RSACONFERENCE2014
FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Share.
Learn.
Secure.
Capitalizing on
Collective Intelligence

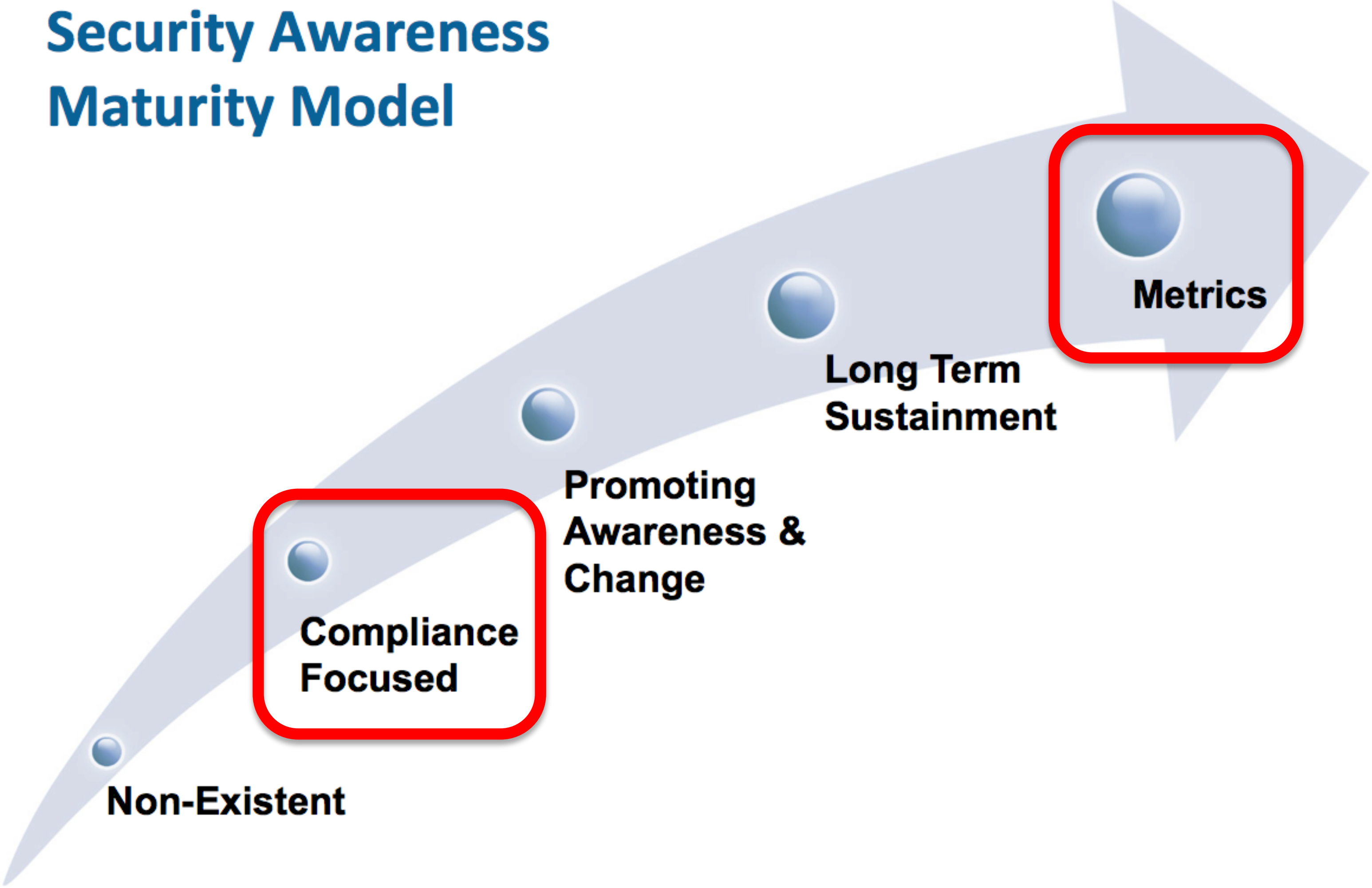
Measuring Change in Human Behavior

SESSION ID: HUM-T07B

Lance Spitzner

Training Director
SANS Securing The Human
@lspitzner

Security Awareness Maturity Model



Non-Existent

Compliance Focused

Promoting Awareness & Change

Long Term Sustainment

Metrics

Two Type of Security Awareness Metrics

- Metrics that measure the deployment of your awareness program. - Are you compliant?
- Metrics that measure the impact of your awareness program. – Are you changing behavior?

