AGARI

Defend Against Social Engineering Attacks

Over 200 enterprises were surveyed to determine:

- The prevalence of social engineering attacks on organizations;
- The toll these attacks are exacting;
- The most effective controls for defending against these targeted strikes.

Of all survey respondents*:

60% say social engineering is one of the most significant threats they face today.

60% know they either were or may have been victims of a social engineering attack during the past year.

65% of those who were attacked say that employees' credentials were compromised as a result of these incidents.

Social Engineering Baseline

94% of security leaders understand the criticality of social engineering, including spear phishing, as a significant business threat.

52% rate their organizations' defenses against social engineering attacks at average or below.

Security leaders understand the criticality of social engineering, including spear phishing, as a business threat.

Attack Volumes & Types

Social engineering attacks are a **critical business issue**.

What is the typical volume of attacks? Is this substantially more than we saw in prior years?

89% of respondents have seen either a steady pace or an increase in social engineering attacks in the past year.
(Consistent with FBI reports)

69%

69% say attackers are after user credentials to commit fraud against the organization.

52%

52% say the fraudsters are looking for the user to take specific actions, **i.e. commit** a fraudulent funds transfer.

27%

27% say the attackers use the compromised credentials to commit fraud or theft against a third party.

Trust & Defenses

49% rate the effectiveness of current controls they deploy to defend against social engineering attacks as average or below.

70% said social engineering is a senior management/board-level concern at their organizations.

8% of responses assess the effectiveness of their current controls as superior.

> *"Once somebody wires a half-million dollars to an offshore account, I promise you that social engineering will very quickly become a board-level concern."*
>
> John Wilson, Agari Field CTO

Partner Vulnerability

Only 7% are "extremely confident" in their business partners' abilities to defend against attacks.

50% say they have no program in place to audit and encourage partners to authenticate email sent to the respondents' organization.

Countermeasure Agenda

Social engineering attacks are enough of a boardroom/senior management issue that **98% expect the same or increased funding in 2017 to combat social engineering attacks**.

How will they invest these resources?

51% expect the budget dedicated to anti-spear phishing to increase in the next year.

Corporate defenses currently are not up to the task of defending against the latest social engineering schemes, and this is a balance that must be shifted to prepare for the challenges of the year ahead.

1. Make it a **management issue**
2. Explore new security solutions to **verify legitimate email senders**
3. Continue **awareness training** with caution
4. Focus on trust and authentication

Get the full report www.agari.com/survey

*Background on Survey Participants

This survey was conducted online in the summer of 2016.
It generated more than 200 responses from organizations across industrial sectors.
Respondent organizations were primarily in:

- Healthcare
- Government
- Financial services
- Education

32% employ 10,000 or more employees.
42% have more than $1 billion in annual revenue.

AGARI
www.agari.com