

THE FIRST 48: THE EARLY HOURS OF INCIDENT RESPONSE

Nick Selby
N4Struct, Inc

Security in
knowledge







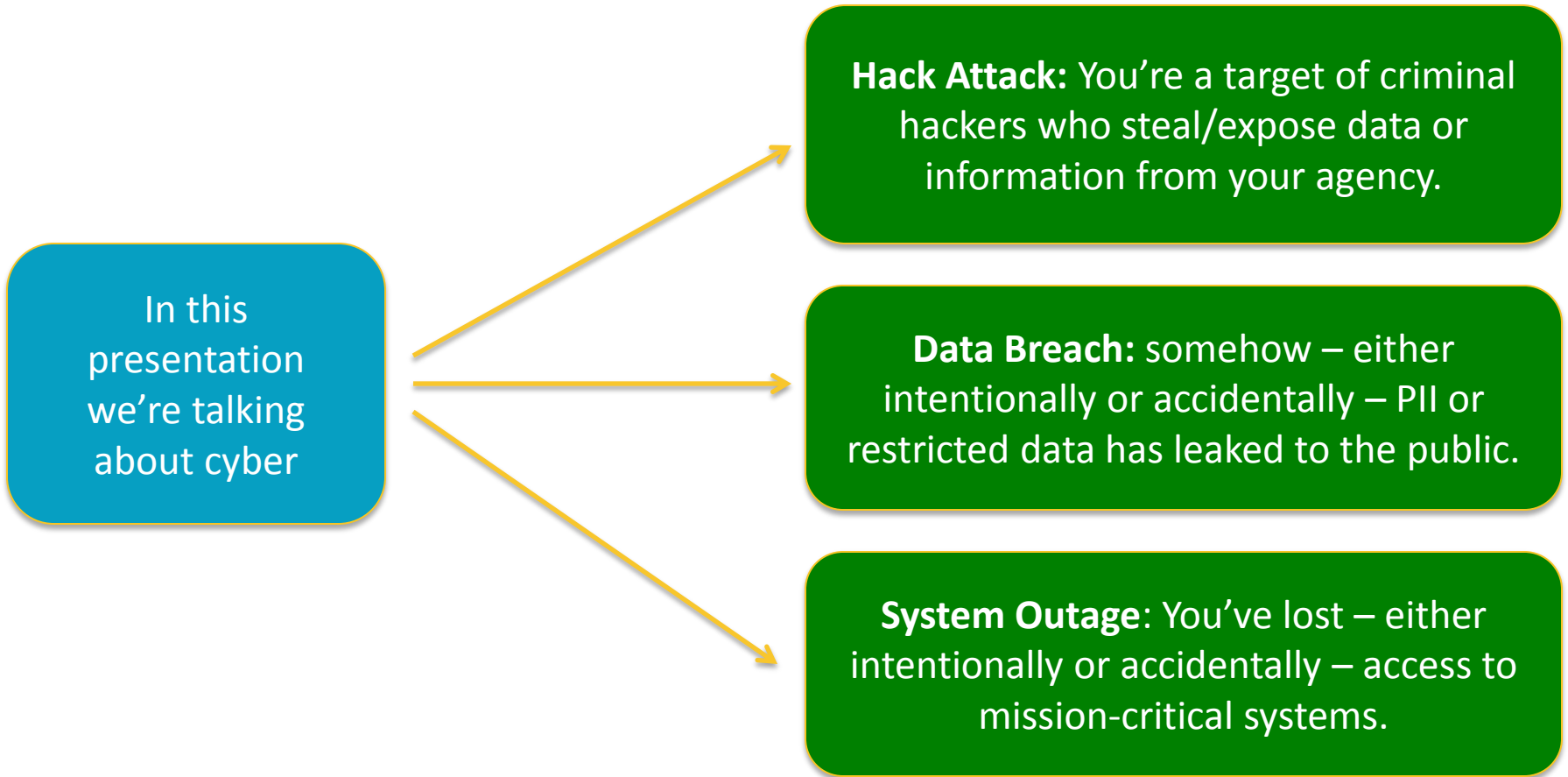






**DON'T GET STUCK IN AN AIR-
CONDITIONING DUCT THAT'S ON
FIRE.**

WHAT IS AN INCIDENT?



