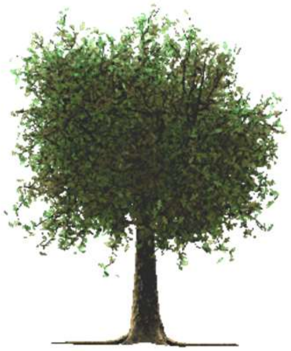
Stop Talking Nerdy to me: Translating the Value Proposition of the Blue Team to the C-Suite

Jake Williams
BreachQuest
www.breachquest.com
@BreachQuest



$whoami

- Founder and CTO of BreachQuest
- IANS Faculty, former SANS Instructor
- Former NSA Hacker, endorsed by Shadow Brokers
  - aka Russian Intelligence
- Breaker of software, responder of incidents, reverser of malware, injector of code, spaces > tabs
- **Dislikes:** those who call themselves “thought leaders,” “crypto bros,” and anyone who **needlessly adds blockchain** to a software solution

Agenda

- Establishing Common Ground
- Putting the Value in “Value Proposition”
- Security Elevator Pitches
- Blue Team Value Objections
- Finalizing Value Proposition
- Closing Thoughts

Blatant Disclaimer

- In this talk, I'll be recommending that IT ***not*** focus on security
  - This will make some of you mad

- I'm ***<u>not</u>*** implying that IT should ignore security
  - Only that it shouldn't be a core competency

- Many of you work in orgs that don't have enough staffing to fully separate security implementation and monitoring from IT
  - Remember that there's a lot of daylight between "we can't roll with the ideal" and "this is wrong"

Establishing Common Ground

Let’s at least agree on the foundations…

Begin By Finding Common Ground

- Blue team is all about security
- Before you try to communicate the value proposition of Blue Team, make sure you and your prospect share a common definition of what security is
- Failing to do this is like explaining the worth of a product in dollars to a hunter-gatherer society

Security Definitions

- Many people start by introducing the well-worn mnemonics of The CIA Triad for the definition of security
  - – Confidentiality
  - – Integrity
  - – Availability
- And IOC for the definition of "threat"
  - – Intent
  - – Opportunity
  - – Capability

Breach Quest

There’s a Better Way

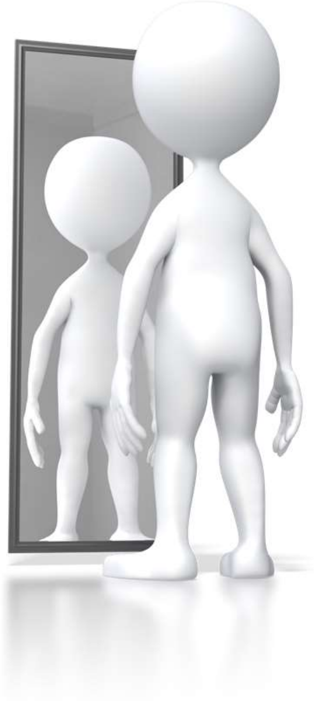
- I always picture my mom in these conversations
  - To be fair, mom is a retired executive, so it fits…

- Will she understand what CIA is and why it matters ***to her?***

*Photo may not represent my actual mom

Finding Common Ground

- The most effective communication happens when you find common ground with the target
- Some infosec pros think this means to build up the basics of technology - talk to them like you would a n00b
  - That's just substituting tech for less advanced tech
- Remember - your job is decision support
  - Your job is **NOT** to teach technojargon to your audience
- You're not helping with decision support if you're confusing or misdirecting the audience

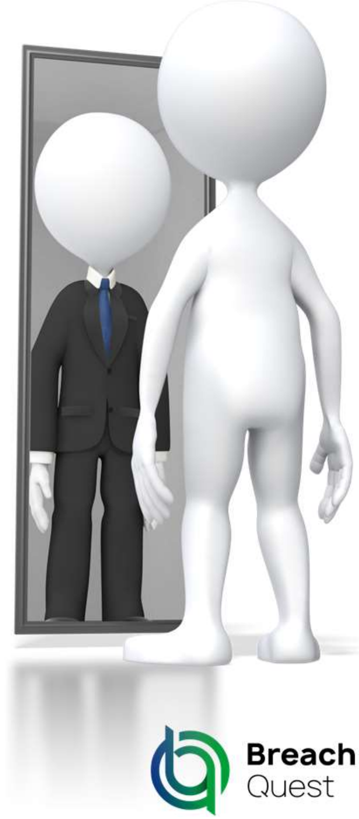


But I Have NOTHING In Common With "A Suit!"

