SECURITY AWARENESS TRAINING: SMALL INVESTMENT, LARGE REDUCTION IN RISK

July 2017

Author: Derek E. Brink, CISSP
Vice President and Research Fellow, Information Security and IT GRC

Report Highlights

p2

The leading driver for enterprise investments in security awareness and training for their users is to *reduce the cyber security risks* related to user behaviors. This raises an important question: On what basis is the *business decision* to invest in security awareness and training being made?

p7

For the *private sector*, Aberdeen's Monte Carlo analysis estimates the annualized business impact of phishing attacks — based on the lost productivity of *1K users* and a data breach of *100K to 1M records* — to be between $0 and $10M, with a median of about $250K.

p8

For the same scenario, an investment in security awareness training results in a median reduction in the annualized risk of phishing attacks of about 50%, a median annual return on investment of about 5 times, and a reduction in the potentially catastrophic "long tail" of risk by about $6M.

p10

For the same scenario, Aberdeen's Monte Carlo analysis provides the additional insight that a modest investment in security awareness and training for all users (about $28K) has a 72% likelihood of a significant reduction in the business impact of phishing attacks (as high as $6M).

Aberdeen Group's research provides insights that speak strongly in favor of the value of an investment in security awareness and training, to reduce the annualized risk of phishing attacks — insights which can only be discovered and described with a quantitative analysis. A qualitative, red / yellow / green approach to risk analysis simply does not help senior business leaders make better-informed business decisions about risk than mere intuition and gut instinct.

ABERDEEN GROUP

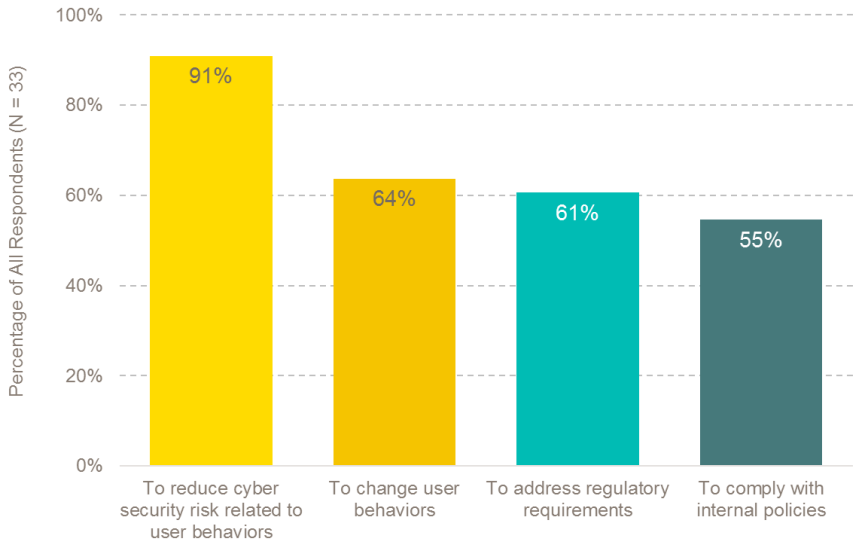
2

The leading driver for enterprise investments in security awareness and training for their users is to *reduce the cyber security risks* related to user behaviors. This raises an important question: On what basis is the *business decision* to invest in security awareness and training being made?

Why Do Organizations Invest in Security Awareness and Training?

It comes as no surprise that the leading driver for enterprise investments in **security awareness and training** for their users is to **reduce the cyber security risks** related to user behaviors (see Figure 1) — for example, opening email attachments or clicking on malicious links in phishing attacks.