THE TIME TO PLAN IS *BEFORE*

If your hair's on fire, you've waited too long...

Start planning now. Use best practice lists from CERT, NIST, ISACs etc.

Knee-jerk reactions are always bad. Any planning you can do is good.

☑ The rest of this presentation assumes you have ignored this slide entirely.



Stupidest Question/Statement:



- ▶ “What Do I Have On My Network?”
 - ▶ This is usually asked by an otherwise smart person.

— Top 5 Dumb Breach Quotes

“Shut it down! Shut it down, NOW!”

“This is an IT problem.”

“There’s no classified information on your network”

“Find out whose fault this is right now.”

“We don’t have anything worth stealing on our network.”

Dumb-o-meter Threshold

The First Rule of Breach Is...



**DON'T
PANIC**

— SO, ACTUALLY DON'T PANIC



Establish That There Has
Been An Incident

- ▶ **This Seems Simple, But It's Not.**
 - In Enterprise, we face events all the time.
 - Why is this an **incident**, not just an event?
 - *How do you know?*
 - *How did you find out?*
 - *Your answer there dictates some things, like media involvement*
 - Once you're *sure*, **declare an incident.**

MANAGE UP

Management will be unrealistic and short-term focused. They want this to be over yesterday.

They need to be managed "up".

Harness that energy but **don't exploit that trust.**

— SET AN INCIDENT COMMANDER

IM == PM
Incident Leaders Recommend,
Leaders Decide

Inside people: What's here?
Outside people: what Risks &
Dangers do you face

Empower your Incident
Commander
(at highest possible level)

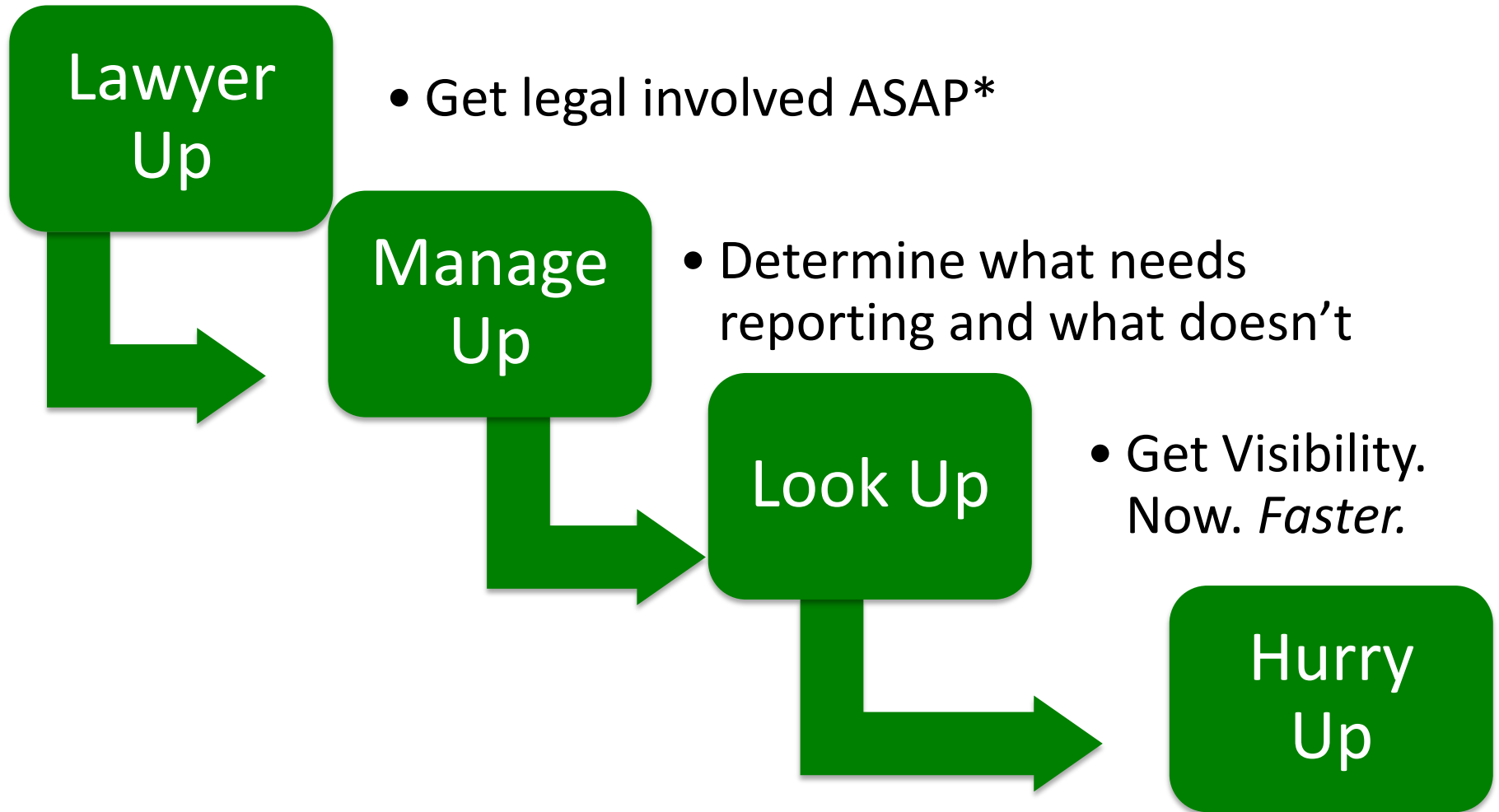
Contact/Resource Lists
(Internal and External)