- You probably have more in common than you think
- Most of us share common knowledge about things like:
  - Household chores
  - Life events (relationships, high school, college, etc.)
  - Childrearing (if applicable to both you and the target)
  - Hobbies
  - Sports
- Can you find infosec themes here?
  - They're present, you just have to look for them

Building Common Ground

- Beyond the obvious common ground, there are two easy ways to build common ground with executives:
  1. Learn industry specific jargon and use it
  2. Learn to speak like a business leader
- Aka - "will I come to them or will they come to me"
- Many (most?) execs have an MBA, get their reading list
  - Good to Great
  - Made To Stick
  - The Wisdom of Crowds



Communication Matters

- Uncomfortable truth: information security is a cost center, not a profit center
  - We exist to provide decision support to the business so they can do what they do as efficiently as possible
- But are you ***talking*** or are you ***communicating***?
- After interviewing boards of directors, executives, and senior management at organizations around the world, the results are pretty conclusive:
  - Infosec is talking far more than we're communicating

Putting the Value in “Value Proposition”

Know what your target values

Start Where They Are

- Your role here is selling security
- If you aren’t using well understood sales tactics, you’re probably making a bad sale
- If it’s socially permissible, ask your target “what are you concerns around security?”
  - Then STFU and ***listen***

Case Study: Porsche Listens Only To Target Market

- Madhavan Ramanujam describes the process of Porsche building an SUV in his talks

- The first (and most important) job was deciding whether there was a market to build the SUV at all
  - And if so, which features to include

- Porsche surveyed potential customers ***who would buy at their price point*** about the features they would pay for

Don’t Overfit Near-parallel Situations

- Security has a key differentiator from the Porsche example:
  - Regulatory frameworks won’t incentivize investment in a Porsche SUV
  - Your target ***is*** externally incentivized to invest in security

- In this case, realize you have two “customers” to please
  - Your target
  - Regulators

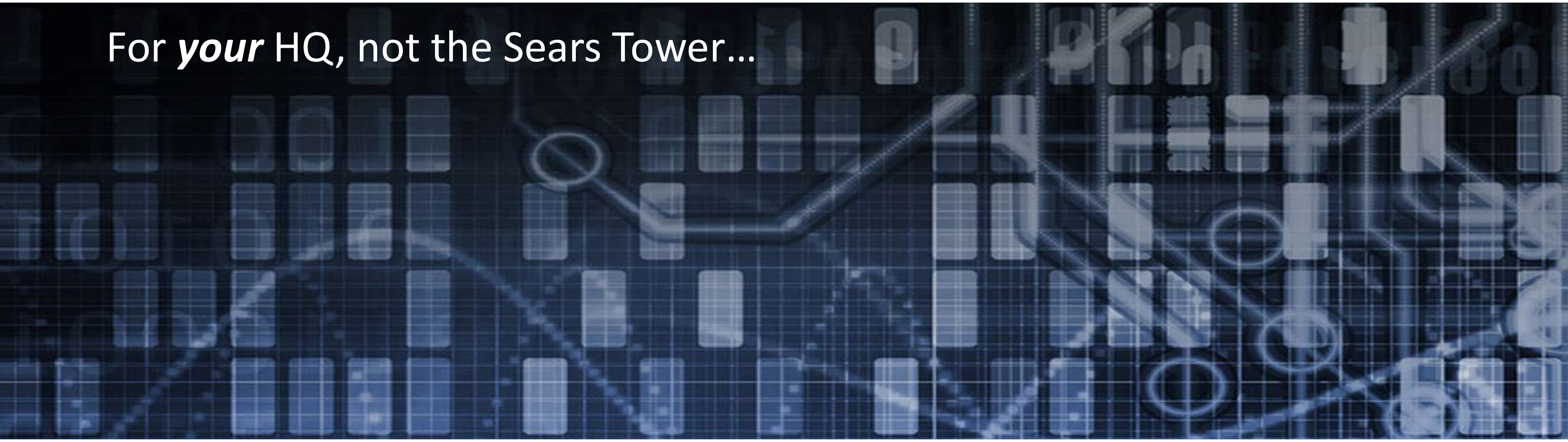
- Regulators (and security-focused staff) value things your target probably will not

Case Study: Subaru Can’t Compete On Price

- Subaru needed to capture more market share
- Taking market share from Toyota was a goal, but they couldn’t compete on price alone
  - Crash test ratings were a key differentiator
  - Nobody was paying for better crash test ratings
- Subaru created an ad campaign highlighting the thing every parent with a driving teenager thinks about
  - Subaru became a market leader to a ***very specific*** market