Figure 1: Reducing the Cyber Security Risks Related to User Behaviors is the Leading Driver for Enterprise Investments in Security Awareness and Training



Source: CISO workshop (N = 33); Aberdeen Group, August 2016

Based on Aberdeen Group's workshop with more than 30 enterprise security leaders, about 9 out of 10 (91%) organizations are investing in some form of computer-based user training. But about 3 out of 4 (73%) train their users only **at the time of hire**, on an **ad hoc** basis (e.g., after an attack), or on an **annual** basis (e.g., to "check the box" for purposes of compliance). This raises an interesting, and important, question: *On what basis is the business decision to invest in security awareness and training being made?*

3

Two Business Questions About Security Awareness and Training That Security Professionals Must Learn to Answer More Effectively

If the leading driver for investment in security awareness and training is to reduce the cyber security risk, the first business question is pretty clear:

➔ **What's the risk of phishing attacks?**

Two business questions that security professionals must learn how to deal with more effectively: What's the risk of phishing attacks? How will an investment in security awareness and training for our users reduce that risk?

The answer to this question is *not* to provide senior business leaders with the technical details of what phishing attacks are; how and why they work; who they target and why; who is behind them, from where; publicly disclosed examples of organizations that have been affected; and detailed statistics and technical information about the latest trends. This kind of information is clearly appropriate for the security professional to understand, in their role as **subject-matter expert**.

But in their dual role as **trusted advisor** to the senior business leaders (who actually own the risk), the security professional's answer to this business question about phishing attacks must be expressed in terms of the proper definition of risk: **How likely are phishing attacks, and how much business impact do they have?**

The second business question that needs to be addressed is equally straightforward:

➔ **How will an investment in security awareness and training for our users reduce the risk of phishing attacks?**

By default, most risk-based business decisions are made based on the *intuition*, *judgment*, and *gut instinct* of the senior business leader. Worse, senior business leaders may abdicate this responsibility to the technical and operational staff, who do their

best to interpret "best practice" and management's appetite for risk to make a business decision that isn't actually theirs to make.

As security professionals, our primary objective is to **help senior business leaders make better-informed business decisions** about security-related risks. To do this, we need to move the decision-making dial away from mere intuition, judgment, and gut feel.

There are many popular approaches to measuring and communicating about cyber security risks, which most security professionals are familiar with … but with respect to making better-informed business decisions about risk, none of these really "move the dial" in a positive direction.

Let's at least be honest about it: a healthy dose of Fear, Uncertainty, and Doubt (FUD) from the latest headlines; a qualitative assessment of "yellow;" and a request for an incremental $30K per year in budget for security awareness and training does not really achieve this goal. Yet many security professionals say they like these **qualitative** and **pseudo-quantitative** risk assessments, because:

- The senior business leaders seem to "get it"
- These kinds of assessments often lead to "better conversations" about risk, and better prioritization
- **Quantitative** risk assessments are (mistakenly) viewed as too difficult, or (ironically) as too imprecise

To more effectively address the primary reason we exist, security professionals simply must learn how to do better than this.

Monte Carlo models are aligned with the proper definition of risk, and are well-suited to deal with the inherent uncertainties in quantitative estimates for likelihood and business impact in the context of cyber security. Proven and widely used for several

➔ Related Research:
7 Ways to Talk About Risk That Don't Help Make Better Business Decisions

Qualitative assessments represent selected factors of likelihood and business impact in terms of *high / medium / low* or *red / yellow / green* — which are sometimes transformed into **pseudo-quantitative** assessments by assigning numeric ranges, such as *1 to 5* or *1 to 100*.

These methods are widely perceived as being easy for senior business leaders to understand, but their value is dubious at best: doing math on these values is meaningless, and leaders are still asked to make important business decisions about risk based on an assessment of "yellow" or "72."

5

In a **Monte Carlo** analysis, each variable in a calculation is expressed as a *range* (lower bound, upper bound) and a *shape* (probability distribution) — as opposed to as a single, static value.

The relevant calculations are then carried out based on a randomly selected value from the probability distribution for each variable, over many (say, 10,000) independent iterations.

In doing so, the result is also expressed as a range and distribution — as opposed to a single, static value such as "the average cost of a data breach is $201 per record" or "the average scrap learning rate is 45%."

Most importantly, the result can then be represented in terms of both *how likely* and *how much business impact* — i.e., in terms of *risk*, as risk is properly defined.

decades across a diverse range of industries and applications, Aberdeen has been successfully using Monte Carlo analysis to gain insights into security-related risks for the last four years.

