# When the Current Ransomware and Payload (CRAP) of the Day Hits the Fan: Breaking the Bad News

Cathy Ullman, University at Buffalo
Chris Roberts, Acalvio

# Introduction

* Who are we?
* Why should I care?
* What are the odds?

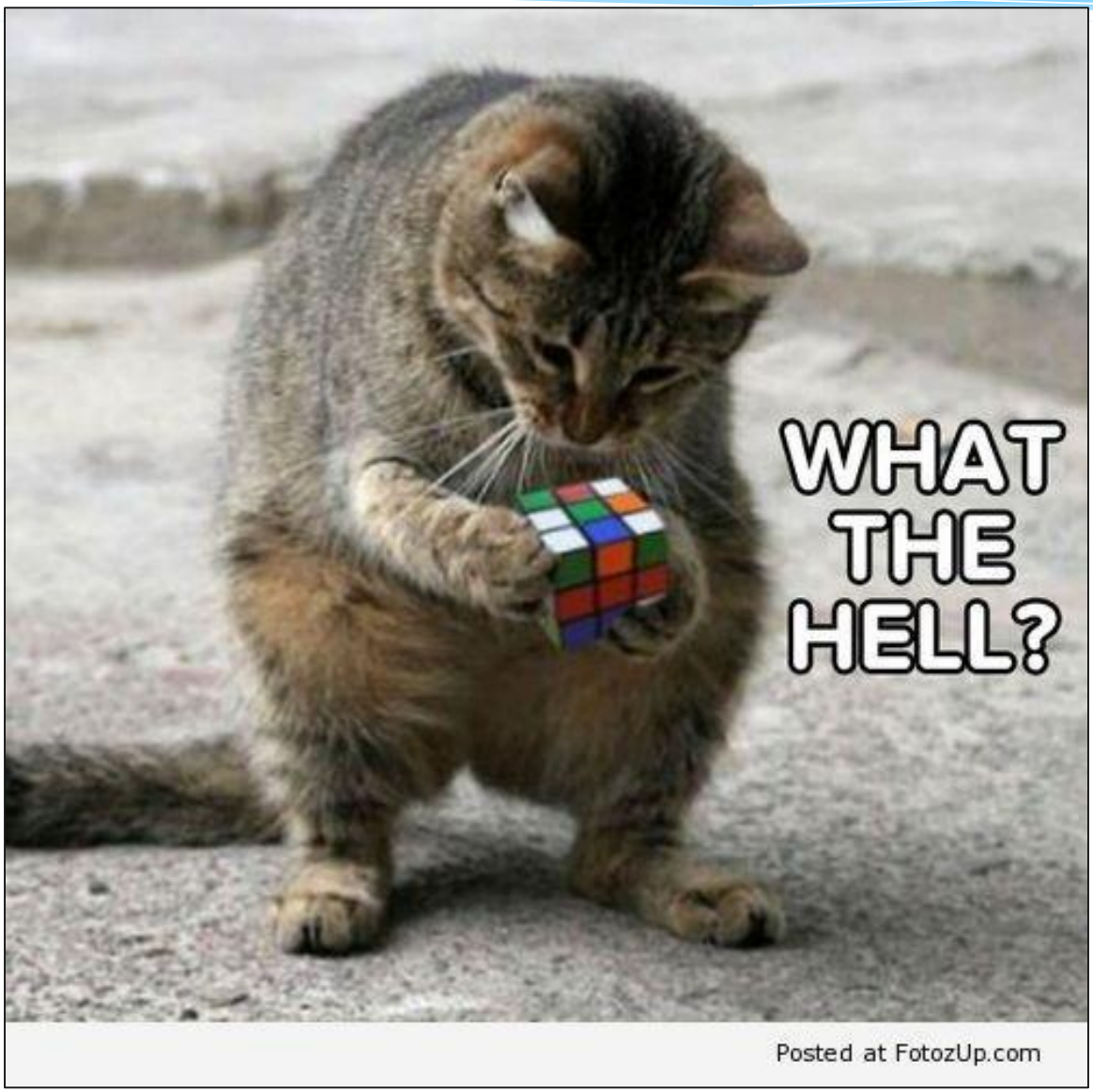
# Who are we?