Case Study: Subaru

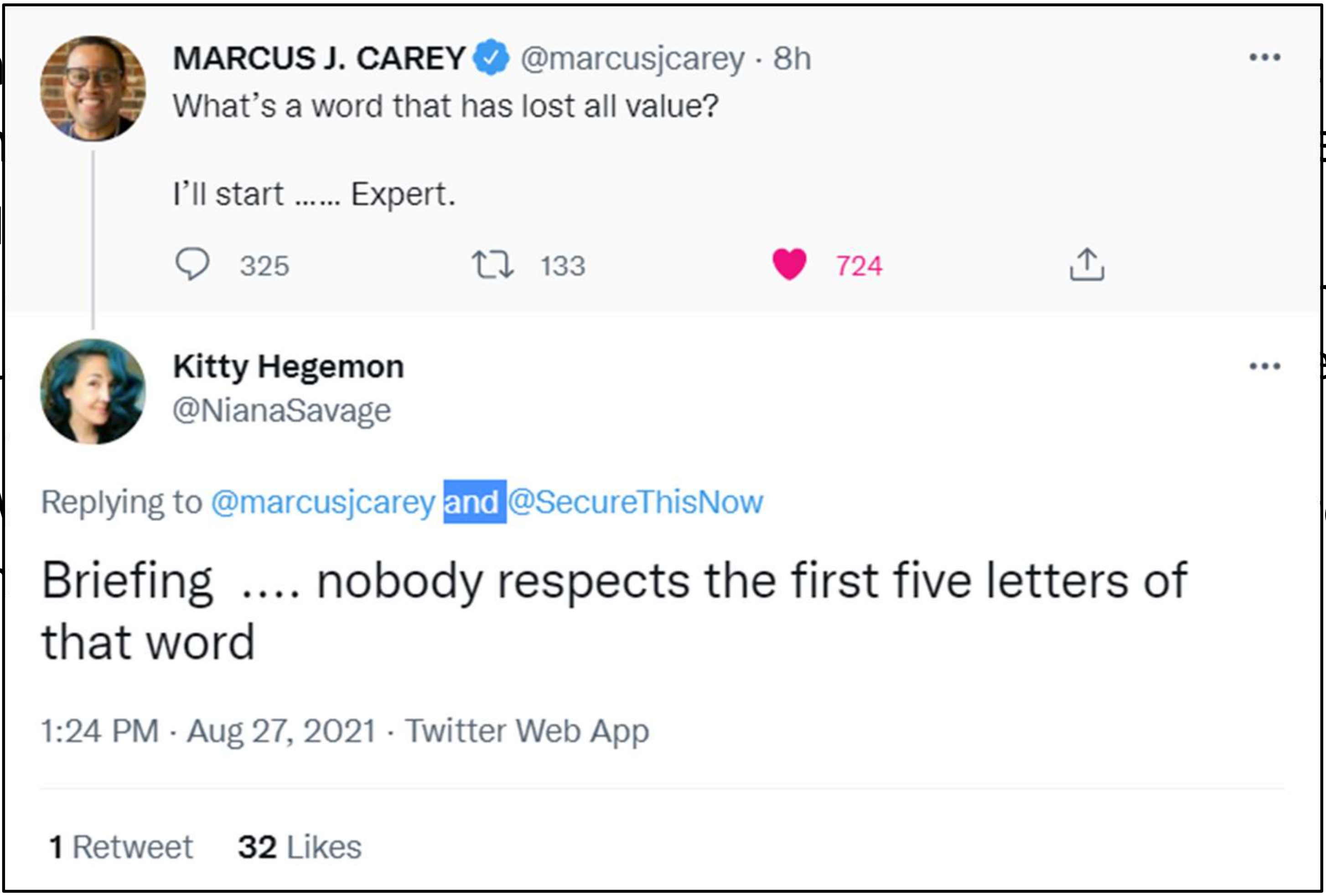
Security Elevator Pitches



For ***your*** HQ, not the Sears Tower…

Elevator Pitch

- When ly want the sh erstand
  - And und now secu erstand the
  - "BT e're goin



MARCUS J. CAREY @marcusjcarey · 8h

What's a word that has lost all value?

I'll start …… Expert.

