

Patching Your Users

Defending against the Social Engineering Threat

Pareto had it right:

20% of our efforts will produce 80% of our results.

Numerous Studies:

Human error and internal threat responsible for more than **80%** of Information Security breaches

BUT

Only **29%** of organizations consider security training as a crucial requirement in preventing security breaches within organizations.

area

e Changing Threat Environment

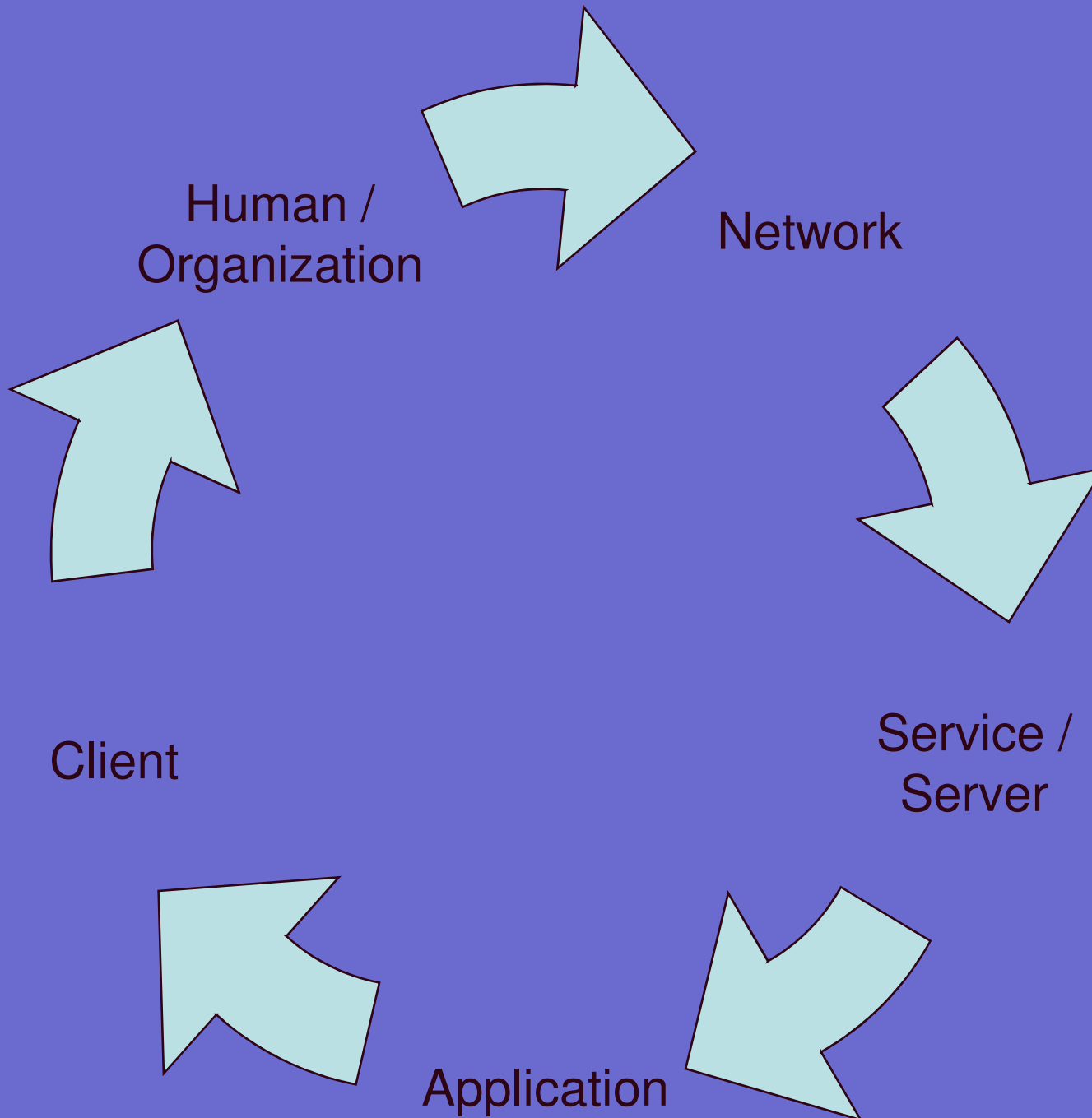
cial Engineering

our Security Awareness Sucks

aking it really work.