# Ok fine…

* Senior Information Security Analyst, University at Buffalo
* Employed at UB 17+ years
* IACIS - Certified Forensic Computer Examiner
* GSEC- GIAC Security Essentials Certification
* MCSE, MCP+I, CNA
* M.F.S. (Master of Forensic Science)
* PhD, Philosophy

# Sideways planes…’nuff said.

# Why should I care?



# What are the odds?

According to reported incidents from idtheftcenter.org:

* 2016: 1093 breaches (US)
  * 55.5% of the breaches were malware/hacking related
* 2017: 791 breaches as of 6/30 (US)
  * 63% of these breaches were malware/hacking related
* 2017 Year End Projected Total: 1500+ breaches (US)
  * An overall 37% Increase from 2016

# Yeah…

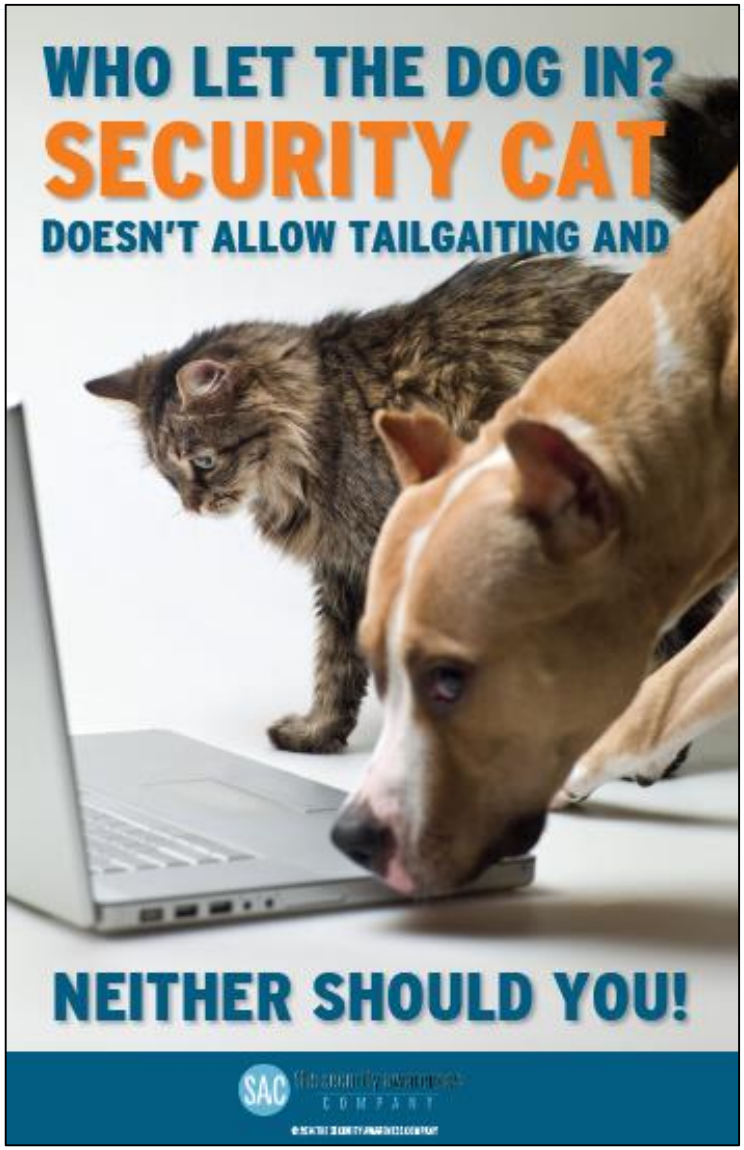
**"There are only two types of companies: those that have been hacked, and those that will be.**

Even that is merging into one category:

**those that have been hacked and will be again,"** FBI Director Robert Mueller (Cowley 2012)

# We are InfoSec Professionals!

Protecting all the Peoplz:

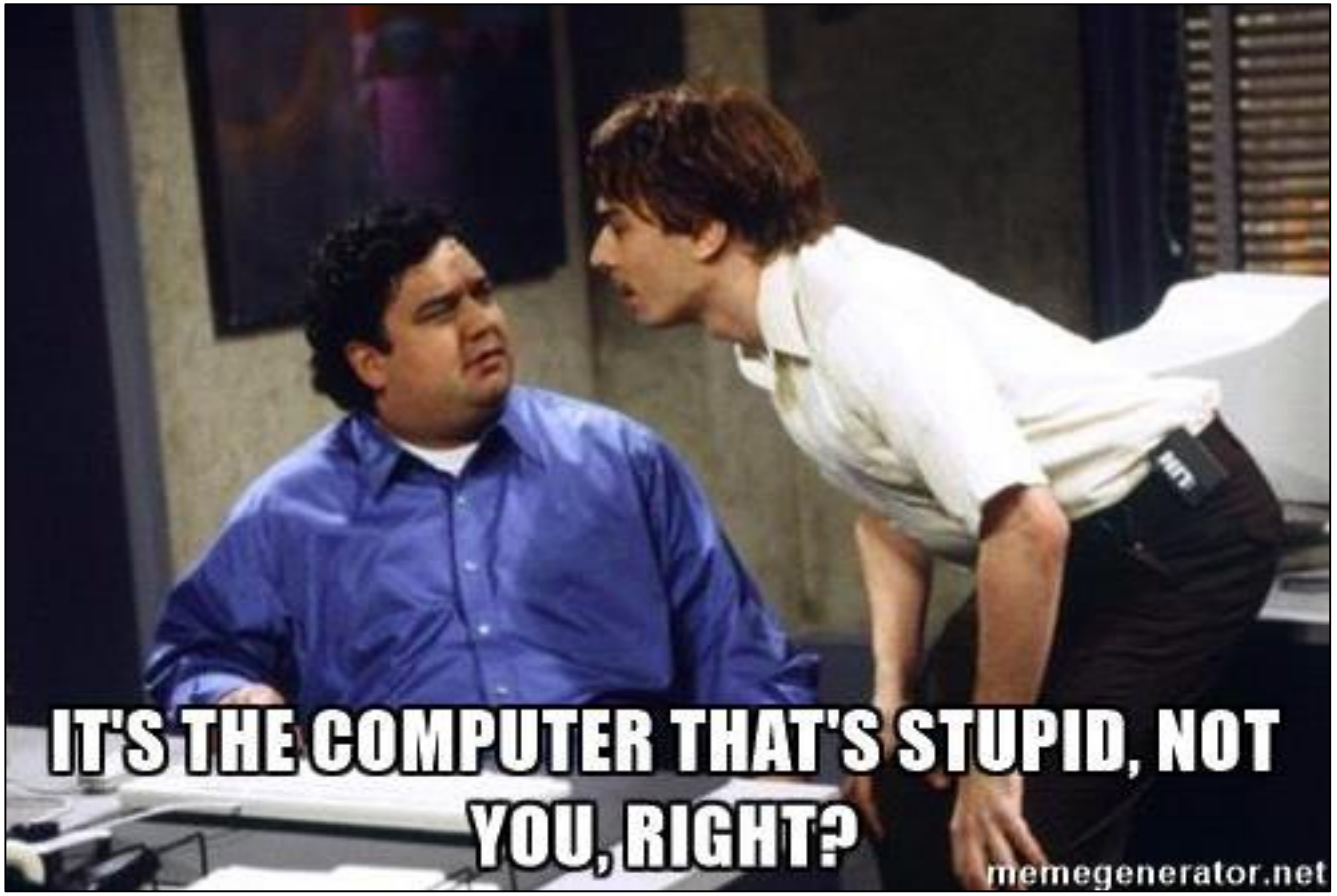


# What we're good at

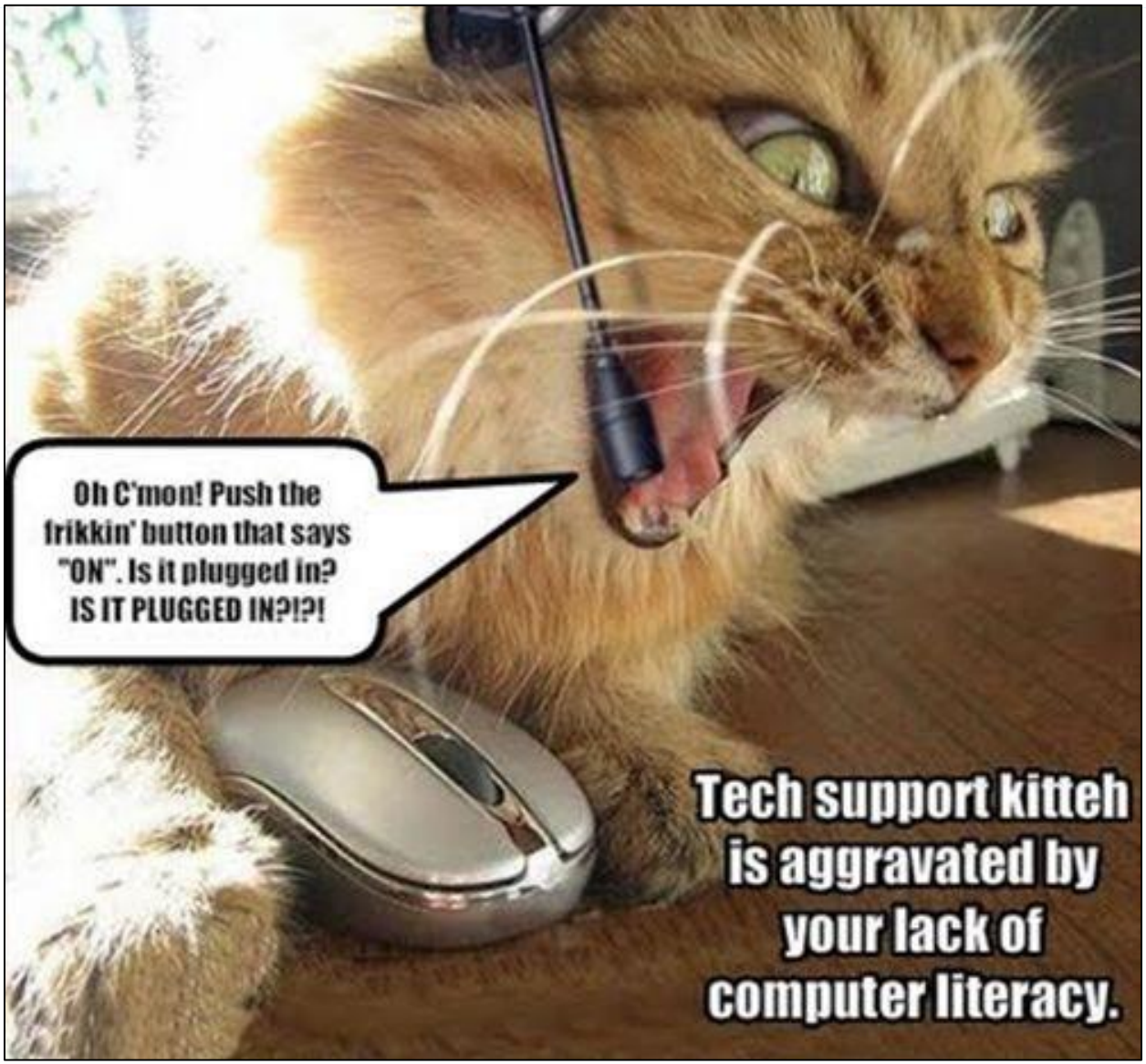
Diagnosing and fixing some problems

# What we're often not so good at

Strong Verbal or Written Communication Skills



# Patience?


Oh C'mon! Push the frikkin' button that says "ON". Is it plugged in? IS IT PLUGGED IN?!?!
Tech support kitteh is aggravated by your lack of computer literacy.

# Repercussions?

* Potential loss of trust
* Difficulty of future communication
* Potential cause of additional conflict
* Negative impact on company reputation
* Decrease in morale
* Elevated stress

# Ransomware Payload Hits!!!

Uh oh… now what?