325 133 724

Kitty Hegemon
@NianaSavage

Replying to @marcusjcarey and @SecureThisNow

Briefing …. nobody respects the first five letters of that word

1:24 PM · Aug 27, 2021 · Twitter Web App

1 Retweet 32 Likes

Elevator Pitch (2)

- Have an elevator pitch ready to capitalize on impromptu opportunities to evangelize the Blue Team

- Include a touch point, keep it brief, and demonstrate value
  - “As you doubtless know from media reports, computer security continues to be a problem. The Blue Team ensures that our networks are defended/customers are protected, freeing IT to focus primarily on supporting revenue generating operations.”

Blue Team Value Objections

They’re all wrong, but they ***are*** objections you may encounter

Objection: Shouldn't good security/defense be a default?

- Let's just agree that it should be
  - But IT is busy herding cats

- Note that IT will almost always prioritize availability over everything else
  - And we want them to
  - Because we pay them to

- Blue Team ensures that someone is always focusing on the rest of the security triad

Objection: Shouldn’t good security/defense be a default? (2)

- In manufacturing, the idea of having a dedicated advocate for something that is “everyone’s job” will be very familiar

- Expediters are people who figure out where to “jump the line” to ensue particularly sensitive orders ship on time

- Shipping orders is everyone’s job, but having people focused only on must win battles lets everyone else focus better on their individual roles

Objection: Security Metrics Are Worse

- It’s the job of the Blue Team to identify security issues and the visibility gaps that create those issues
  - When visibility gaps close, detections increase
  - This is especially true with newer security programs

- Your security position isn’t worse – you can just see it now
  - Enron’s financial position didn’t get worse when independent auditors began reviewing their books
  - We just got a chance to see reality for the first time

Objection: IT Knows What Attacks Look Like

- First, this is rarely true
  - When dealing with this objection, note your own objection and then cede the point

- Focus on the point: IT should no more be focusing on ensuring security than Blue Team should build and deploy infrastructure
  - Are there stalled IT projects that should be enhancing revenue?
  - Is management satisfied with IT SLAs?

- These are clear signs that IT has plenty of non-security work

Objection: Blue Team is Delaying Release

- So you wanted to release a vulnerable product?
  - Nobody ever does, but you can't fix all possible issues before release
- When teaching SDLC, we recommend setting a "bug bar" that precommits the org to what will delay a release
- If leadership agrees the bug bar is a good idea (hard to argue against), then it's just a matter of who will handle evaluation and triage of security issues
  - Blue Team is well positioned for this
  - They will also need to implement detections for the unresolved issues

Objection: Blue Team is Demanding Outages

- This typically indicates the Blue Team is demanding outage windows for emergency patches
  - The debate is usually only because the outage is impacting business
- Setting a vulnerability bar (much like an SDLC bug bar) is the best defense against this objection
  - It effectively constrains the org on the conditions under which business will be conducted
  - This turns security (and the Blue Team) into a guiding principle

Objection: Everyone Knows What Good Looks Like

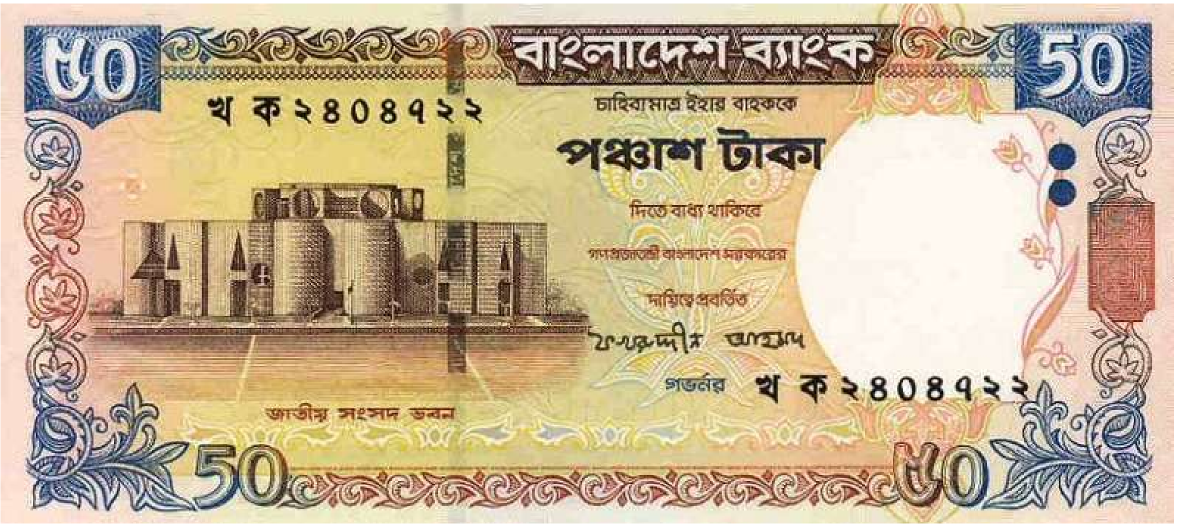
- This is my absolute favorite objection
  - It is usually levied when discussing building baselines to detect and alert on anomalies

