Resiliency Rates

Key Metrics in Evaluating Your Email Security Risk Profile

KEY TAKEAWAYS

Your Security Awareness and Training (SAT) program is a critical component to your security posture. But, how do you know if your program is effectively reducing your risk profile? The answer is your organization's resiliency rate, a key metric in evaluating your email security risk profile.

- Resiliency rate is the ratio of users that reported an email, without falling susceptible to it, compared to the total number of susceptible users to that email
- Resiliency rate is the "heartbeat" of your phishing defense program and is classified as a "risk score" by Gartner in the most recent SAT Market Guide (2021)

To maximize your resiliency rate, SAT programs must condition employees to identify and report suspicious emails by leveraging a positive, rather than punitive, security focused culture.

WHAT ARE RESILIENCY AND SUSCEPTIBILITY RATES?

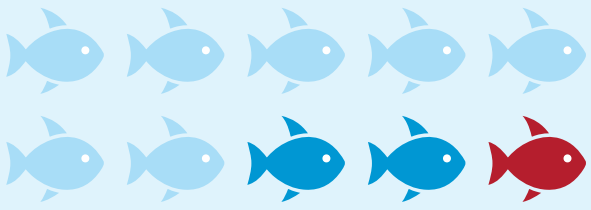
Phishing attacks make up 44% of social engineering incidents and is the most common social engineering breach (Verizon DBIR 2023). Despite an SAT program being part of most organization's security postures, employees still click. The goal of SAT programs is to condition employees to identify and report suspicious emails so that SecOps can analyze and remediate the event before one of potentially thousands of employees click on a malicious link.

Resiliency rate is the "heartbeat" of your phishing defense program and is a key metric in evaluating your email risk profile. Resiliency rate is the ratio of users that reported an email, without falling susceptible to it, compared to the total number of susceptible users to that email. A susceptible user is a user that fell victim to an email, such as clicking on a malicious link. Susceptibility measures how many users fell victim to an email to the total number of users that received that email and is often expressed as a percentage.

$$\text{RESILIENCY} = \frac{\text{RATIO OF USERS THAT REPORTED AN EMAIL WITHOUT FALLING SUSCEPTIBLE}}{\text{TOTAL NUMBER OF SUSCEPTIBLE USERS}}$$

For example, a phishing email with a malicious link is delivered to ten users. Seven users do not engage with the email, two users report the email and do nothing else, and one user clicks on the malicious link. This organization would have a resiliency rate of 2.00 and a susceptibility rate of 10%.

RESILIENCY RATE OF 2.00 AND A SUSCEPTIBILITY RATE OF 10%



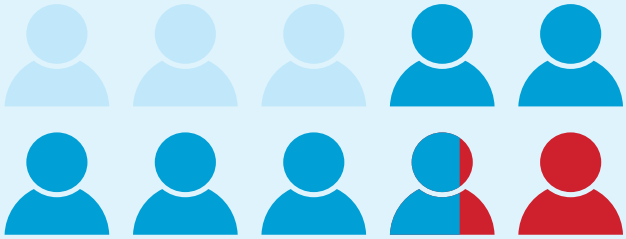
WHY IS RESILIENCY RATE A BETTER MEASUREMENT THAN SUSCEPTIBILITY?

Susceptibility is a common SAT metric, but focusing on susceptibility alone is a defensive approach, centered around program failure. Resiliency is a positive, growth-centered approach. When the number of reports equals the number of clicks (1.00), the attacker's edge is reduced. When the number of reports exceeds the number of clicks (>1.00), the phishing email is more likely to be reported than to have a user fall susceptible.

WHEN
NUMBER OF REPORTS = NUMBER OF CLICKS
THE ATTACKERS EDGE IS REDUCED

WHEN
NUMBER OF REPORTS > NUMBER OF CLICKS
THE PHISHING EMAIL IS MORE LIKELY TO BE REPORTED

AVERAGE RESILIENCY RATE OF COFENSE CUSTOMERS = 5.29



While susceptibility measures how many users are likely to be compromised, resiliency measures how likely you are to detect an attack compared to being compromised. In the past 12-months, Cofense clients averaged a resiliency rate of 5.29, meaning they are more likely to detect and remediate an attack before being compromised.

HOW ORGANIZATIONS CAN MAXIMIZE THEIR RESILIENCY RATE

Maximizing your resiliency rate is an excellent goal for SAT programs and focuses the program on reducing risk through detection. Cofense's customers with the highest resiliency rates follow these program guidelines:

- Organizations with a positive rather than punitive culture see higher report rates, improving resiliency
- Organizations prioritizing relevancy of simulation content rather than breadth improve employee detection, improving resiliency
- Organizations prioritizing timeliness, such as sending simulations when employees are active in their inboxes, see increased reporting, improving resiliency
- Organizations communicating current threats, conduct frequent (recommend monthly) simulations, and follow-up with users who need more conditioning see increased user engagement
- Organizations incorporating rewards and recognition programs for users who report simulations as their only action improve morale and foster teamwork, improving resiliency

Would you like to compare your organization's resiliency rate to other Cofense customers and industry peers? **Request a Board of Directors report from Cofense PhishMe.**

COFENSE

W: cofense.com/contact **T:** 703.652.0717

A: 1602 Village Market Blvd, SE #400
Leesburg, VA 20175