A CASE FOR EXPANDING STRONGER USER AUTHENTICATION: EXECUTIVE SUMMARY

July 2016

Traditional economic ceilings for the broader deployment of stronger user authentication are rapidly rising. Aberdeen Group's analysis provides new, quantitative insights into making a business case for deploying stronger user authentication to an expanded user base.

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

➔ Related Research: "IAM Beyond Control, Compliance, and Cost: The Rise of the User"

➔ Related Research: "IAM for Everyone: How a Broader Strategic Focus on Users Pays Off"

Summary and Key Takeaways

➔ As Aberdeen Group described in its research report, *IAM Beyond Control, Compliance, and Cost: The Rise of the User* (September 2015), enterprise **identity and access management (IAM)** systems are increasingly being seen not only as the technical means for *control*, *compliance*, and *cost efficiencies* focused on protecting the organization's **applications and data** , but also as an essential *enabler* for the organization's **users**, who are the tactical means for achieving its strategic business objectives.

➔ A follow-on Aberdeen research report on identity and access management, *IAM for Everyone: How a Broader Strategic Focus on Users Pays Off* (November 2015), confirmed that enterprise IAM systems are now being looked to for help with both *unrewarded* (e.g., protection) and *rewarded* (e.g., enablement) types of business risks. Among the respondents in Aberdeen's study, both types of risk are strongly evident among the **leading drivers for current investments in IAM**.

- For the modern enterprise, the rewarded risks of **enablement**, the unrewarded risks of **protection**, and the obligation of **regulatory compliance** make stronger authentication of an expanded user base a growing necessity.

- As the foundation for a quantitative business case for expanding the deployment of stronger user authentication, Aberdeen has developed a simple **Monte Carlo model** for the annualized risk of data breaches related to the exploitation of weak, stolen, or compromised user credentials, based on estimates for just five variables:

    - **The likelihood of experiencing a security incident** (i.e., an attempt to compromise the confidentiality, integrity or availability of an information asset)

    - **The likelihood of experiencing a data breach** (that is, a security incident that results in the confirmed disclosure of an information asset to an unauthorized party)

    - If successfully breached at least once, **the number of data breaches experienced per year**

    - **The percentage of data breaches involving weak, stolen, or compromised credentials**

    - **The business impact of a data breach**

- This simple model, as is, makes a *conservative*, *understated* estimate of the total risk of the status quo. Why? Because it addresses only the unrewarded risks of weaker authentication — i.e., it does not address *the business impact of non-compliance* with regulatory requirements related to third-party risks, or *the business*

Monte Carlo Models and Risk

In a **Monte Carlo** model, each variable in a calculation is expressed as a *range* (lower bound, upper bound) and a *shape* (probability distribution), rather than a single, static value.

The 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). The result can then be represented in terms of *how likely*, and how much — i.e., in terms of **risk**, as risk is properly defined.

This provides security professionals with exactly what they need to quantify estimates for fundamental business questions such as:

- **The risk of data breaches** as a result of weak, stolen, or compromised user credentials
- **The value of an investment** in stronger authentication for reducing that risk
- **A comparison of an investment** in one form of stronger authentication with an investment in another

Defining "Factors" in Stronger User Authentication

An everyday example of "two-factor" authentication is the *ATM card*, where the first factor that authenticates a given transaction is the possession of a validly issued debit or credit card (*something you have*), and the second factor is the user's PIN (*something you know*). The combination of these two factors provides higher assurance of a valid, authorized user than either factor alone. In general, factors for user authentication include:

- **Something you know** (such as a username or PIN)
- **Something you have** (such as a card, token, or other device)
- **Something you are** (such as a fingerprint biometric)
- **Something you do** (such as typical patterns of user behavior, or the unique dynamics of user typing on a keyboard)

One-time passwords are classic examples of two-factor authentication, because they typically combine *something you know* (a PIN) with *something you have* (a hardware token, a software token, or a pre-registered mobile device to receive a tokencode via SMS). The combination of PIN plus tokencode creates a unique password that is valid for a single use.

impact of failing to capture the rewarded risks of user enablement.

➔ In the **private sector** (across all industries), based on a compromise of *100,000 to 1,000,000 records*, the *median* annualized business impact of data breaches as a consequence of weak authentication is **about $370K**, with an *80% confidence interval* of between **$0** and **$1.9M**.

➔ Estimating the value of an investment in **stronger user authentication**, based on reducing the annualized risk of data breaches, calls for extending Aberdeen's simple Monte Carlo model with just three additional variables:

- **The number of users** to which stronger user authentication will be deployed
- **The percentage of data breaches involving stronger user authentication**
- **The annual cost per user for stronger user authentication**

➔ In the **private sector** (across all industries), based on a compromise of *100,000 to 1,000,000 records*, Aberdeen's analysis shows that an investment in stronger user authentication — in this case, **one-time passwords (OTP)** — results in a *median* reduction in the risk of data breaches of **about 90%**, as well as in cutting off the "long tail" of risk by **more than 50%**.

➔ As simple and conservative as it is, Aberdeen's quantitative analysis demonstrates how the **traditional economic ceilings for the deployment of stronger user authentication are rapidly changing**. For example, lower-cost solutions for stronger user authentication — such as *OTP based on SMS* — can provide organizations

with an economically justifiable business case for significantly expanding their user base.

- As always, the selection of user authentication still involves making trade-offs between several characteristics, in three high-level areas:
  - **Total cost of ownership**, including *cost to acquire*; *cost to deploy*; and *cost to manage*
  - **Fit for users**, including *convenience*; *ease of use*; and *acceptance*
  - **Fit for the organization**, including *acceptable level of risk*; *effectiveness of the solution in reducing risk*; *integration with high-value applications and data*; and *integration with existing IT infrastructure*
- Aberdeen's Monte Carlo models have been implemented using standard functionality of Microsoft Excel, and include simple drop-down menus to enable personalization by **industry**, **number of employees**, and **number of records**. A snapshot of Aberdeen's analysis for each of 17 industries is also available in a series of industry-specific *Knowledge Briefs* and *SmartBites*.

→ Read the full report: "Stronger User Authentication: A Case for Expanding Your Base"