- Focus on a few good metrics.

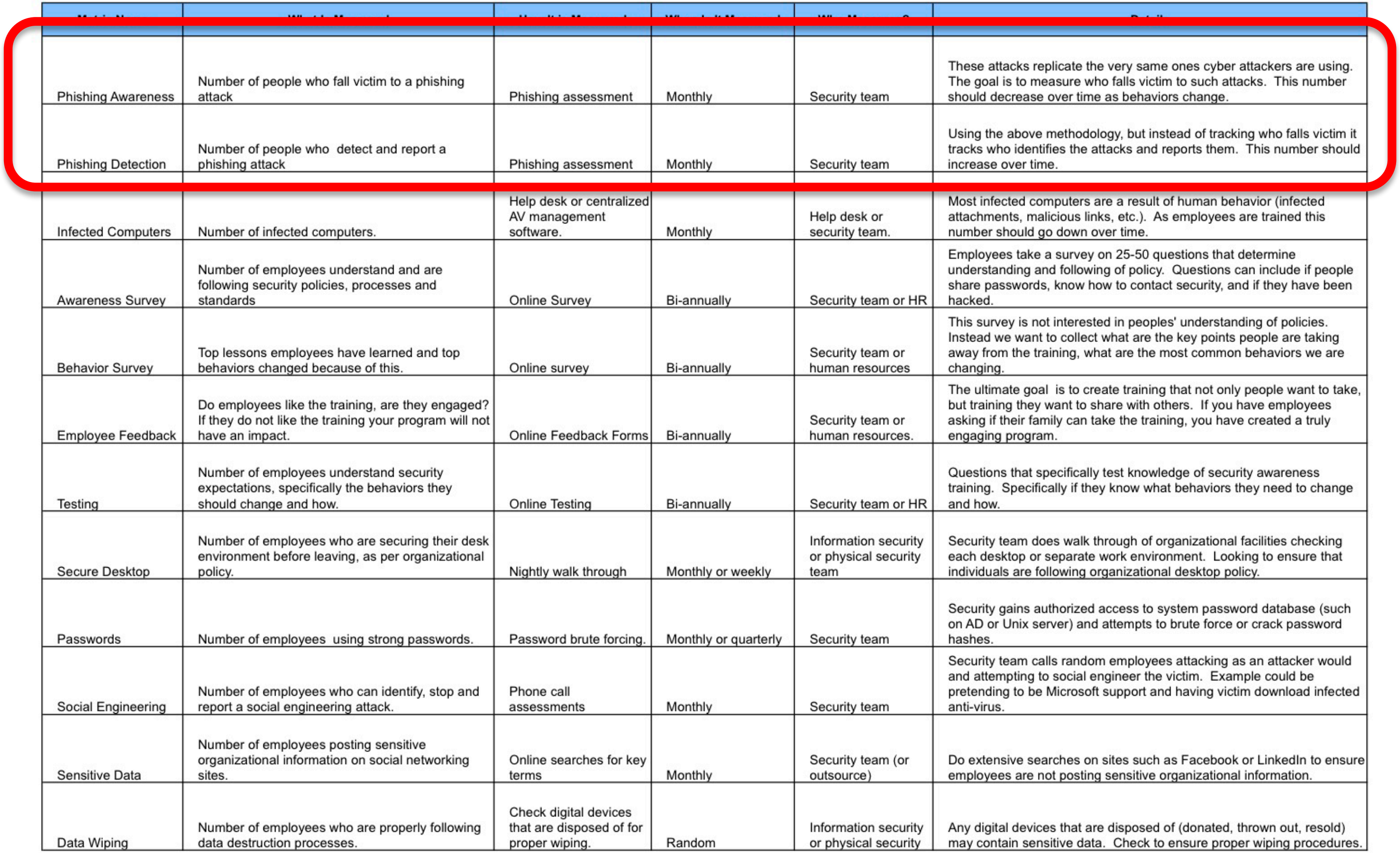
Just Ask

- What is one thing you have learned as a result of this training?
- What behavior have you changed as a result of what you learned?

Traditional vs. Human Security Metrics

- Often human metrics are assessments. Just like any other assessment, make sure you have approval.
- Unlike computers, people have feelings. The challenge is creating / implementing metrics that people like.
- Having trouble getting approval? Do a trial against HR / Legal.