This takes minutes to hours (if
the right people are in the
room)

Don't React until you
understand your plan's
ramifications



FIRST STEPS FIRST



REALLY? LAWYERS?

You're looking for stroke. Lawyers have it.
General counsel, IP counsel, Jacoby &
Meyers - no matter.
Get legal air-cover ASAP.

When it comes to it, which has more juice: a
request from you? Or a request from legal?

You need to understand what requires
notification and what *does not*. You need
legal help getting dept heads in line.



VISIBILITY

▶ You need it.

The first big assessment you make is, ‘What can I see? Where?’

- Flow
- Logs
- Full packet capture



IT'S NOT JUST SEEING. IT'S TAKING ACTION

A photograph of a boxing match. In the foreground, a boxer with tattoos and a beard is wearing a red and black boxing ring with the word 'TORNADO' on it. He is being punched in the face by an opponent who is wearing a white boxing ring. The background is a blurred arena with bright lights.

- **VISIBILITY IS NOT ABOUT BOXES, OR PRODUCTS.**
- **VISIBILITY IS NOT THE END.**
- *You cannot buy an incident response appliance*
- You need VISIBILITY, but you also need quality ANALYSIS of what you are seeing.
- **DECIDE EARLY** if you can do this in-house, or whether you need help



**LET'S LOOK
OUTSIDE THE
ENTERPRISE
FOR A
MOMENT...AT
GOVERNMENT**

SIMPLE P

“NOT D

- ▶ Just because they won't hit you.
- ▶ Just because they they do it, doesn't mean

We infiltrated a server on their network that basically had no security measures in place. We were able to run our own application, which turned out to be a shell and began plundering some booty. Most shiny is probably a list of roughly 90,000 military emails and password hashes.



Booz-Allen Hamilton hack

— AND IN EVERY
GOVERNMENT HACK
SINCE...




CLASSIFIED != "IMPORTANT"

-----Original Message-----
From: Robert Wieners <rbw7799@yahoo.com>

Date: 24 Mar 2008 15:34:12

• Texas Takedown Thursday



identityfinder

Explanation and Clarification of Statistics:

- Identity Finder searched 30,579 files and found 19,206 files containing personal information;
- 13,124 email messages, 3,339 PDF documents and 2,188 Word documents contained personal information;
- 647 Social Security Numbers, of which 418 were unique;
- 42 Credit Card and Bank Account Numbers, of which 26 were unique;
- 174 Passwords
- 83 Drivers License Numbers;
- 6,182 Dates of Birth;
- 78,869 Phone Numbers, of which 14,701 were unique;
- 10,175 Personal Postal Addresses, of which 4,631 were unique; and
- 325,596 e-mail addresses, of which 39,419 were unique.

