Human Metrics: Measuring Behavior

Lance Spitzner
www.securingthehuman.org/blog
lspitzner@sans.org
@securethehuman
Security Awareness Maturity Model

- Non-Existent
- Compliance Focused
- Promoting Awareness & Change
- Long Term Sustainment
- Metrics
2 Types of 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?
Few Good Metrics

Focus on just a few, high value metrics.

– A metric that measures a human risk or behavior that you care about
– A metric that is actionable
– A metric that is low cost / automate
– A metric that is repeatable
Traditional vs Human Metrics

• Often human metrics are assessments. Just like any other assessment, make sure you have approval.

• Having trouble getting approval? Do a trial against HR / Legal.

• Unlike computers, people have feelings. The challenge is creating / implementing metrics that people like.
# Metrics That Measure the Impact of Your Program

<table>
<thead>
<tr>
<th>Metric Name</th>
<th>What Is Measured</th>
<th>How It Is Measured</th>
<th>When Is It Measured</th>
<th>Who Measures?</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phishing Awareness</td>
<td>Number of people who fall victim to a phishing attack</td>
<td>Phishing assessment</td>
<td>Monthly</td>
<td>Security team</td>
<td>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.</td>
</tr>
<tr>
<td>Phishing Detection</td>
<td>Number of people who detect and report a phishing attack</td>
<td>Phishing assessment</td>
<td>Monthly</td>
<td>Security team</td>
<td>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.</td>
</tr>
<tr>
<td>Infected Computers</td>
<td>Number of infected computers.</td>
<td>Help desk or centralized AV management software.</td>
<td>Monthly</td>
<td>Help desk or security team</td>
<td>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.</td>
</tr>
<tr>
<td>Awareness Survey</td>
<td>Number of employees understand and are following security policies, processes and standards</td>
<td>Online Survey</td>
<td>Bi-annually</td>
<td>Security team or HR</td>
<td>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.</td>
</tr>
<tr>
<td>Behavior Survey</td>
<td>Top lessons employees have learned and top behaviors changed because of this.</td>
<td>Online survey</td>
<td>Bi-annually</td>
<td>Security team or human resources</td>
<td>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.</td>
</tr>
<tr>
<td>Employee Feedback</td>
<td>Do employees like the training, are they engaged? If they do not like the training your program will not have an impact.</td>
<td>Online Feedback Forms</td>
<td>Bi-annually</td>
<td>Security team or human resources</td>
<td>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.</td>
</tr>
<tr>
<td>Testing</td>
<td>Number of employees understand security expectations, specifically the behaviors they should change and how.</td>
<td>Online Testing</td>
<td>Bi-annually</td>
<td>Security team or HR</td>
<td>Questions that specifically test knowledge of security awareness training. Specifically if they know what behaviors they need to change and how.</td>
</tr>
<tr>
<td>Secure Desktop</td>
<td>Number of employees who are securing their desk environment before leaving, as per organizational policy.</td>
<td>Nightly walk through</td>
<td>Monthly or weekly</td>
<td>Information security or physical security team</td>
<td>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.</td>
</tr>
<tr>
<td>Passwords</td>
<td>Number of employees using strong passwords.</td>
<td>Password brute forcing</td>
<td>Monthly or quarterly</td>
<td>Security team</td>
<td>Security gains authorized access to system password database (such on AD or Unix server) and attempts to brute force or crack password hashes.</td>
</tr>
<tr>
<td>Social Engineering</td>
<td>Number of employees who can identify, stop and report a social engineering attack</td>
<td>Phone call assessments</td>
<td>Monthly</td>
<td>Security team</td>
<td>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.</td>
</tr>
<tr>
<td>Sensitive Data</td>
<td>Number of employees posting sensitive organizational information on social networking sites.</td>
<td>Online searches for key terms</td>
<td>Monthly</td>
<td>Security team (or outsource)</td>
<td>Do extensive searches on sites such as Facebook or LinkedIn to ensure employees are not posting sensitive organizational information.</td>
</tr>
<tr>
<td>Data Wiping</td>
<td>Number of employees who are properly following data destruction processes.</td>
<td>Check digital devices that are disposed of for proper wiping.</td>
<td>Random</td>
<td>Information security or physical security</td>
<td>Any digital devices that are disposed of (donated, thrown out, resold) may contain sensitive data. Check to ensure proper wiping procedures.</td>
</tr>
</tbody>
</table>

**NOTE:** These metrics are used to measure the impact of your security awareness program. Specifically how employee understanding and behavior has changed. This is used to measure value of the program, including reducing costs and risk. For more resources visit [http://www.securingsafe.com/resources/planning](http://www.securingsafe.com/resources/planning)
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 automate
- Repeatable and quantifiable measurements
- Actionable
Example

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

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

SEE MORE OF THE WORLD

12,000 Bonus Miles

Automatically added to your account

Dear Frequent Flier,

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.flytravel.com/RFsummerbonus2013

This offer expires on Tuesday, February 04, 2014.