A History Lesson....

The Vulnerability Cycle



Early Years

Those were the days

Software Vulnerabilities weren't significant - most based on configuration weakness

Only a handful of people understood how to exploit technologies

Small Target Surface - Few internet-connected computers

Focus was on phone phreaking and academia

Social Engineering reigned supreme

Most successful attacks involved social engineering

Unsophisticated controls environments

Few understood the jargon

Policies encouraged trust over security



Two Vital Dates

October 13, 1994

- Mosaic Netscape 0.9 released
- The web becomes easy to navigate

August 24, 1995

- Windows 95 Released
- Home computer use proliferates massively

The Internet Experiences exponential growth

Money starts to change hands

Internet connected computers become a viable target

This creates a target rich environment...

Smashing Computers Memory

Crack 49 - November 8, 1996.

Aleph1 - Smashing the Stack for Fun and Profit

readily available exploit code actually makes breaking into computers easier

The “golden age” of server hacking begins.

1996-2003 - More of the same

Memory attacks become more sophisticated

Polymorphic shell-code designed to evade detective controls

More advanced use of memory spaces (format strings, integer expl

Windows XP Service Pack 2 Appears

Microsoft finally hardens their operating systems

The world changes overnight

Security is now baked in to the computer.

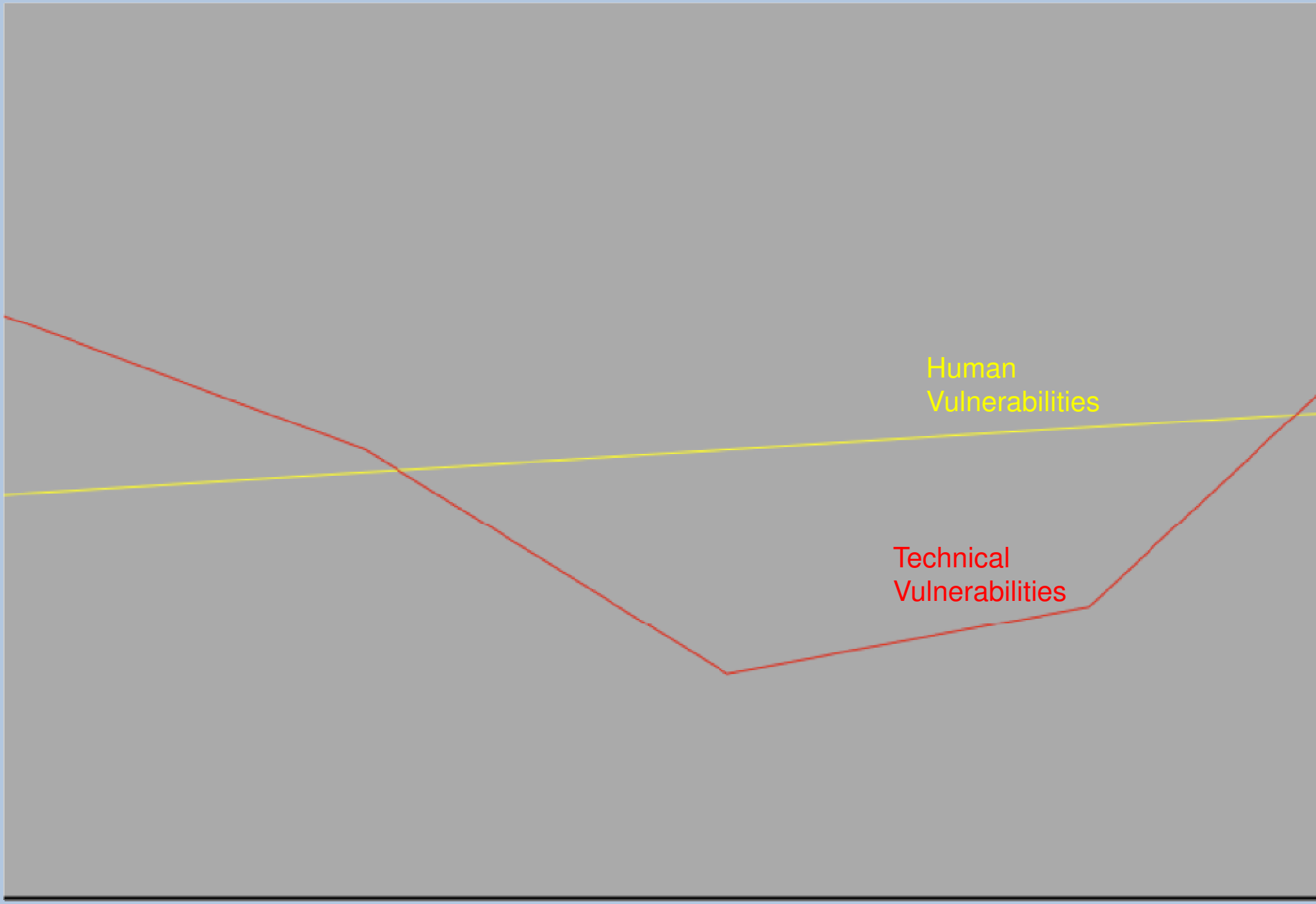
Server based vulnerabilities disappear

As massive server-based vulnerabilities disappear, client interaction becomes key

The number of issues continues to increase but the type of issues start to change radically

Security of Information

of



1985

1995

Human
Vulnerabilities

Technical
Vulnerabilities

since 2005

No major direct-exploitation worm outbreaks

Less than a handful of “remote root” direct exploitation vulnerabilities

Major Classes of Attacks

Drive-by Download

Exploitation through Email, Web and Social Networking Sites

Phishing / Pharming / Spear-Phishing

What’s the similarity?

If you said “human interaction”, you get a gold star.

human/organization are the main exploit targets ag

Social Engineering

defined (by Wikipedia):

"The practice of obtaining confidential information by manipulating users."

The Art of Exploiting Human Weakness

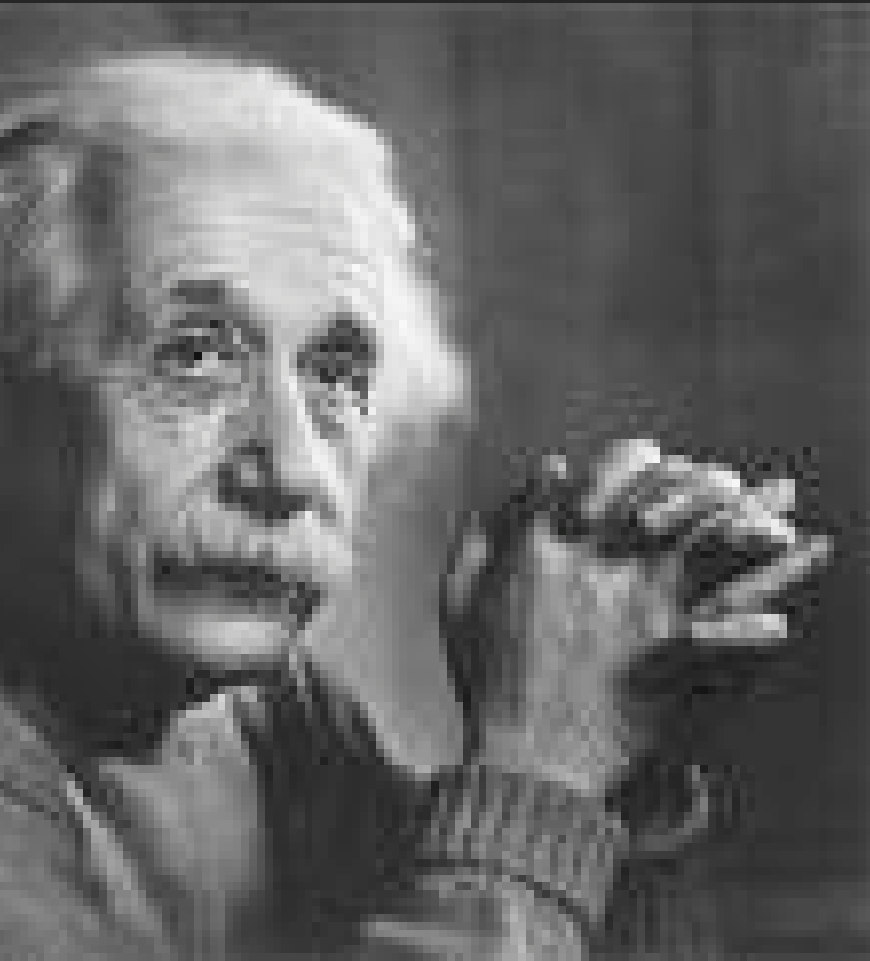
Humans are social creatures

Human nature makes us vulnerable to each other

Social engineers exploit weaknesses in human nature to obtain information or access to computer systems.