Impact

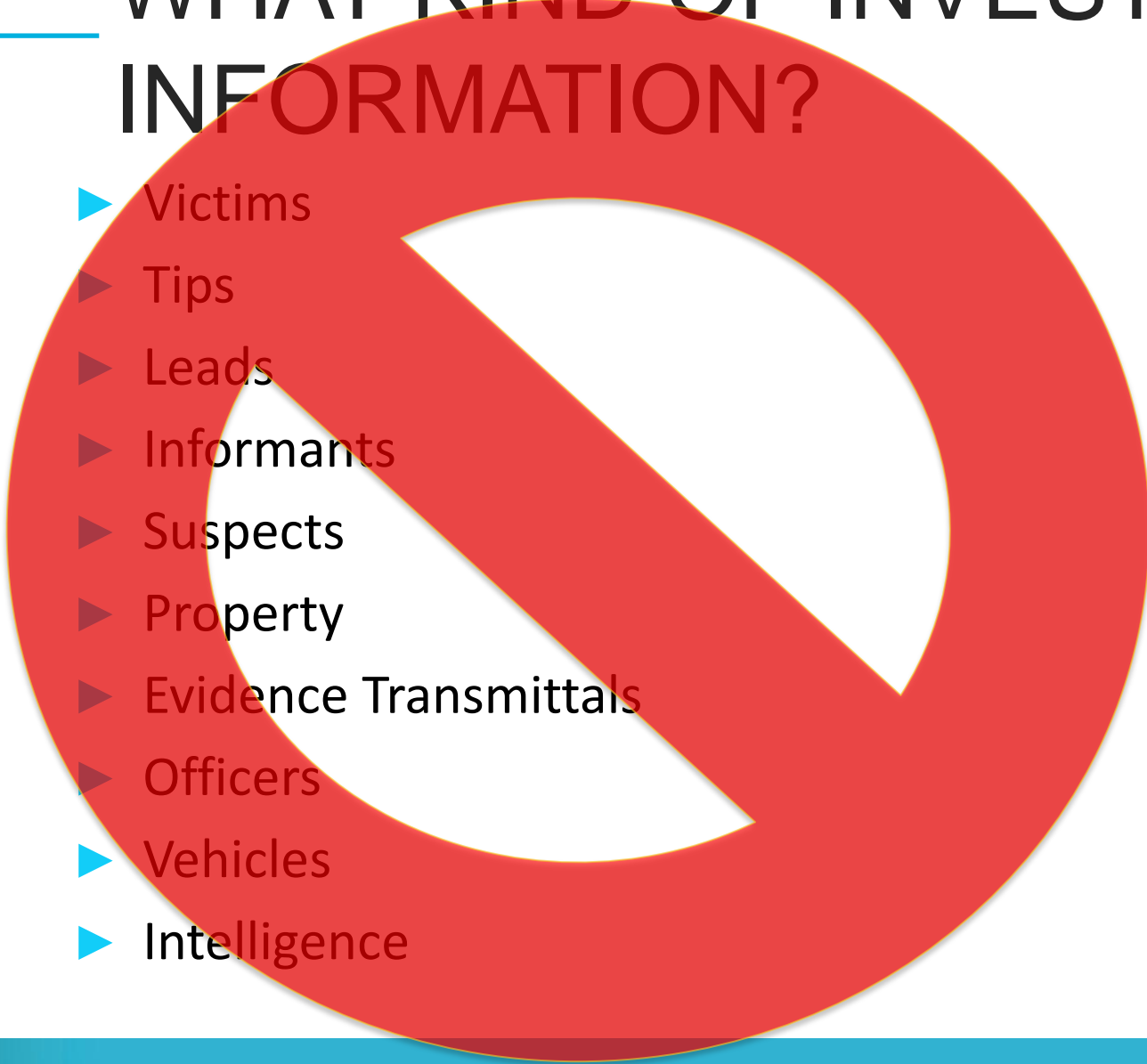
- Embarrassment
- Possibly more?