To illustrate, let's **quantify the risk of phishing attacks,** and **the value of an investment in security awareness training for reducing that risk**.

Quantifying the Risk of Phishing Attacks

A quantitative risk analysis starts by *factoring* (e.g., see The Open Group Standard for Risk Taxonomy) the key elements of likelihood and business impact. Aberdeen's simple model for factoring the annualized risk of phishing attacks is outlined in Table 1.

Table 1: Factoring the Annualized Risk of Phishing Attacks

Factors Related to the Likelihood of Phishing Attacks	Factors Related to the Business Impact of Phishing Attacks
▪ Likelihood of experiencing *at least one* phishing attack in the next 12 months	
▪ If attacked, number of phishing attacks experienced per year	
▪ Likelihood that a phishing attack will be successful (i.e., user "*click rates*")	▪ Damage to reputation / brand (i.e., from public disclosures of successful attacks)
▪ Percentage of user actions that result in a need for response, remediation, and recovery (e.g., *endpoint infections*, *account compromises*)	▪ Lost productivity of users during the time of response, remediation, and recovery (i.e., how long to respond; cost of user time; percentage of user productivity truly lost)
▪ Percentage of user actions that result in a successful *data breach*	▪ Cost of a data breach

Source: Aberdeen Group, July 2017

6

The factors in Aberdeen Group's quantitative risk analysis are influenced and informed by empirical, publicly available insights about phishing attacks, such as those published annually in the Wombat Security *State of the Phish* report and the Verizon *Data Breach Investigations Report*, along with analyst estimates based on Aberdeen research.

These factors are influenced and informed by empirical, publicly available insights about phishing attacks, such as those published annually in the Wombat Security *State of the Phish* (SOTP) report and the Verizon Data Breach Investigations Report (DBIR), along with analyst estimates based on Aberdeen Group research.

The next step is to use the best available data to establish a *range* (i.e., a lower bound, and an upper bound) and a *shape* (i.e., a probability distribution, within that range) for each of the factors. For example, the 2016 SOTP report found that about 85% of all organizations experienced at least one phishing attack over a 12-month period — for which Aberdeen model the likelihood as a range of 0% to 100%, with a probability distribution whose "fat" part is around 85%. This quantitative approach to risk assessment reflects the inherent **uncertainties** in the factors of likelihood and business impact for cyber security risks: computations based on precise values, if they were possible, would result not in *risks* but in *facts*. Remember, the goal is not to be precise — the goal is to help senior business leaders make a better-informed business decision than mere intuition and gut feel.

At this point, quantifying the annualized risk of phishing attacks can achieved using standard Microsoft Excel, based on carrying out the relevant calculations using a randomly selected value from the probability distribution for each variable over 10,000 independent iterations. The result is also expressed as a range and distribution, can then be represented in terms of both how likely and how much business impact — exactly what we are looking for.

The Annualized Risk of Phishing Attacks in the Private Sector

For the **private sector** as a whole (i.e., across all industries for which empirical data on click rates and data breaches is available), Aberdeen's Monte Carlo model estimates the annualized risk of

7

For the private sector, the annualized business impact of phishing attacks before security awareness and training — based on the lost productivity of 1K users and a data breach of 100K to 1M records — is estimated to be between $0 and $10M, with a median of about $250K.

phishing attacks as follows, based on the lost productivity of **1,000 users** and a data breach of **100K to 1M records**:

- ➔ The **median** annual business impact of phishing attacks under the status quo is **about $250K**
- ➔ On an annualized basis, there's a **90% likelihood** that phishing attacks in this scenario will cost **more than $0**, and a **10% likelihood** that phishing attacks will cost **more than $10M** (i.e., this is the *80% confidence interval*)

Take special note of the difference between the lower end of the range and the median (*$0 to $250K*), as compared to the much larger difference between the median and the upper end of the range (*$250K to $10M*). The inherent asymmetry (*skew*) of this risk distribution is a perfect illustration of the **"long tail"** of risk that is so common in the context of cyber security: Most of the time the business impact may be below some acceptable threshold, but there is also be a material likelihood that the business impact is unacceptably high.

