QUANTIFYING THE VALUE OF SECURITY AWARENESS TRAINING IN EDUCATION

Building on its previous estimates for the risk of a single phishing attack, Aberdeen Group has extended its simple Monte Carlo analysis to quantify the annualized risk of phishing attacks, and to quantify the value of security awareness training for reducing that risk.

In Educational Services, based on the lost productivity of 10,000 users and a data breach of 100,000 to 1,000,000 records:

$400K — **The median annualized business impact of phishing attacks under the status quo (before security awareness training) is about $400,000.**

$16M — **The 80% confidence interval for the annualized business impact from phishing attacks is between $0 and a "long tail" of $16 million.**

34% — **An incremental investment in security awareness training results in a median reduction in the annualized risk of phishing attacks of about 34%.**

1.4x — **Based on this analysis, an incremental investment in security awareness training yields a median annual return on investment of about 1.4 times.**

$5M — **Equally important, an incremental investment in security awareness training in this scenario reduces the "long tail" of the annualized risk of phishing attacks by about $5 million, or more than 1.5 times.**

Read the full report: *Quantifying the Value of Security Awareness Training*, June 2016

The bottom line: Aberdeen's analysis of the annualized risk of phishing attacks provides a good example of the "long tail" of risk that is so common in the context of information security. It serves as a powerful reminder that estimates based on simple averages (e.g., "$201 per record") can be highly misleading, and can easily lead to bad decisions about acceptable levels of risk. As always, the role of the information security professional is to identify and assess risks properly — in terms of likelihood, and business impact — and to communicate effectively about these risks with the business decision-makers they are advising.

ABERDEEN GROUP