"A Confidence Trick - Social Engineering is the age-old art of the Confidence Man"

The bad guys are exploiting your people



*Only two things are
infinite: the universe and
human stupidity.*

*And I'm not sure about
the former.*

- Albert Einstein

There is no patch for human stupidity.

Security Awareness Training

the solution for social engineering

Train your users on security topics

Use case-study training and scenarios so that users understand.

Ensure that users complete at least one multiple-choice test per quarter

Make sure that users pass, and they are now “aware”.

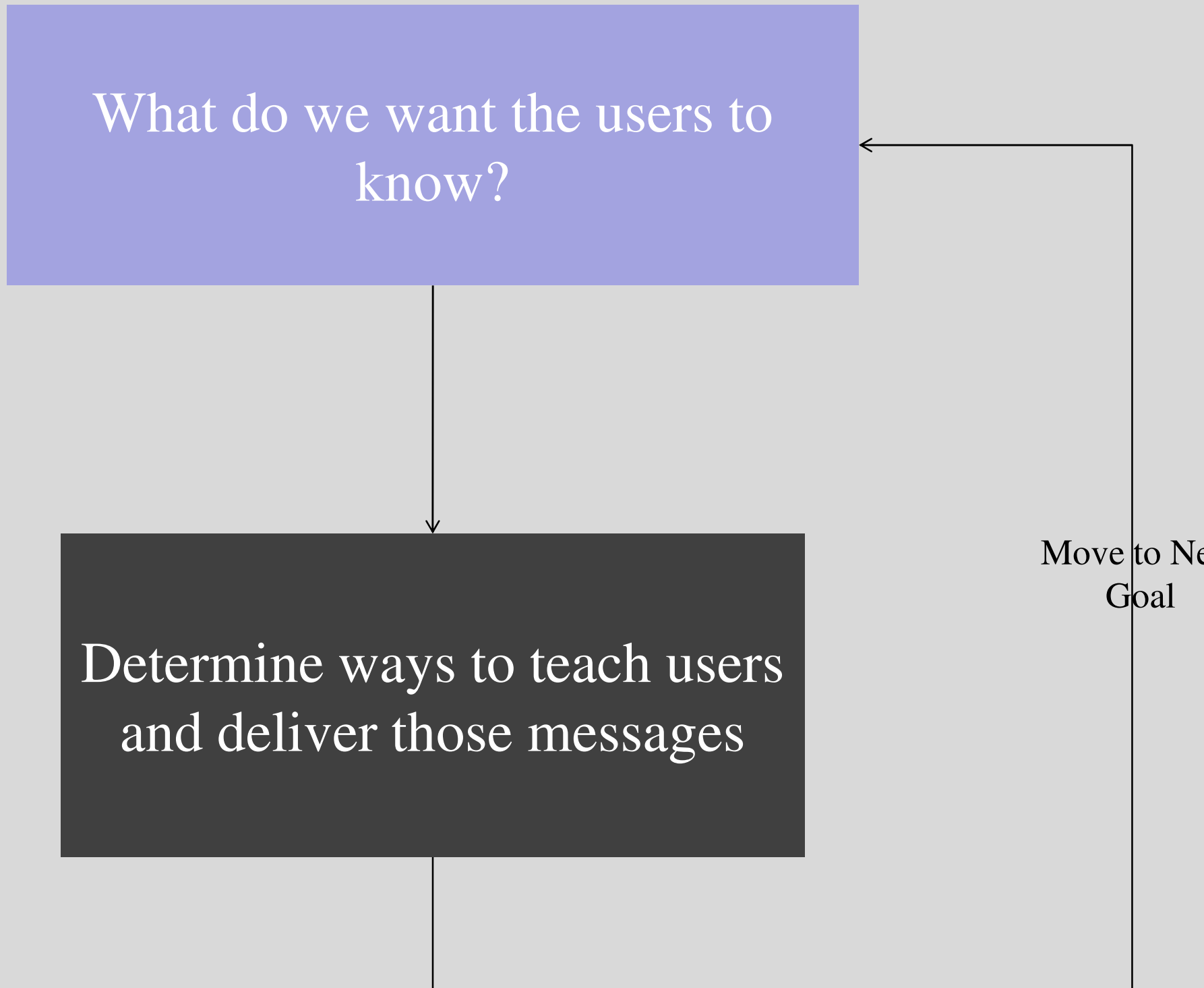
Two step process

Decide what we want the user to know

Find ways to “train” them on those things.