- Few people notice the detail around them in their daily lives, let alone in complex processes like enterprise IT systems

- But people feel like they are far more observant than they are
  - Let’s demonstrate this with a little experiment…

So About Those Baselines…

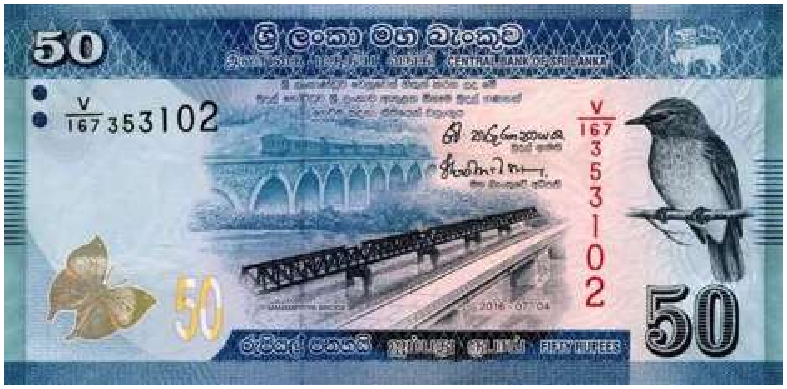
- We need to explain why investing in baselining the network is important, when management thinks we should "just know"
- I like to ask "can you find the problem with this counterfeit 50 Sri Lankan Rupee bill?"



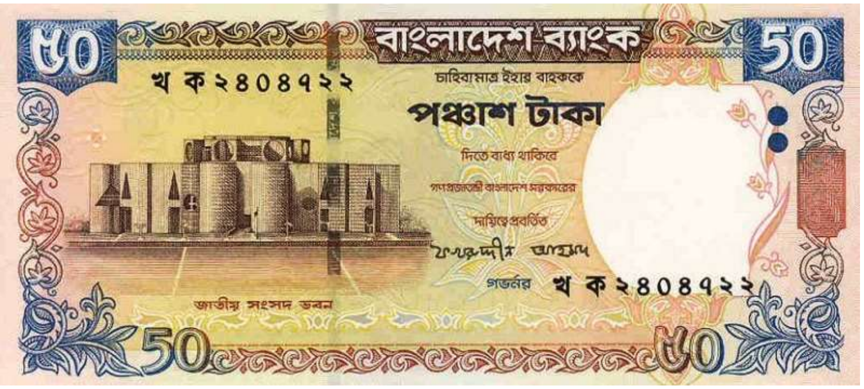
So About Those Baselines… (2)

- Plot twist - it's not counterfeit!
  - But without a baseline in what a normal Sri Lankan bill looks like, how would you know that?!

Sri Lankan
50 Rupees



Bangladeshi
50 BDT



Finalizing Value Proposition

Remember – value is a matter of perception

A Few Key Points

- Always remember that the main goal of a business is to keep doing business while maximizing profit
  - “Detecting and preventing exploitation” are adjacent to maximizing profit, but are ***not*** the same

- Always bring definitions of value proposition back to the overarching mission of the organization
  - Never forget that infosec is a cost center
  - Do not pretend that “avoiding a regulatory fine” is not the same thing as “saving the organization money”

DNT – Listen FTW!

- A sales tactic for listening to prospects without talking too much is to take furious notes while the prospect talks
  - In a conversation, only one person should be talking
- Either the prospect is telling you ***what they value*** or you’re trying to tell the prospect ***what to value***
  - The former lets you tailor your message and demonstrate value
- One salesperson recalls just scribbling DNT over and over again on their notepad while the prospect tells them their needs
  - DNT means “Do Not Talk”

Closing Thoughts

- Think like a salesperson
  - Start by learning how "value" is defined by your target
  - Default to maximizing profit
- Learn and use the language of stakeholders
  - People like people like themselves
- Be ready to address common objections
  - Every salesperson has lines ready for objections
  - You should too

Jake Williams

@MalwareJake

@BreachQuest

BreachQuest

breachquest.com