Metrics That Measure the Impact of Your Program



Metric Name	What is Measured	How it is Measured	When is it Measured	Who Measures ?	Details
Phishing Awareness	Number of people who fall victim to a phishing attack	Phishing assessment	Monthly	Security team	These attacks replicate the very same ones cyber attackers are using. The goal is to measure who falls victim to such attacks. This number should decrease over time as behaviors change.
Phishing Detection	Number of people who detect and report a phishing attack	Phishing assessment	Monthly	Security team	Using the above methodology, but instead of tracking who falls victim it tracks who identifies the attacks and reports them. This number should increase over time.
Infected Computers	Number of infected computers.	Help desk or centralized AV management software.	Monthly	Help desk or security team.	Most infected computers are a result of human behavior (infected attachments, malicious links, etc.). As employees are trained this number should go down over time.
Awareness Survey	Number of employees understand and are following security policies, processes and standards	Online Survey	Bi-annually	Security team or HR	Employees take a survey on 25-50 questions that determine understanding and following of policy. Questions can include if people share passwords, know how to contact security, and if they have been hacked.
Behavior Survey	Top lessons employees have learned and top behaviors changed because of this.	Online survey	Bi-annually	Security team or human resources	This survey is not interested in peoples' understanding of policies. Instead we want to collect what are the key points people are taking away from the training, what are the most common behaviors we are changing.
Employee Feedback	Do employees like the training, are they engaged? If they do not like the training your program will not have an impact.	Online Feedback Forms	Bi-annually	Security team or human resources.	The ultimate goal is to create training that not only people want to take, but training they want to share with others. If you have employees asking if their family can take the training, you have created a truly engaging program.
Testing	Number of employees understand security expectations, specifically the behaviors they should change and how.	Online Testing	Bi-annually	Security team or HR	Questions that specifically test knowledge of security awareness training. Specifically if they know what behaviors they need to change and how.
Secure Desktop	Number of employees who are securing their desk environment before leaving, as per organizational policy.	Nightly walk through	Monthly or weekly	Information security or physical security team	Security team does walk through of organizational facilities checking each desktop or separate work environment. Looking to ensure that individuals are following organizational desktop policy.
Passwords	Number of employees using strong passwords.	Password brute forcing.	Monthly or quarterly	Security team	Security gains authorized access to system password database (such on AD or Unix server) and attempts to brute force or crack password hashes.
Social Engineering	Number of employees who can identify, stop and report a social engineering attack.	Phone call assessments	Monthly	Security team	Security team calls random employees attacking as an attacker would and attempting to social engineer the victim. Example could be pretending to be Microsoft support and having victim download infected anti-virus.
Sensitive Data	Number of employees posting sensitive organizational information on social networking sites.	Online searches for key terms	Monthly	Security team (or outsource)	Do extensive searches on sites such as Facebook or LinkedIn to ensure employees are not posting sensitive organizational information.
Data Wiping	Number of employees who are properly following data destruction processes.	Check digital devices that are disposed of for proper wiping.	Random	Information security or physical security	Any digital devices that are disposed of (donated, thrown out, resold) may contain sensitive data. Check to ensure proper wiping procedures.

