

## Behavior Metrics

Metric Name	What Is Measured?	How Is It Measured?	When Is It Measured?	Who Measures?	Why is This Being Measured?
<b>Social Engineering</b>					
Phishing Click Rate	Number of people who fall victim to a phishing simulation. The definition of falling victim is clicking on the link or opening an attachment.	Phishing Simulation Program	Monthly	Security / Phishing Team	Phishing is one of the primary and most common attack methods of cyber attackers. This metric measures the succetibility of our workforce to these attacks. The more vulnerable our workforce is the greater the risk. The goal of the awareness program is to reduce the click rate, which reduces overall risk of a phishing incident.
Phishing Reporting	Number of people who detect and report a suspected phishing email.	Phishing Simulation Program	Monthly	Security / Phishing Team	Uses the above methodology, but instead of tracking who falls victim, it tracks who identifies the phishing email and reports them. This number should increase over time. This measures the Human Sensor, key to improving our detection capabilities and reducing attacker dwell time.
Phishing Repeat Offenders	Number of workforce that repeatedly fall victim to phishing simulations. These individuals are not changing behavior and represent a high risk.	Phishing Simulation Program	Monthly	Security / Phishing Team	These individuals represent a high risk as they are not changing behavior and must be addressed. This can include an escalation in training and consequences, being moved to a different job role or department, or being managed in some other way.
Vishing / Smishing	This metrics replicates any of the first three metrics, but instead of measuring against email based attacks this measures again Voice (Vishing) or Messaging (Smishing) attacks	Vishing or Smishing Simulation Program	Monthly	Information Security Team	Just like Phishing (email based), Vishing or Smishing attacks are highly effective and common attack methods of cyber attackers. These attacks are also becoming more common as organizations are getting better at blocking most email phishing attacks.
<b>Passwords / Authentication</b>					
Passwords	Percentage of employees using strong passwords.	Password brute forcing	Monthly or quarterly	Security Team	Strong, long passwords are a key part of securing work accounts. Security gains authorized access to system password database (such as AD or Unix server) and attempts to brute force or crack password hashes, attempting to find any weak / short passwords.
MFA or Password Manager Adoption	What percentage of accounts have enabled MFA or what percentage of workforce has adopted and are using work issues Password Managers	Work with IT Admin or Operational team responsible for deploying the technology	Monthly	Security team or Operations	MFA is considred by many to be one of the most effective means of protecting system accounts and data. Track how extensive MFA adoption is, especially for any sensitive systems or privileged accounts. Same can be done for Password Manager adoption.
Password sharing / reuse	What percentage of the workforce is actively sharing passwords or reusing work passwords for personal accounts	As part of annual Security Culture survey. Accurates results depend on how questions are worded.	Annual	Security Team or Human Resources	Sharing or reusing passwords exposes the organization to tremendous risk. Even if people are using extremely strong passwords, sharing or reusing them for other accounts can compromise the security of them. These behaviors are often best measured by asking your workforce.
<b>Device Security</b>					
Updated Mobile Devices / Screenlocks	Percentage of devices that are updated and current and / or have screenlocks enabled.	Random spot checks, mobile device checkup booths or MDM based software.	Monthly	Security or Technology Team	Ensuring devices remain patched and current are one of the most effective ways to ensure they are secure. Not only does this ensure that the devices have known vulnerabilities patched, but have the latest security features and functionality. Screenlocks ensure security of device if lost.
Lost/Stolen Devices	Number of devices (laptops, smartphones, tablets) that were lost or stolen.	Lost devices reported to security team, physical security team or by physical asset audits	Monthly	Security Team or Asset Management	Employees are far more likely to lose a device or have it stolen than have their device infected with malware. Since lost / stolen devices represent such a high risk, training people on how to physically secure and keep track of them is key.
Secure Desktop	Number of employees who are securing their desk environment before leaving, as per organizational policy.	Physical walk through of facilities	Monthly	Information Security or Physical Security Team	Organizations may have a policy on securing desktops before people leave them unattended (lunch, enf of the workd day). Security team does a walkthrough of organizational facilities, checking each desktop, office space, whiteboard, etc - looking to ensure individuals are following organizational secure desktop / work environment policy.
Mobile Device Storage in Personal Vehicles	Number of employees who left their devices unsecured in their cars in the organization's parking lot.	Do a physical walkthrough of the parking lot and identify any cars that have devices that are visible on a car seat.	Monthly	Information Security or Physical Security	While your organization's parking lot may be a secured environment, this measures employee behaviors. If they are leaving unsecured or visible devices in their car at work, they are most likely doing the same when they are at off-site facilities.
<b>Data Handling</b>					

Accidental Data Loss due To Auto-Complete in Email	Employees accidentally sharing highly sensitive documents with unauthorized individuals, often due to auto-complete in email	Data Lose Prevention (DLP) solution	Monthly	DLP Owners	Accidental data lose is a huge driver of breaches, to include accidentally sharing information with unauthorized individuals. People type the name of an employee in email, but auto-complete brings up a different person instead. This happens far more often than people realize.
Posting / Sharing of Sensitive Data	Number of employees posting or sharing sensitive organizational information on social networking sites.	Online searches for key terms	Monthly	Security Team (or outsource to a vendor)	There is no way to technically control what employees share on their own personal social media accounts (LinkedIn, etc) so we have to train people to be careful. Do extensive searches on sites such as Facebook and LinkedIn to ensure employees are not posting sensitive organizational information.
Data Wiping or Destruction	Number of employees who are properly following data destruction processes.	Check digital devices that are disposed of for proper wiping. Check dumpsters for sensitive documents.	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. Check any rubbish bins or dumpsters for any sensitive documents that were not shredded.
<b>Additional Behaviors / Impact Metrics</b>					
Facility Physical Security	Number of employees who understand, follow, and enforce policies for restricted or protected access to facilities.	Test how many employees are wearing their badges or stopping those who are not.	Monthly	Information Security or Physical Security	For many organizations, physical security is a major control in reducing risk, especially when dealing with secured facilities. This metric will test and measure people's understanding and enforcement of this control. This ensures that unauthorized individuals are not able to gain access to controlled facilities.
Knowledge	Does workforce know and understand what is expected of them?	Knowledge assessments and online quizzes	Annual or after training	Learning Management or Security Awareness Team	To be able to exhibit a behavior, people need to understand what is expected of them. Do they know the indicators of a phishing attack? Do they know your policies? Do they know how to identify sensitive data?