Framing risks properly in this way — including insights into the often-catastrophic long tail — is critical to helping the owners of the risk make better-informed business decisions.

The Value of an Investment in Security Awareness and Training

The first step in quantifying how an investment in security awareness and training for an organization's users reduces its annualized risk from phishing attacks is to estimate ranges and distributions for just three additional factors:

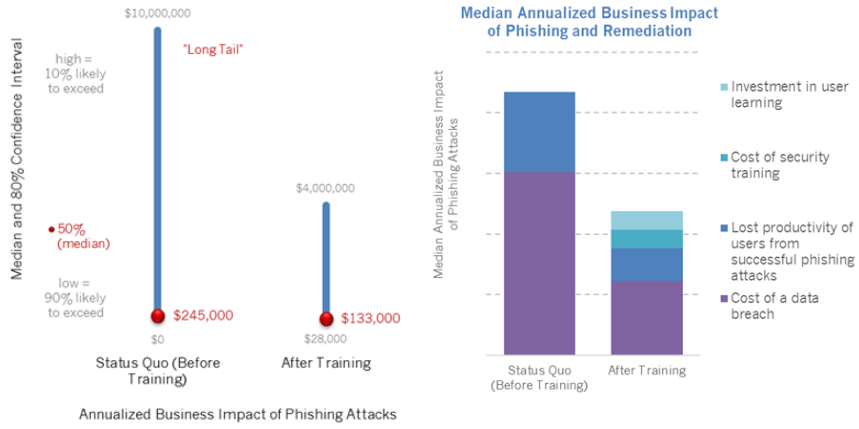
- ➔ The *reduction in user click rates*, as a result of the investment in security awareness and training for all users

For the same scenario, an investment in security awareness training results in a median reduction in the annualized risk of phishing attacks of about 50%, and a median annual return on investment of about 5 times. Equally important, it reduces the potentially catastrophic "long tail" of the annualized risk of phishing attacks in this scenario by about $6M, or approximately 2.5 times.

- The *cost of security training* itself (e.g., the annualized cost per user, for training solutions from third-party specialists)
- The *investment in user learning* (i.e., the value of the time for all users to complete the security awareness training annually, along with that of a second round of remedial security awareness training for those users who fall for a simulated phishing attack after the initial round of training)

For the same scenario (public sector, 1K users, 100K to 1M records), the **median** annual business impact of phishing attacks is reduced to **about $130K**, with an **80% confidence interval** of **between $28K** (the cost of training for all users) and **$4M** (the long tail). See Figure 2.

Figure 2: The Value of an Investment Security Awareness and Training, for Reducing the Annualized Risk of Phishing Attacks



Source: Monte Carlo analysis, based on the productivity losses of 1K employees and a data breach of 100K to 1M records in the private sector; data adapted from Wombat 2016 SOTP and Verizon 2016 DBIR; Aberdeen Group, July 2017

Based on this analysis, an incremental investment in security awareness training results in a **median reduction in the annualized risk of phishing attacks of about 50%**, and a **median annual return on investment of about 5 times**.

Equally important, an incremental investment in security awareness training reduces the potentially catastrophic "long tail" of the annualized risk of phishing attacks in this scenario by **about $6M, or approximately 2.5 times**.

A Third Business Question About the Value of Security Awareness and Training — Which Security Professionals Can Now Deal With

A third business question that security professionals can now address: How likely is it that we will really be better off by making an investment in security awareness and training for our users — as opposed to by doing nothing at all?

Perceptive readers may have noticed that in the "before" scenario of Aberdeen's analysis the lower end of the range is $0 (i.e., there's a chance that we'll get lucky, and have zero impact from phishing attacks over the next 12 months), while in the "after" scenario the lower end of the range is about $28K (i.e., we're making a commitment to invest in security awareness training for all users). Senior business leaders are prone to notice this detail as well. This raises a third business question: **How likely is it that we will really be better off by making an investment in security awareness and training for our users — as opposed to by doing nothing at all?**

For many security professionals, these have traditionally been among the "deer-in-the-headlight" moments in making recommendations to senior business leaders, on which our resource allocation requests are made or broken.