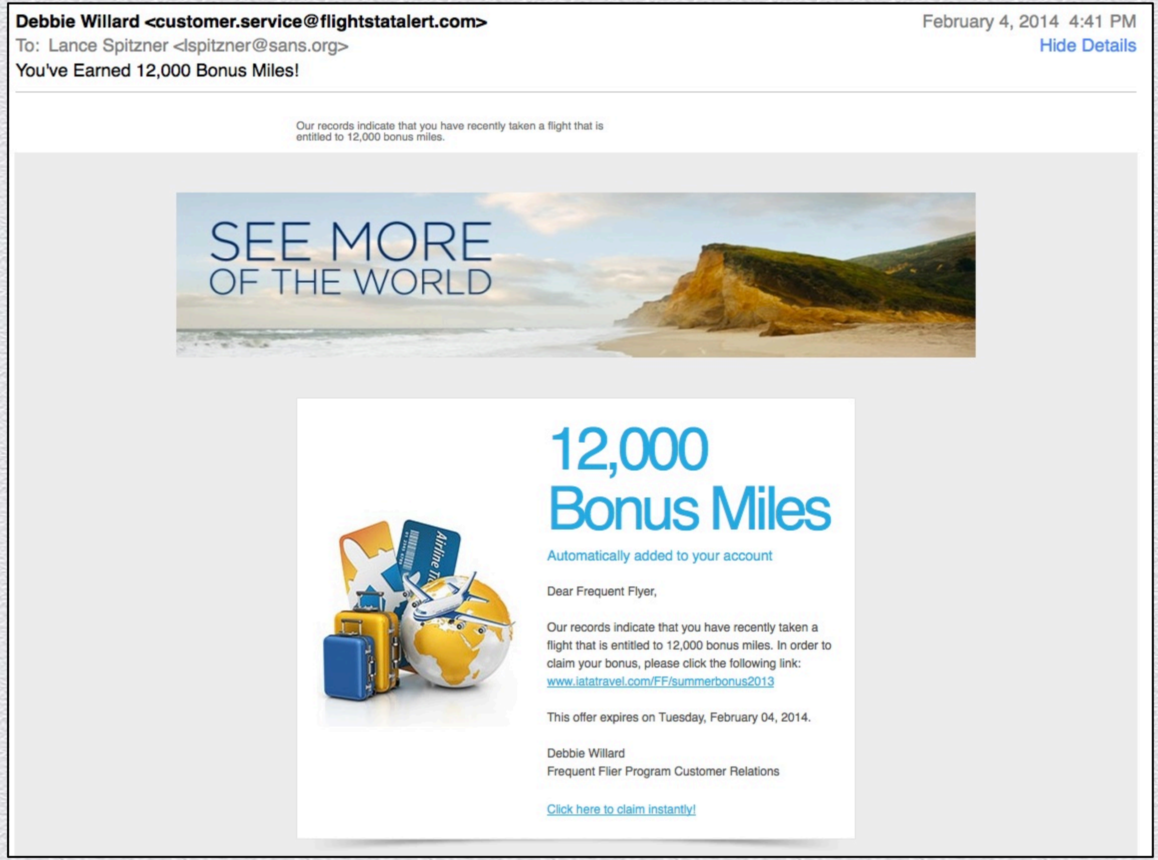
Why Phishing?

Recreate the very same attacks that the bad guys are launching. Excellent way to measure change in behavior.

- Measures a top human risk
- Simple, low cost and easy to repeat
- Quantifiable measurements
- Actionable

Key Points for Success

- Recommend monthly or quarterly.
- Explain program ahead of time, then start slow & simple.
- Never embarrass people, no Viagra phishing emails nor release names who fell victim.
- Only release names to senior mgmt for repeat offenders.
- Ensure at least 2-3 ways people could have detected test.
- 90% of victims in first hour.



Debbie Willard <customer.service@flightstatalert.com>
To: Lance Spitzner <lspitzner@sans.org>
You've Earned 12,000 Bonus Miles!

February 4, 2014 4:41 PM
Hide Details

Our records indicate that you have recently taken a flight that is entitled to 12,000 bonus miles.

12,000 Bonus Miles

Automatically added to your account

Dear Frequent Flyer,

Our records indicate that you have recently taken a flight that is entitled to 12,000 bonus miles. In order to claim your bonus, please click the following link: www.iatatravel.com/FF/summerbonus2013

This offer expires on Tuesday, February 04, 2014.