# Audiences

**Framing the conversation: What is important to THEM?**

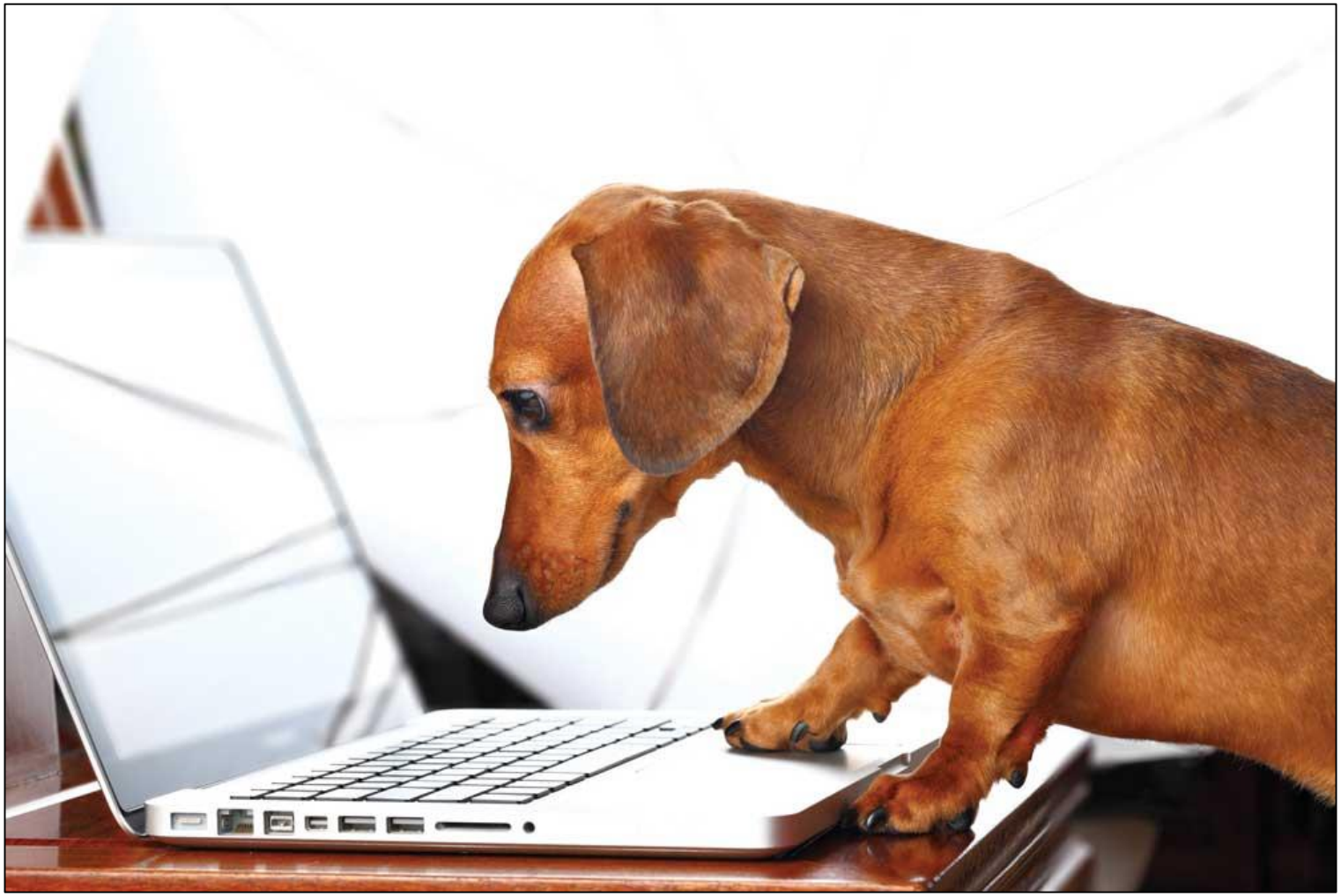
* End User
* Middle Management
* C-level

**Anticipate the questions each level might ask!**

# Proper Communication Channel?

* Internal web site?
* Presentations?
* Email?
* In person?
* Lawyer approved pigeon carriers…

