KB

ENTERPRISE EMAIL: ARE YOU ADEQUATELY ADDRESSING YOUR RISKS?

August 2017

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

ABERDEEN

Enterprise email is indispensable to your business — and is also the leading delivery mechanism for malware and social engineering. Aberdeen's analysis estimates that an investment in advanced email security reduces the median risk of phishing attacks by about 85%, for a median annual return on investment of nearly 12 times.

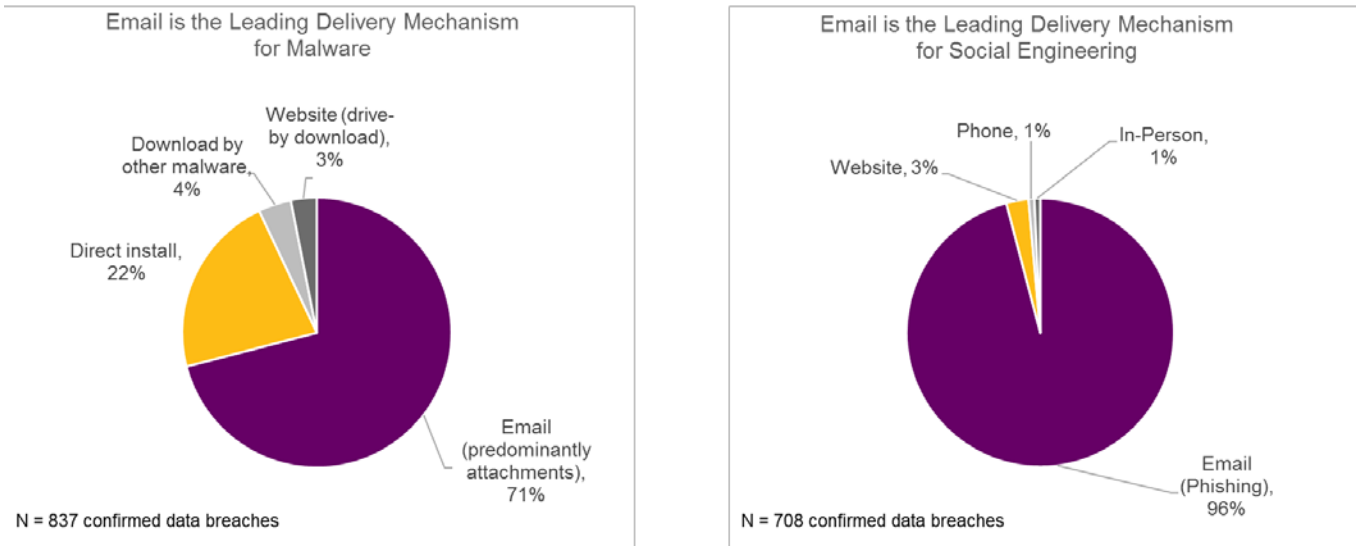
Enterprise Email is Indispensable to Your Business

In our contemporary world of *posts*, *tweets*, *snaps*, and *grams*, good old-fashioned **enterprise email** continues to be the ubiquitous workhorse of corporate communications.

As organizations transition from a traditional, *PC-oriented* endpoint strategy to a *mobile-first approach*, email is the number one category of enterprise software that organizations have mobilized for employee use, and the number one corporate resource to which employees are granted access from employee-owned mobile devices.

Because of its ubiquity — as well as its fundamental reliance on the actions of human users — email is also the leading **delivery mechanism for malware** (71%) and **social engineering** (96%). See Figure 1.

Figure 1: Email is the Leading Delivery Mechanism for Attackers



Source: Adapted from Verizon 2017 DBIR; Aberdeen Group, August 2017

These conditions lead to a growing list of undesirable outcomes from attacks on enterprise email, including infected endpoint systems, lost productivity for users (and responders), data breaches, and ransomware.

Quantifying the Risk of Phishing Attacks, and the Value of Advanced Email Security

Based on empirical, publicly available insights about phishing attacks and data breaches — such as those published in the Wombat Security 2016 *State of the Phish* (SOTP) report and the Verizon 2017 DBIR, along with analyst estimates based on Aberdeen Group's ongoing research — Aberdeen has developed a Monte Carlo model to estimate **the annualized risk of phishing attacks**, and **the value of advanced email security** for reducing that risk.