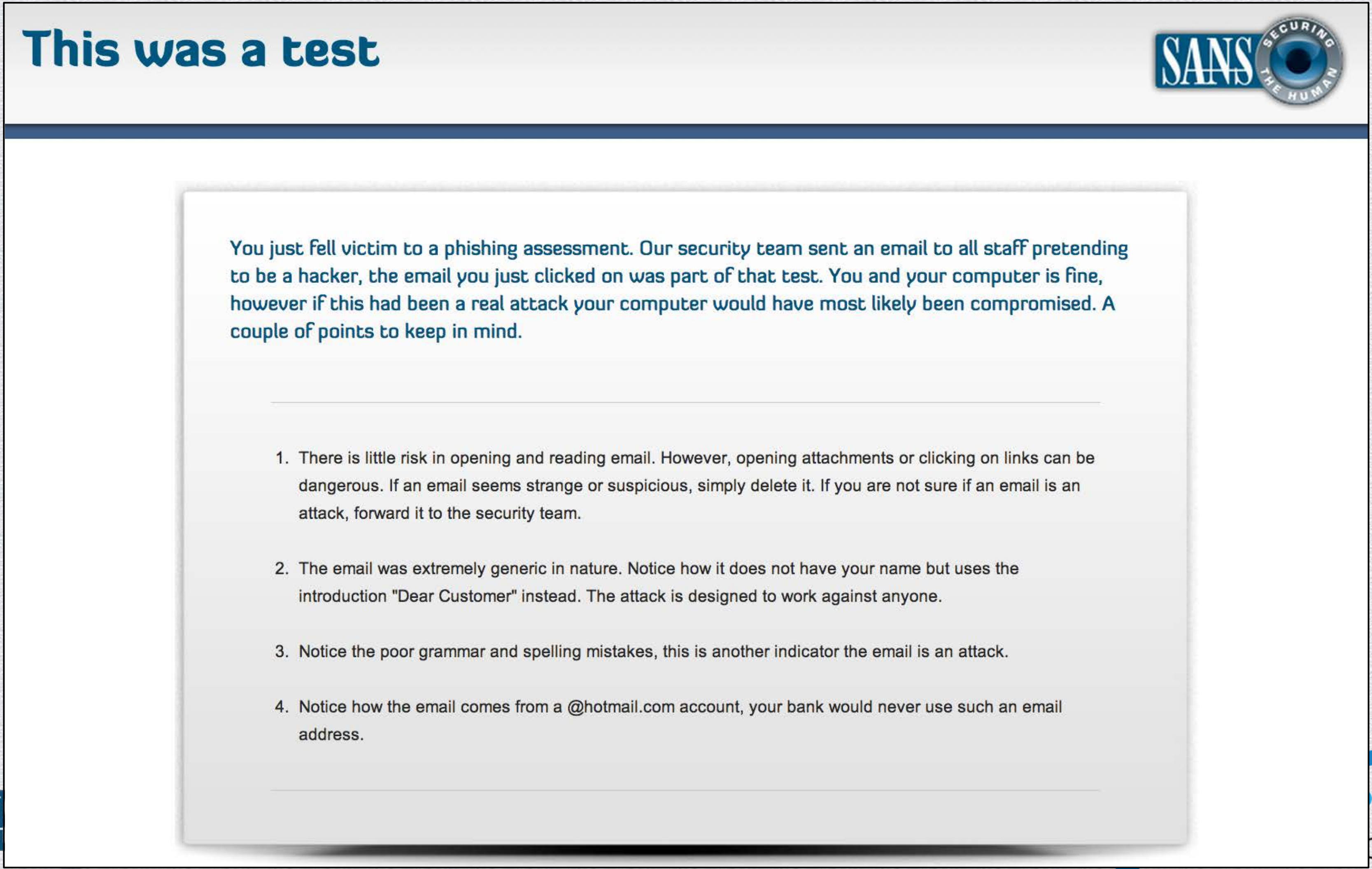
Debbie Willard
Frequent Flier Program Customer Relations

Click here to claim instantly!

Feedback

If an end user falls victim to an assessment you have two general options

- Error message / no feedback
- Immediate feedback



This was a test

You just fell victim to a phishing assessment. Our security team sent an email to all staff pretending to be a hacker, the email you just clicked on was part of that test. You and your computer is fine, however if this had been a real attack your computer would have most likely been compromised. A couple of points to keep in mind.

1. There is little risk in opening and reading email. However, opening attachments or clicking on links can be dangerous. If an email seems strange or suspicious, simply delete it. If you are not sure if an email is an attack, forward it to the security team.
2. The email was extremely generic in nature. Notice how it does not have your name but uses the introduction "Dear Customer" instead. The attack is designed to work against anyone.
3. Notice the poor grammar and spelling mistakes, this is another indicator the email is an attack.
4. Notice how the email comes from a @hotmail.com account, your bank would never use such an email address.

Follow-up

- Send results of test to all employees 24 hours later.
- Explain results and how they could have detected phishing email and what to look for in the future. Include image of phishing email.
- Include your monthly security awareness newsletter.

Trends

- First phish: 30-60% fall victim.
- 6-12 months later: Low as 5%.
- The more often the assessments, the more effective the impact.
  - Quarterly: 19%
  - Every other month: 12%
  - Monthly: 04%
- Over time you will most likely have to increase difficulty of phishing tests, as they become too simple.

Human Sensors

- Another valuable metric is how many reported the attack.
- At some point, may need to develop a policy on what to report. On example.
  - Do not report when you know you have a phish, simple delete.
  - Report if you don’t know (think APT)
  - Report if you fell victim.

Summary

- There are numerous ways to measure human behavior, focus on a few metrics that focus on the key humans risks to your organization.
- Phishing assessments are a common example of how to measure (and reinforce) one of the top human behaviors.

<u>www.securingthehuman.org/resources/metrics</u>