Debbie Willard
Frequent Flier Program Customer Relations

Click here to claim instantly!
Key Points

• Recommend monthly or quarterly
• Announce and explain program ahead of time, then start slow & simple
• Never embarrass people, no Viagra phishing emails nor ‘wall of shame’
• Only release names to senior management when you have repeat offenders
• Ensure at least 2-3 ways people can detect phish
• 90% of victims in first hour.
How To Phish

• URL Shorteners
• E-mail Marketing Solutions
• Cloud Phishing Services
• Pen Testing Software
Lance,

Here are the photos from last week, enjoy!

http://goo.gl/CUlpM

David
From Name: Michelle Hackerton via LinkedIn
From Email: <member@linkedin.com>
Subject: Join my network on LinkedIn

LinkedIn
Michelle Hackerton has indicated you are a Friend
I'd like to add you to my professional network.
- Michelle Hackerton

Accept [Link to View invitation from Michelle Hackerton]

WHY MIGHT CONNECTING BE A GOOD IDEA?
Michelle Hackerton's connections could be useful to you
After accepting Michelle Hackerton's invitation, check Michelle Hackerton's connections to see who else you may know and who you might want an introduction to. Building these connections can create opportunities in the future.

© 2012, LinkedIn Corporation
Create Campaign

What Type Of Campaign Do You Want To Run?

Please choose from the following campaign types:

**Drive-by phishing campaign**

This campaign tries to get the target user to click on a link to a simulated malicious website. When the user clicks the link they are forwarded directly to SpearTraining, or silently fingerprinted and sent to an error page.

**Data entry phishing campaign**

This campaign tries to get the target user to enter in their credentials or other information into a fake web site. Note: Passwords are not collected. Users are then sent to SpearTraining, or silently fingerprinted and sent to an error page.

Create Drive-by Campaign

Create Data Entry Campaign
Click Results

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

– Error message / no feedback
– Immediate feedback that explains this was a test, what they did wrong and how to protect themselves
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.
Team,

As some of you may have noticed we had our monthly phishing assessment this week. As always the purpose of these assessments is to help you identify and protect yourself against common email based attacks. I've attached at the bottom of this email a screenshot of the scam that went out. If this had been a real attack, simply clicking on the attachment could have infected your computer. There were some very simple ways to determine that this was a scam.

1. 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. If your bank had sent you an email it would have used your name.

2. Notice the poor grammar and misspellings, this is another indicator the email is an attack.

3. Notice how the email comes from a @hotmail.com account, your bank would never use such an email address.

As for the assessment, only 13 people fell victim. Great job folks. Finally, be sure to download this month's security awareness newsletter "Social Engineering" from our internal company portal. As always, if you have any questions (or suggestions) about security please contact the help desk.

Thanks!
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.
Violations

- First violation, employee is notified with additional or follow-on training.
- Second violation, employee is notified and manager is copied.
- Third violation, manager is required to have meeting with employee and report results to security.
- Fourth violation, employee reported to HR.
The Impact

• 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: 05%
• Over time you will most likely have to increase difficulty of tests.
Are People Updating Devices?

Qualys® BrowserCheck Summary

1 Security Issue Detected
Scan start time: Tue Apr 08 2014, 11:09 AM
Scan duration: 00:01 (mm:ss)

Follow the recommended actions in the results below to get software updates and resolve security issues.

INFO: For more comprehensive and automated scans install Qualys BrowserCheck Plugin.

Silverlight Plug-In
5.1.20913
Insecure Version
Fix It

Mac OS
10.9.2
Up To Date

Google Chrome
33.0.1750.152
Up To Date

Adobe Flash
12.0.0.77
Up To Date

QuickTime Plug-in
7.7.3
Up To Date
Desktop Physical Security

Does your organization require staff to secure desktops before leaving at night?

- Do sweeps at night.
- Desktops or computers left unsecured, leave note explaining violation.
- Desktops or computers secured, leave Hershey’s chocolate kiss.
Rogue Wi-Fi Access Points

Does your organization require only authorized Wi-Fi Access Points?

– Do sweeps of the organization to find rogue Access Points.

– Implement Network Access Controls to automatically detected unauthorized Access Points.
Summary

Metrics are powerful way to both measure and reinforce your awareness program.

[links to resources]
- securingthehuman.org/resources/metrics
- sans.org/mgt433