This is how most corporations are approaching user protection

Security Awareness Process



What do we want the users to know?

Determine ways to teach users and deliver those messages

Move to Next Goal

...
e recently surveyed a number of security pros in orgs w
curity awareness programs:

*If you could wake up tomorrow and the users understood 3 things
ecurity, what would they be?"*

e heard answers like:

Separation of duties / Principle of Least privilege

Seeing the big picture of enterprise security

Password Hygiene

Internet Hygiene

How to do business WHILE following policy

That security is their responsibility.

That there really are bad people who are out to get them.

Infosec isn't there to stop you from doing your job.

So...

Why Don't They Know Those Things Already?

Typical CISO/CIO/General Counsel Response:

We Trained Them!!!

They should have “Security Awareness”!!!

Explanation #1

“Users are stupid.”*

Training Doesn't Work

People aren't puppies

Requires significant funding

Low uptake level – most users ignore or go through the motions.

The only way to “rub their noses in it” is through an incident

Training is the first thing to cut

When cutting costs, training is viewed as a luxury.

More importantly, ROI is generally not measured

“Success” is nebulous at best

“Training” is the wrong model

ing and a problem

we have two main issues in getting users on-board

Users view security as a braking (breaking?) function

Users believe security is solved by the Information Security Department and that it's not their responsibility.

the biggest problem:

NEITHER OF THESE ARE TRUE!

these are both perception issues

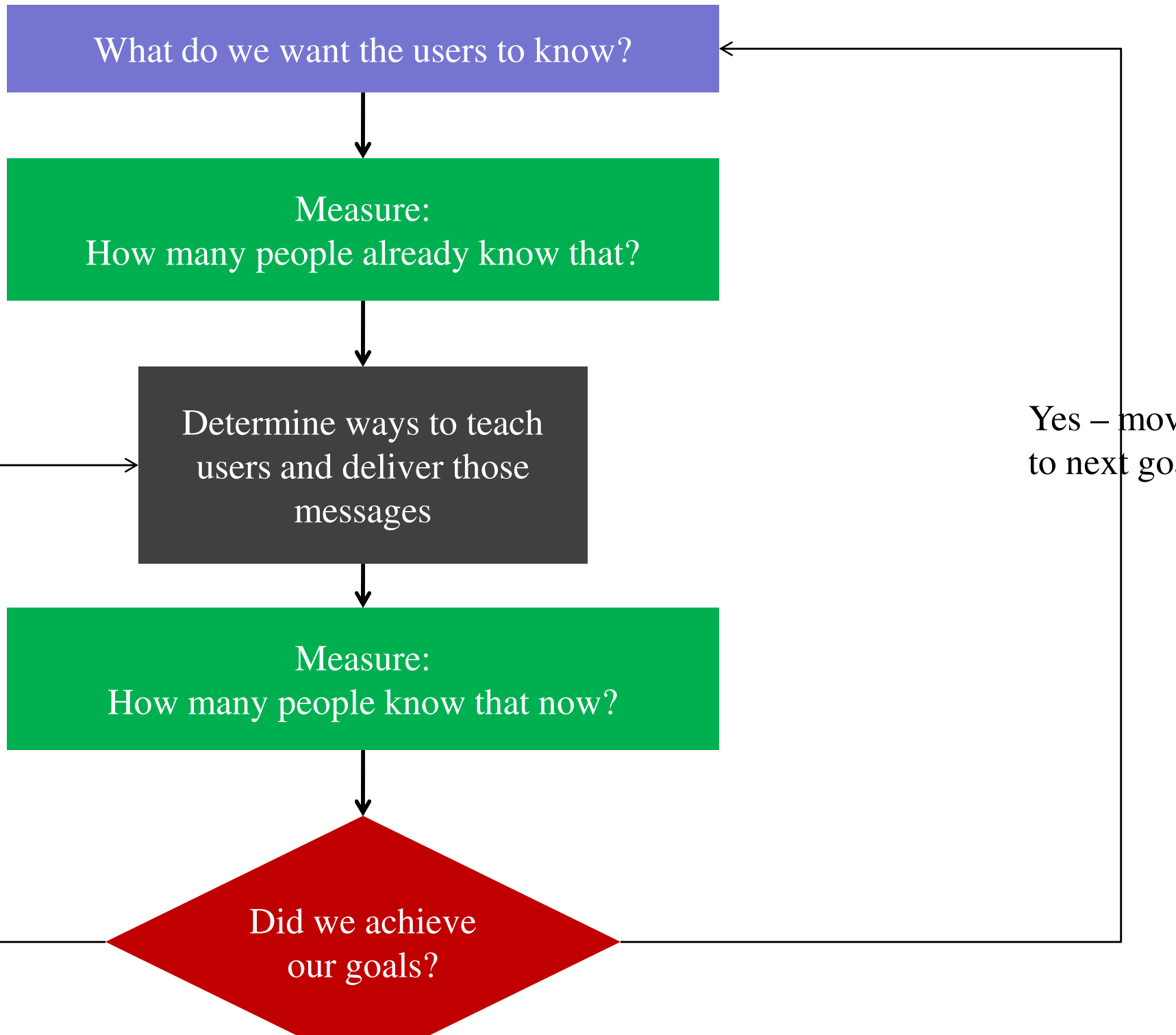
how do other industries solve perception issues?