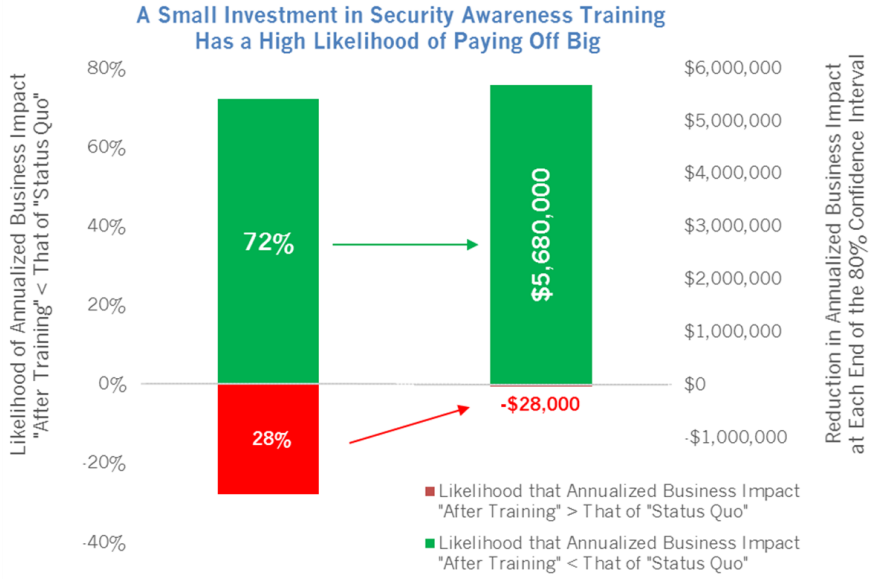
Technical details, FUD-inducing headlines, averages, infographics, falsely precise calculations, and qualitative and pseudo-quantitative assessments are not going to provide senior business leaders with any useful insights into this legitimate question. Fortunately, our quantitative analysis has *already produced* the insight we are looking for, which will help to address this legitimate business question with relative ease:

For the same scenario, the likelihood that an investment in security awareness and training for all users will cost less than the annualized business impact of phishing attacks is about 72%. That's a 28% likelihood of investing about $28K "for nothing," and a 72% likelihood of a payoff as high as $6M.

- ➔ The likelihood that an incremental investment in security awareness and training for all users will cost less than the annualized business impact of phishing attacks is **about 72%**
- ➔ However, the investment of about $28K is extremely small, especially in comparison to the large payoff (about $6M) of cutting off the long tail of the risk of phishing (see Figure 3)

This is an insight that speaks strongly in favor of the value of an investment in security awareness training — one which can only be discovered and described with a *quantitative* analysis. A qualitative, *red / yellow / green* approach to risk analysis simply does not help senior business leaders make better-informed business decisions about risk than mere intuition and gut feel.

Figure 3: Small Investment in Security Awareness and Training for Users, Large Reduction in the Annualized Risk of Phishing



Source: Aberdeen Group, July 2017

What action the senior business leaders in any given organization will take as a result of this analysis is by no means certain. That is, they may decide to *accept* the risk; *ignore* the risk (which is an inferior form of acceptance); *transfer* the risk to another party; or take steps to *manage* the risk to an acceptable level. The role of the security professional is to *advise* and *recommend*; it falls to the senior business leader to *decide*, based on the organization's appetite for risk.

Summary and Key Takeaways

- The leading driver for enterprise investments in **security awareness and training** for their users is to **reduce the cyber security risks** related to user behaviors. This raises an interesting, and important, question: On what basis is the business decision to invest in security awareness and training being made?
- The primary objective of security professionals is to **help senior business leaders make better-informed business decisions** about security-related risks. To do this, we need to move the decision-making dial away from mere intuition, judgment, and gut feel.
- In this context, there are two business questions that security professionals must learn how to deal with more effectively: **What's the risk of phishing attacks? How will an investment in security awareness and training for our users reduce that risk?**
- **Qualitative** and **pseudo-quantitative** assessments are widely perceived as being easy for senior business leaders to understand, but their value is dubious at best: doing

math on these values is meaningless, and leaders are still asked to make important business decisions about risk based on an assessment of "yellow" or "72."

