Human Metrics: Measuring Behavior

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

- Non-Existent
- Compliance Focused
- Promoting Awareness & Behavior Change
- Long Term Sustainment & Culture Change
- Metrics Framework
Useful Metrics

• Focus on just a few, high value metrics (a metric that measures a human risk or behavior that you care about).
• A metric is a measurement, it does not have value unless you can understand, analyze and act on it.
• Just need to be better then what you had before.
2 Types of Awareness Metrics

1. Metrics that measure the deployment of your awareness program. - Are you compliant?

2. Metrics that measure the impact of your awareness program. – Are you changing behavior?
## Measure the Impact of Your Security Awareness 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>B-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>Updated Devices</td>
<td>Percentage of devices that are updated and current</td>
<td>When employees connect to internal server or use an external service such as browsercheck.qualys.com.</td>
<td>Monthly</td>
<td>Security or technology team.</td>
<td>Measure the behavior if people are keeping their devices updated and current, especially BYOD (Bring Your Own Device).</td>
</tr>
<tr>
<td>Lost/Stolen Devices</td>
<td>Number of devices lost (laptops, smartphones, tablets) that were lost or stolen. What percentage of those devices were encrypted.</td>
<td>Reports to security team or by physical asset audits.</td>
<td>Monthly</td>
<td>Security team or asset management.</td>
<td>Employees should be trained on maintaining physical security of their devices. In addition, if your organization has policies on use of encryption for devices this measures if employees are following that.</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 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>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>Do extensive searches on sites such as Facebook or LinkedIn to ensure employees are not posting sensitive organizational information.</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>Any digital devices that are disposed of (donated, thrown out, resold) may contain sensitive data. Check to ensure proper wiping procedures. Check any rubbish bins or dumpsters for any sensitive documents that were not shredded.</td>
</tr>
<tr>
<td>Data Wiping or Destruction</td>
<td>Number of employees who are properly following data destruction processes.</td>
<td>Check digital devices that are disposed of for proper wiping. Check dumpsters for sensitive documents.</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. Check any rubbish bins or dumpsters for any sensitive documents that were not shredded.</td>
</tr>
<tr>
<td>Device Physical Security</td>
<td>Number of employees who left their devices unsecured in the cars in the organization’s parking lot.</td>
<td>Do a physical walk through of the parking lot and identify any cars that have devices that are visible on a car seat.</td>
<td>Monthly</td>
<td>Information security or physical security</td>
<td>While your organization’s parking lot may be a secured environment, this measures employee behaviors. If they are leaving devices in their car unsecured or visible, they are most likely doing it when off facilities also.</td>
</tr>
<tr>
<td>Facility Physical Security</td>
<td>Number of employees who understand, follow, and enforce your policies for restricted or protect access to facilities.</td>
<td>Test how many employees are wearing their badges or stopping those who are not.</td>
<td>Monthly or weekly</td>
<td>Information security or physical security</td>
<td>For many organizations physical security is a major control in reducing risk, especially when dealing with secured facilities. This metric will test and measure peoples’ understanding and enforcement of this control.</td>
</tr>
</tbody>
</table>
Example Metric - Phishing

Recreate the very same attacks that the bad guys are launching. Excellent way to measure human risk and the mitigation of that risk (change in behavior).

- Measures a top human risk
- Simple, low cost and easy to automate
- Easy to analyze
- Actionable
Key Points

• Computers do not have feelings, people do. Remembering this is key for any human metrics program.
• Announce and explain your metrics program ahead of time.
• Start simple, do not try to fail or trick people.
• Do not publicly post names of people who fall victim nor embarrass anyone.
• Only give names to management of repeat offenders.
Get Approval

- Before conducting any type of assessment, make sure you have approval.
- Can’t get approval, try a test run against the blockers (HR, Legal)
- Make sure security team knows ahead of time, let them know each time when you do it and whom to contact when things go wrong
How Many to Assess?

• Most metrics use a statistical sampling, you may not have the time or resources to test everyone.
• Take lessons learned from sample and apply to whole organization.

www.surveysystem.com/sscalc.htm
Starting Simple

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.istanbul.com/fffsummerbonus2013

This offer expires on Tuesday, February 04, 2014.

Debbie Willard
Frequent Flier Program Customer Relations

Click here to claim instantly!
Feedback?

If a person falls victim to an assessment you have two options

– No feedback / error message
– 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.
Repeat Offenders

- 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.
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.
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.

<table>
<thead>
<tr>
<th>Software</th>
<th>Version</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Silverlight Plug-In</td>
<td>5.1.20913</td>
<td>Insecure Version</td>
</tr>
<tr>
<td>Mac OS</td>
<td>10.9.2</td>
<td>Up To Date</td>
</tr>
<tr>
<td>Google Chrome</td>
<td>33.0.1750.152</td>
<td>Up To Date</td>
</tr>
<tr>
<td>Adobe Flash</td>
<td>12.0.0.77</td>
<td>Up To Date</td>
</tr>
<tr>
<td>QuickTime Plug-in</td>
<td>7.7.3</td>
<td>Up To Date</td>
</tr>
</tbody>
</table>
Physical Security Behaviors

• See if unauthorized person can enter or walk around facilities without an ID badge

• Check desktops to make sure computer screens are locked and there is no sensitive information left on desks

• Check parked cars for mobile devices left in open
Human Vulnerability Scanner

• Sometimes the simplest way to measure a behavior is simply ask.
• Survey can measure behaviors that you normally do not have access to.
• Think of the human risk survey as the human vulnerability scanner.
Data May Already Be There

• There may not be a need to collect data as you already have the data. Check with
  – Security Operations Center
  – Incident Response Team
  – Help Desk
  – Human Resources

• Example: Number of infected computers per month.
Summary

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

[link to securingthehuman.org/resources]

[link to sans.org/mgt433]