# The End User



# End User Communications

* Typically focused on how it will Impact work completion
* Communication should involve **WHAT** happened and **WHY** whenever possible
  * Use as an opportunity for awareness training both for use at work AND at home (i.e. show as a benefit to them)
  * **Effective** and **efficient** communication is a MUST whether in person or electronically as well as continuous whenever possible

# End User Communications

* How does one “effectively and efficiently” communicate?
  * Provide communication at a level that they can both understand and relate to
  * Be **Concise** – tl;dr: Less is more.
  * Be **Judicious** – don’t blame management or provide irrelevant information
  * Be **PATIENT**: Even if you have to go into the closet afterwards to scream and tear your hair out….

# End User Communications

* Engagement is KEY
  * Be up front and honest – the "lies-to-children" approach will come back to bite you
    - Be sure to address potential fear and uncertainty
  * Perception often IS reality for the end user
    - Listen and investigate, even if *you* know it's not a problem

# Middle Management

# Middle Management Communication

* Typically focused on the Impact to business processes
  * Impact will depend on where they are (Ops, IT, HR, etc.)
  * Speak at a level that they can understand and relate to
  * Provide effective and efficient communication appropriate to the individual – i.e. use technical terminology only if this manager is a tech him/herself

# Ideal Middle Manager Skillset

* Delegation skills (both over their scope of control and influencing other groups)
* Effective communication skills
* Interpersonal skills both human and alliance based
* Negotiation skills
* Emotional intelligence
* Influencers

# Where are the Ideal Middle Managers?

# Engaging with “regular” Middle Managers

* Be supportive – come to them with a **complete** plan for action including communications both down and UP the chain
* Empathy is critical – mid management is HARD
* Make them look good

# Engaging with “regular” Middle Managers

Plan should include the following:

* Communicate what happened (i.e. explain what ransomware is)
* End goal(s)
* How to get there

# Engaging with “regular” Middle Managers

Plan should also include:

* *All* stakeholders, internal and external
* Recovery options
* Time frames
* Reduction of potential recurrence
* Clear statement of any uncertainties

# Engaging with “regular” Middle Managers

Management should take responsibility for their users’ behaviors

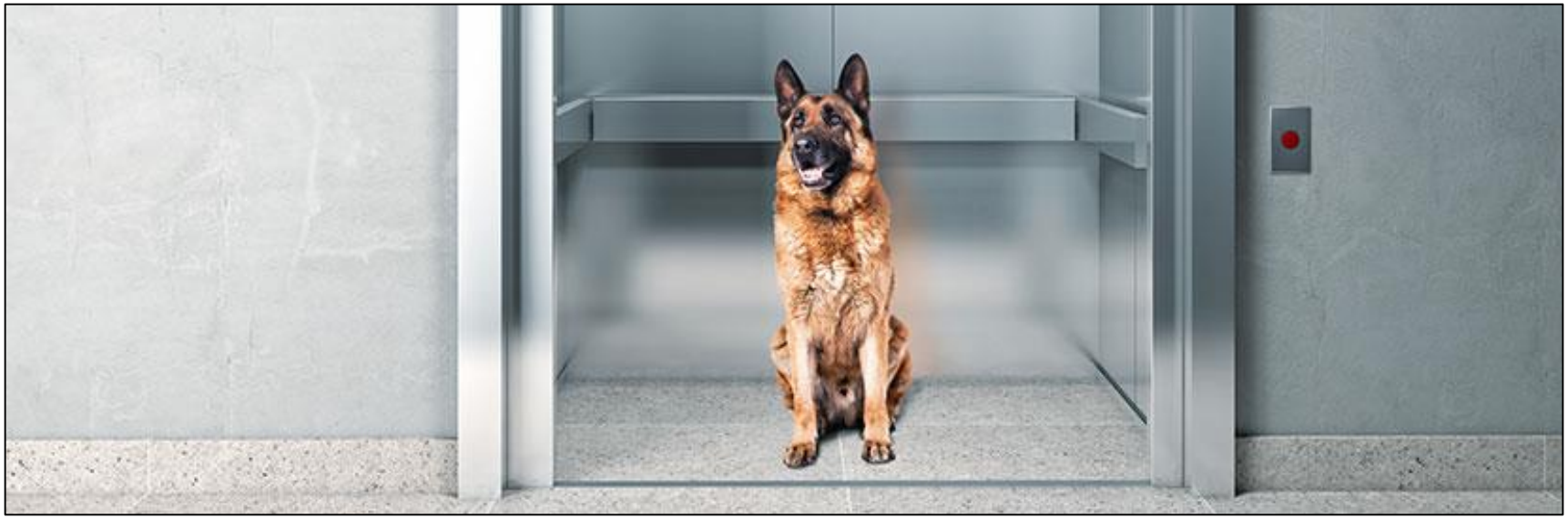
# Engaging with “regular” Middle Managers