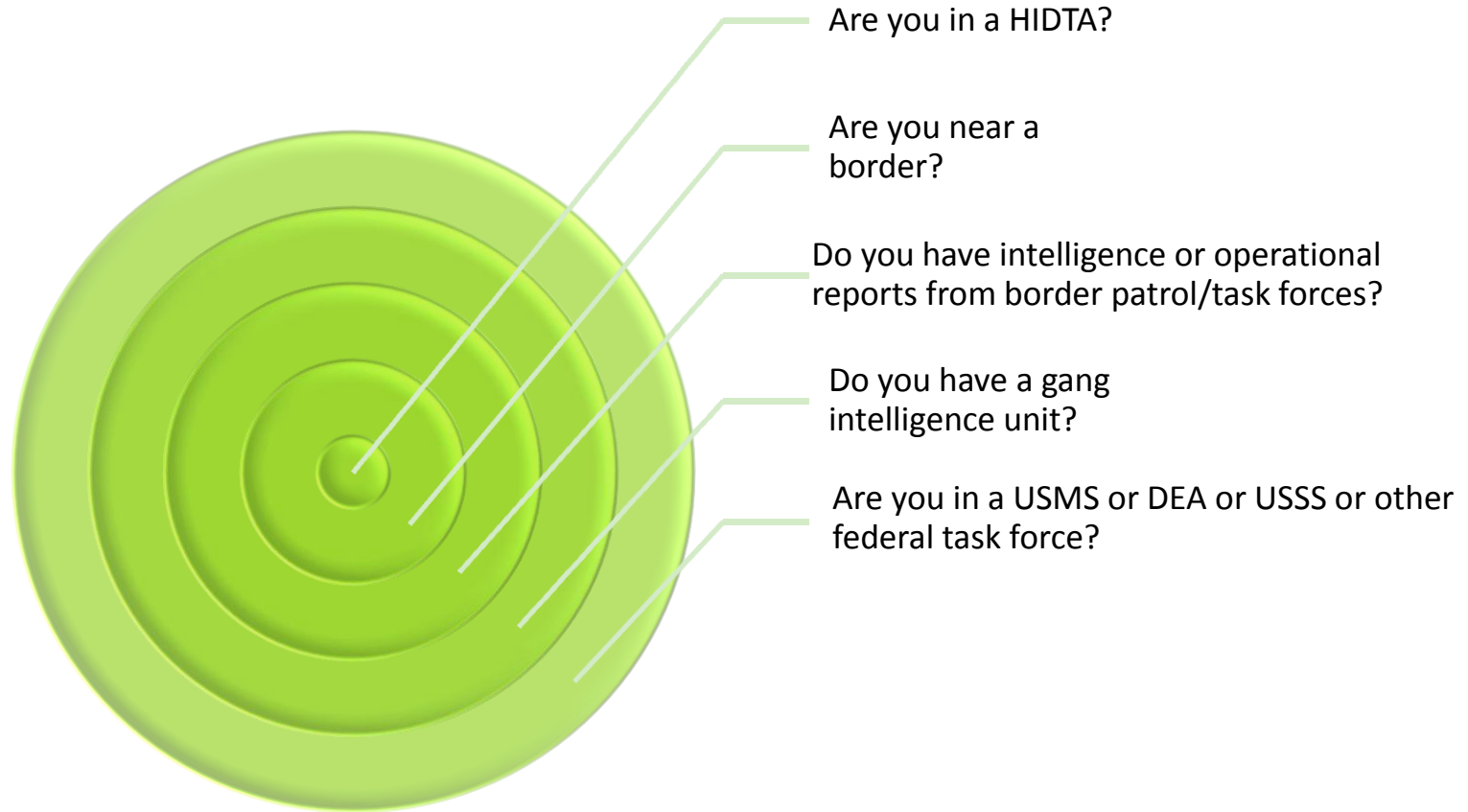
— WHAT DO COPS HAVE ON THEIR NETWORKS?

- ▶ Rosters of officers
- ▶ Contracts
- ▶ Intelligence Reports
- ▶ Tactical manuals
- ▶ Detailed plans and narratives of raids and arrests

WHAT KIND OF INVESTIGATIVE INFORMATION?