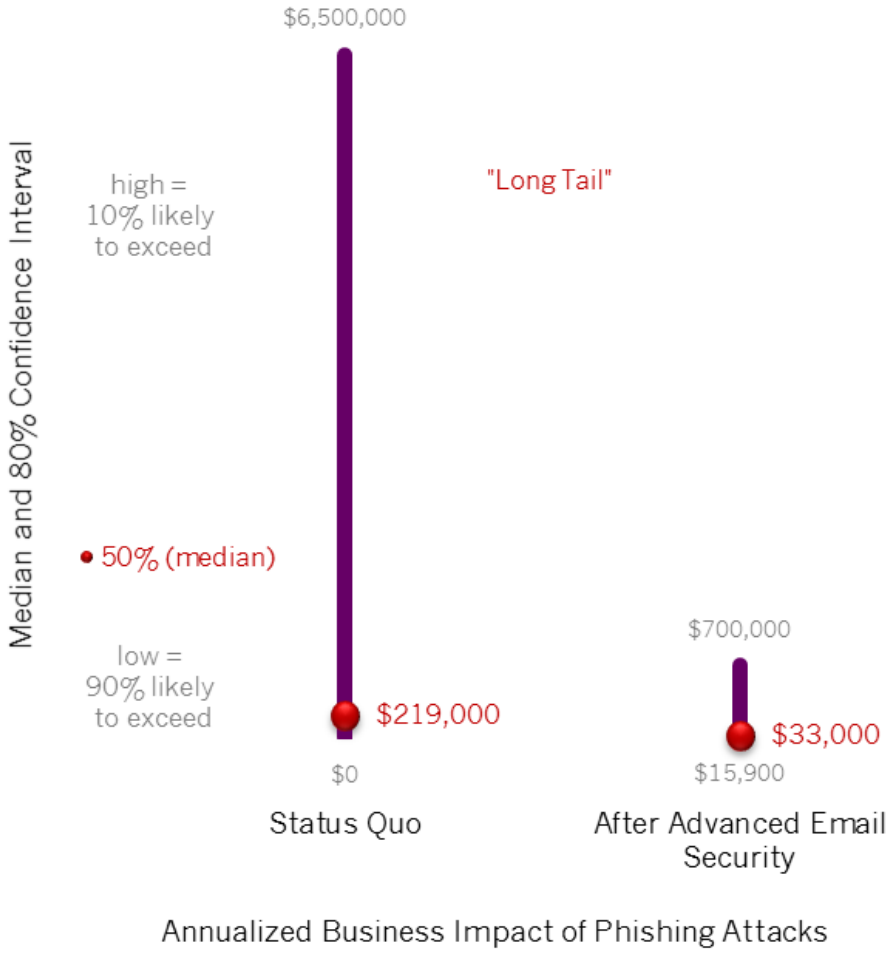
Based on this analysis, the following insights can help senior leaders to make a better-informed business decision about phishing risks:

- For the *private sector* as a whole, the annualized business impact of phishing attacks — based on the lost productivity of *1K users* and a data breach of *100K to 1M records* — is estimated to be **between $0 and $6.5M**, with a **median of about $220K**.
- For the same scenario (private sector, 1K users, 100K to 1M records), an investment in advanced email security reduces the annualized risk of phishing attacks to **between $15.9K and $700K**, with a **median of about $33K** — a median reduction in risk of **about 85%**, for a median annual return on investment of **about 11.7-times**. See Figure 2.
- An investment in advanced email security reduces the potentially catastrophic "long tail" of the annualized risk of phishing attacks in this scenario by **about $5.8M**, or **approximately 9.3 times**.
- The likelihood that an investment in advanced email security for all users will "pay off" is **about 85%**. Said another way, the likelihood that investing $15.9K in advanced email security will cost more than the "do nothing" option is about 15%.
- The modest investment in advanced email security (about $15.9K) is extremely small in comparison to the potentially large payoff (about $5.8M) of cutting off the **long tail** of the risk of phishing attacks.

The quantitative risk analysis described in this research report is one of literally hundreds of scenarios that Aberdeen's Monte Carlo model can accommodate, based on the selection of *industry sector*, *number of users*, and *number of records*.

Read the full report: *Enterprise Email: Are You Adequately Addressing Your Risks?*

Figure 2: Quantifying the Value of Advanced Email Security for Reducing the 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; Data adapted from Wombat Security 2016 SOTP and Verizon 2017 DBIR; Anti-phishing efficacy adapted from AV-Comparatives 2017; Email security MSRP based on analyst estimates; Aberdeen Group, August 2017

As always, what action the senior business leaders in any given organization will take as a result of this analysis is by no means certain: *accept* the risk, *transfer* the risk to a third 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 leaders to *decide*, based on the organization's appetite for risk.

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.