* Manage/control vs. delegate/negotiate?
* Coach/encourage collaboration
* How to handle potential ransom payments?
* Outside entities (e.g. Mandiant) and/or law enforcement?

# C-Suite

* Typically focused on big picture stuff
  * Overall company goals/reputation
  * Overall company performance
  * Overall company vision

Think: 30 seconds in an elevator



# C-Suite - General

* Describe in general terms (not technical) what/when happened
* Provide best case, worst case, most likely scenario
* Provide consequences and underlying cause(s) of incident

# CEO

* Do your homework
* Enter/exit gracefully
* Present and discuss strategically
* They are people too!

# CFO

* Numbers and **meaningful as well as measurable** metrics
* Ground goal/solution in practicality
* CFO knows legal – use YOUR knowledge of IT regs to help

# COO

The Executor:

* Responsible for day-to-day operations
  * Will need to understand *any* interruption

The Change Agent:

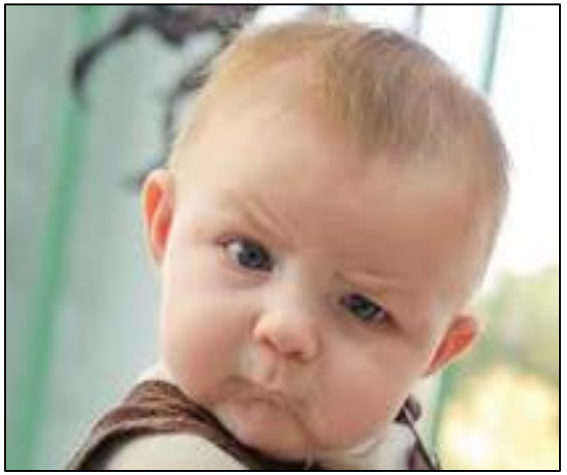
* Responsible for specific successes/deliverables
  * Align communications to assist

The Mentor/Future CEO:

* Tutoring
  * Help gain necessary insight to align w/ business practices

# Message received ?

# Pay Attention to Body Language!



# *Caveat!*

* Subject to assumption of *genuine* behavior
  * i.e. not intentionally masking behavior
* No guarantees
* Another useful tool

# Non-Verbal Communication

Non-verbal communication (body language) includes:

* Facial expression
* Body postures
* Gestures
* Handshakes
* Breathing

# Interpreting Non-verbal Cues

* Raised eyebrows
  * discomfort or true surprise or doubt?
* Excessive eye contact
  * lying eyes or real interest?
* Crossed arms and legs
  * resistance to ideas or chilly room?
* Exaggerated nodding
  * Anxiety about approval or real project excitement?

# Synthesis of Non-verbal Cues

* Single, isolated cue, possible misinterpretation

* Synthesis of cues needed to “read” person/situation:

Raised eyebrows

+

Fleeting eye movement

+

Unnecessarily hard grip on something

=

Likely Discomfort

# Judgement Free Zone

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

# Be the Change!

# With Gratitude

* To Wall of Sheep for inviting us to share these thoughts with you
* To the University at Buffalo for allowing Cathy to be here today
* To Acalvio for allowing Chris to be here today
* To the folks who originally created the images, videos, and other creative content – thank you!

(Note that this content was used in accordance with copyright law – if you want to quote, please give credit where it is due!)

# Questions?