- 
- ▶ Victims
 - ▶ Tips
 - ▶ Leads
 - ▶ Informants
 - ▶ Suspects
 - ▶ Property
 - ▶ Evidence Transmittals
 - ▶ Officers
 - ▶ Vehicles
 - ▶ Intelligence

THEY ALSO HAVE HIGH-VALUE INFORMATION



CAN YOU THINK OF ANYONE



— ALL THIS IS BY WAY OF SAYING...



Do not take advice on what is important to you from any person who does not appear in the device at the left when you wake up in the morning.

**BACK TO STUFF
YOU CARE
ABOUT: THE
ENTERPRISE**



— FOCUS ON THE IMPACT

How It Happened

Why It Happened

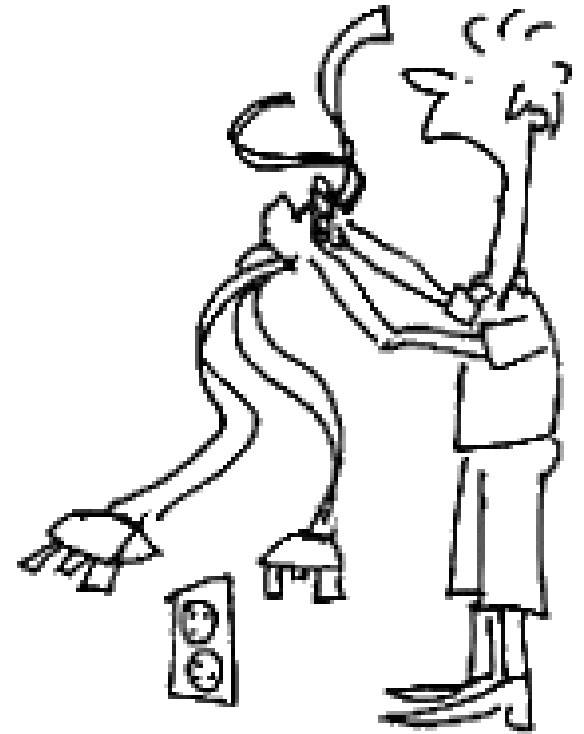
When It Happened

IMPACT



— SIMILARLY: THIS IS *NOT* AN IT PROBLEM

When your information goes out the door, it's your business' problem



A COMMUNICATION STRATEGY IS KEY

Develop an internal communication plan, grounded in the concepts of “least privilege” – if they don’t need to know, they should not.

August 11

Develop an external communication plan, being as transparent as possible once you know the facts – and not a moment before you know the facts.

CONDUCT A BRUTALLY HONEST SELF ASSESSMENT

Conduct a post-breach inventory – what might you have lost?

What are your internal capabilities? What do you need help with?

Where can you get help?

Make lists of what you can do, what partners can do, what you need to hire

Remember, you haven't even discovered what's happening yet, you're just getting prepared to find out