- **Monte Carlo** models are aligned with the proper definition of risk, and which are well-suited to deal with the inherent uncertainties in **quantitative** estimates for likelihood and business impact in the context of cyber security.

- The factors in Aberdeen Group's quantitative risk analysis are influenced and informed by empirical, publicly available insights about phishing attacks, such as those published annually in the Wombat Security *State of the Phish* report and the Verizon *Data Breach Investigations Report*, along with analyst estimates based on Aberdeen research.

- For the *private sector*, Aberdeen's Monte Carlo analysis estimates the annualized business impact of phishing attacks before security awareness and training — based on the lost productivity of *1K users* and a data breach of *100K to 1M records* — to be **between $0 and $10M**, with a **median of about $250K**.

- The difference between the lower end of the range and the median (*$0 to $250K*), as compared to the much larger difference between the median and the upper end of the range (*$250K to $10M*) is a perfect illustration of the **"long tail"** of risk that is so common in the context of cyber security. Framing risks properly in this way is critical to helping the owners of the risk make better-informed business decisions.

- For the same scenario, Aberdeen's Monte Carlo analysis estimates that an investment in security awareness training results in a **median reduction in the annualized**

risk of phishing attacks of about 50%, and a **median annual return on investment of about 5 times**. Equally important, it reduces the potentially catastrophic "long tail" of the annualized risk of phishing attacks in this scenario by **about $6M**, or **approximately 2.5 times**.

- A third business question that security professionals can now address: **How likely is it that we will really be better off by making an investment in security awareness and training for our users — as opposed to by doing nothing at all?**

- For the same scenario, Aberdeen's Monte Carlo analysis estimates that the likelihood that an investment in security awareness and training for all users will cost less than the annualized business impact of phishing attacks is **about 72%**. That's a 28% likelihood of investing about $28K "for nothing," and a 72% likelihood of a payoff as high as $6M.

- **This is an insight that speaks strongly in favor of the value of an investment in security awareness training** — one which can only be discovered and described with a *quantitative* analysis. A qualitative, *red / yellow / green* analysis simply does not help senior business leaders make better-informed business decisions.

- Even so, the action that the senior business leaders in any given organization will take as a result of this analysis is by no means certain. They may decide to *accept* the risk; *ignore* the risk (which is an inferior form of acceptance); *transfer* the risk to another party; or take steps to *manage* the risk to an acceptable level. The role of the security professional is to *advise* and *recommend*; it falls to the

senior business leader to *decide*, based on the organization's appetite for risk.

For more information on this or other research topics, please visit www.aberdeen.com.

Related Research

Smaller Businesses Have Bigger Risk: Quantifying the Risk of a Data Breach; July 2017
7 Ways to Talk About Risk That Don't Help Make Better Business Decisions; July 2017
Use It, Or Lose It: Quantifying the Risk of "Scrap Learning"; May 2017
Cutting Off the Long Tail of Risk from Phishing Attacks; August 2016
Quantifying the Value of Security Awareness Training; May 2016

Author: Derek E. Brink, CISSP, Vice President and Research Fellow, Information Security and IT GRC

About Aberdeen Group

Since 1988, Aberdeen Group has published research that helps businesses worldwide to improve their performance. Our analysts derive fact-based, vendor-neutral insights from a proprietary analytical framework, which identifies Best-in-Class organizations from primary research conducted with industry practitioners. The resulting research content is used by hundreds of thousands of business professionals to drive smarter decision-making and improve business strategies. Aberdeen Group is headquartered in Waltham, Massachusetts, USA.

This document is the result of primary research performed by Aberdeen Group and represents the best analysis available at the time of publication. Unless otherwise noted, the entire contents of this publication are copyrighted by Aberdeen Group and may not be reproduced, distributed, archived, or transmitted in any form or by any means without prior written consent by Aberdeen Group.