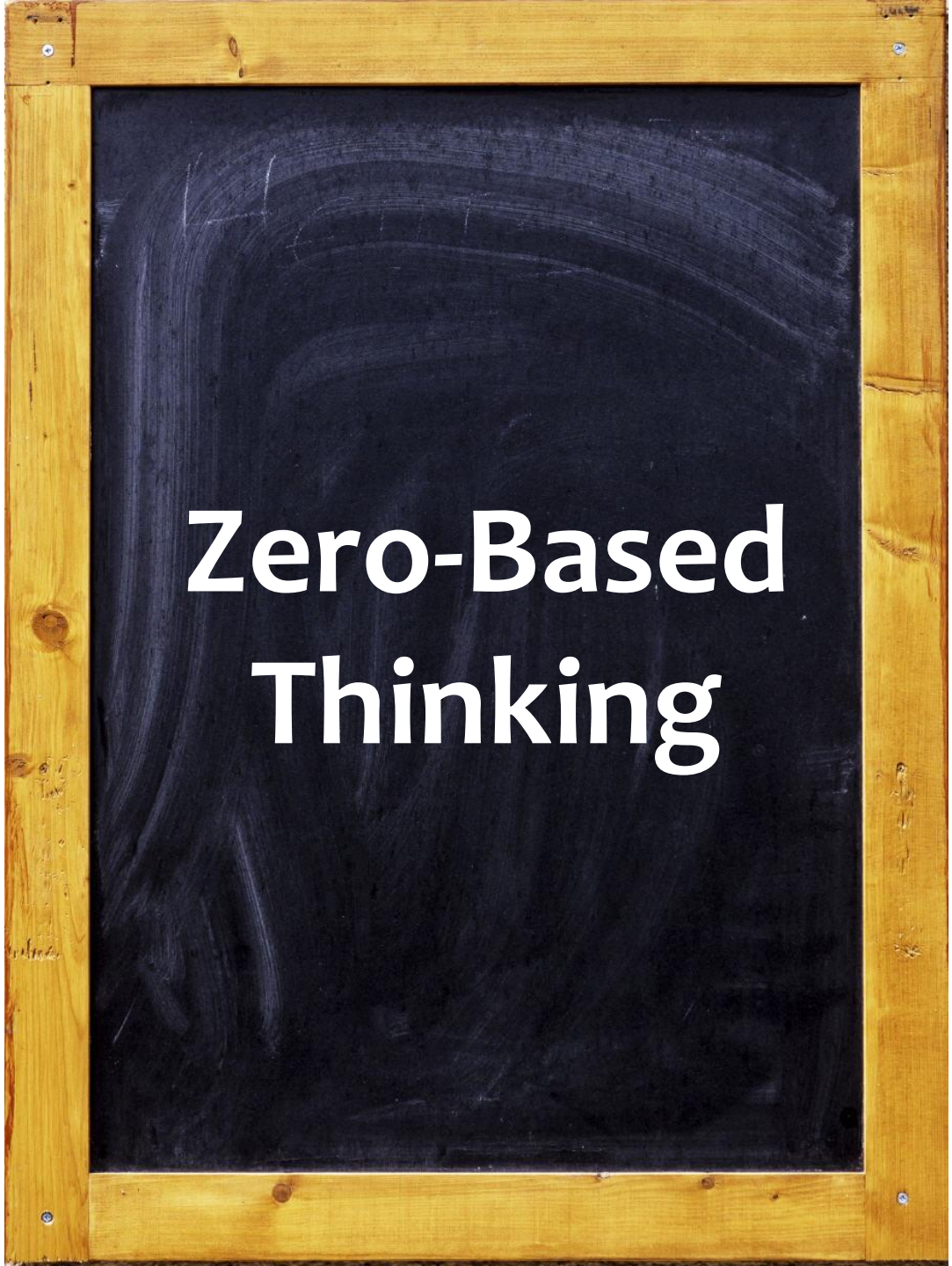
Step 2: Develop goals.

Step 3: Prioritize.

Step 4: Outline specific steps.

Step 5: Set deadlines.

...Get help when you need it.


Zero-Based
Thinking

Ask Yourself

1. If our security program was perfect in every way, it would have these things…

2. Knowing what we now know, what would we have more of? Less of?

Facts

vs.

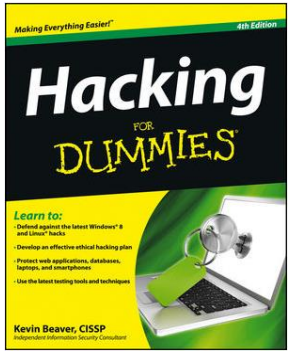
Problems

80/20 Rule

for your situation.

Additional Resources

- My website: principlelogic.com/resources
- My blog: securityonwheels.com/blog
- My audio programs: securityonwheels.com
- My latest books:



@kevinbeaver

www.linkedin.com/in/kevinbeaver

PrincipleLogic


Reactive
Proactive

Expect it to spill.