CAPTURE EVIDENCE, DON'T DESTROY IT

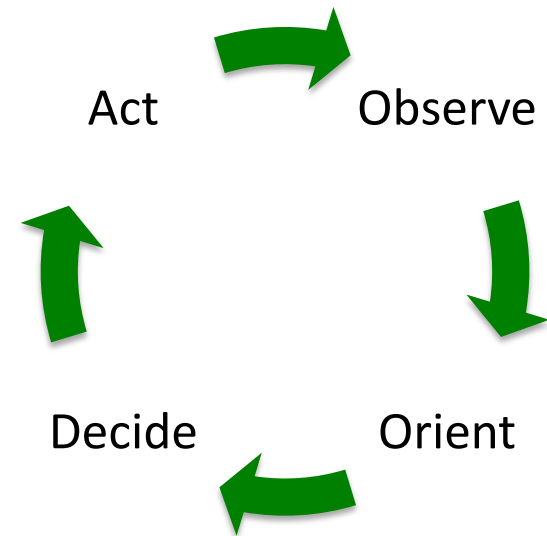
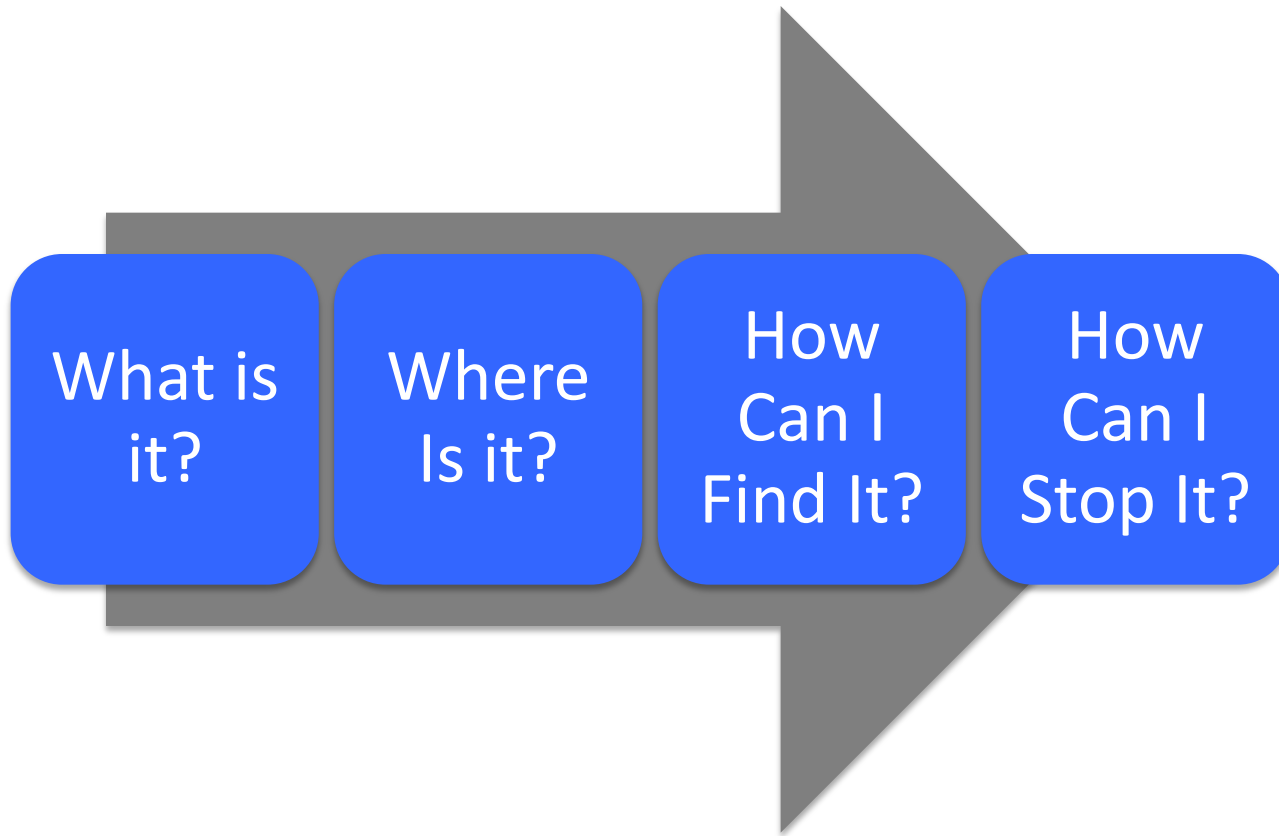
This is not a technical brief, but your evidence collection must take back seat to getting you aware and back up

Don't destroy evidence unless you have to

Expect that it will take *years* to get your drives back.
If you ever do.

Don't get hung up on attribution, get hung up on fixing stuff and making sure it don't get re-broke

— GET ALL OODAd OUT



— NOTA BENE: IF YOUR BREACH IS PUBLIC?

HOLY SMOKES, WHAT A CHANCE TO MAKE LEMONADE

- Negotiate with Vendors
- Use their PR machine
- Get what you need cheaper



IN CONCLUSION

Start Now. It's never too early

Inform leadership: directors, lawyers, chiefs

Establish an incident commander

Understand what happened. Really.

Create a communication strategy – int & ext

Conduct an inventory of your skills & get help

Let impact drive your response.

Consider, but don't be paralyzed by, evidence collection requirements

Find, then follow, those with passion to fix it.

CONTACT ME:

NICK SELBY
nick.selby@n4stru
ct.com
817-203-4074