Explanation #2

“Your marketing sucks.”

Mark Stevens

Marketing Process



Measurement is Key

Good Marketers Measure their Impact

This involves understanding how their messages impact their target

Goals need to be set based on measurability

Define your goals based on how you will measure them

You Need a Baseline

Measure before you start your “Awareness” efforts

This lets you know how many of your users are already aware

Measure at the End

This gives you an idea of the success of your efforts

This is called “ROI”.

Position and Reality

Positioning is the art of changing reality.

The technique by which marketers try to create an image or identity in the minds of target market for its product, brand, or organization. (Wikipedia)

The key question is: How are we positioned?

Strong positioning is the key to strong marketing

What is the position of the following brands?

- Rolls Royce
- Ferrari
- Chevy
- Information Security within Your Organization?

What position do you want to have?

What would make you think that?

Warning: Fear Message

veat: It's far easier to say it than to do it.

They have a say in this process too.

Positioning is a dance between what the users think and what you

is means you have to say it often.

Rule of thumb: a user has to see your message **at least 7 times** before your message has ANY effect

This is the main reason that “awareness training” doesn't work!!!

Breaking the “Awareness Shield”

Users are marketed to repeatedly

We need to break through their “awareness shield”.

Marketing

The art of creating favorable impressions in your target audience

Tools of Marketing

PR

Advertising

Direct Interaction

Does this work internally???

Steps to Executive Marketing

Marketing is an integrated process

Identify innovative initiatives that can command the attention of the marketplace

Integrate all the elements of your marketing program

Do not engage in any initiatives that fail to produce positive ROI

Pick the low hanging fruit first

Don't be linear

Be persistent, relentless, inventive, counterintuitive, challenging, combative
Strategic and tactical.

(Mark Stevens, Your Marketing Sucks)

Goal

Client wants to teach their users to select strong passwords where password controls are not enforceable (e.g. cloud services)

Security Awareness Plan

Send emails telling people to choose strong passwords

Ask users to take multiple choice test that confirms that they know how to create strong passwords.

Study: Strong Passwords

Security Marketing Campaign

Step 1: Measure strength of passwords chosen for baseline

- Tools: survey random set of users, create application and test strength, etc.

Step 2: Create Marketing Campaign

- Send emails to users – both instructional and examples that offer resources
- Use multiple choice tests
- Newsletters, articles, etc.
- Repeat messages over short period of time

Step 3: Measure strength of passwords, look for changes.

- Use SAME measurement technique as baseline

Did we get results? If no, repeat step 2 *with different tactics*.

Questions?

Feel free to email:

mike@foregroundsecurity.com