RR

# REDUCING THE RISK OF PHISHING ATTACKS: IT'S ABOUT TIME

November 2017

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

ABERDEEN

Phishing attackers hook virtually 100% of their victims within the first 24 hours — by which time they have already shut down nearly 50% of their phishing URLs and moved on. With so much at stake, based on the first few minutes of time, successfully protecting your organization's email and websites against phishing attacks requires a high-speed, purpose-built approach.

## The Risk of Phishing Attacks: How Likely; How Much Impact?

*"What's our organization's risk from phishing attacks?"*

As Aberdeen described in its research report, *Security Awareness Training: Small Investment, Large Reduction in Risk* (July 2017), senior business leaders rely on their organization's security professionals to answer this question in a way that helps them to **make a better-informed business decision about risk**.

The answer 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, and from where; publicly disclosed examples of organizations that have been affected; and detailed statistics about the latest technologies and trends. This kind of information is clearly appropriate for security professionals to understand, in their traditional role as **subject-matter experts**. But it does not describe *risk*.

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

Many security professionals perceive **qualitative** and **pseudo-quantitative** risk assessments as being easiest for senior business leaders to understand, but their value for making better-informed business decisions about risk is dubious at best: doing math on these values is meaningless, and leaders are left to make important business decisions based on an assessment of "yellow" or "72." By default, most

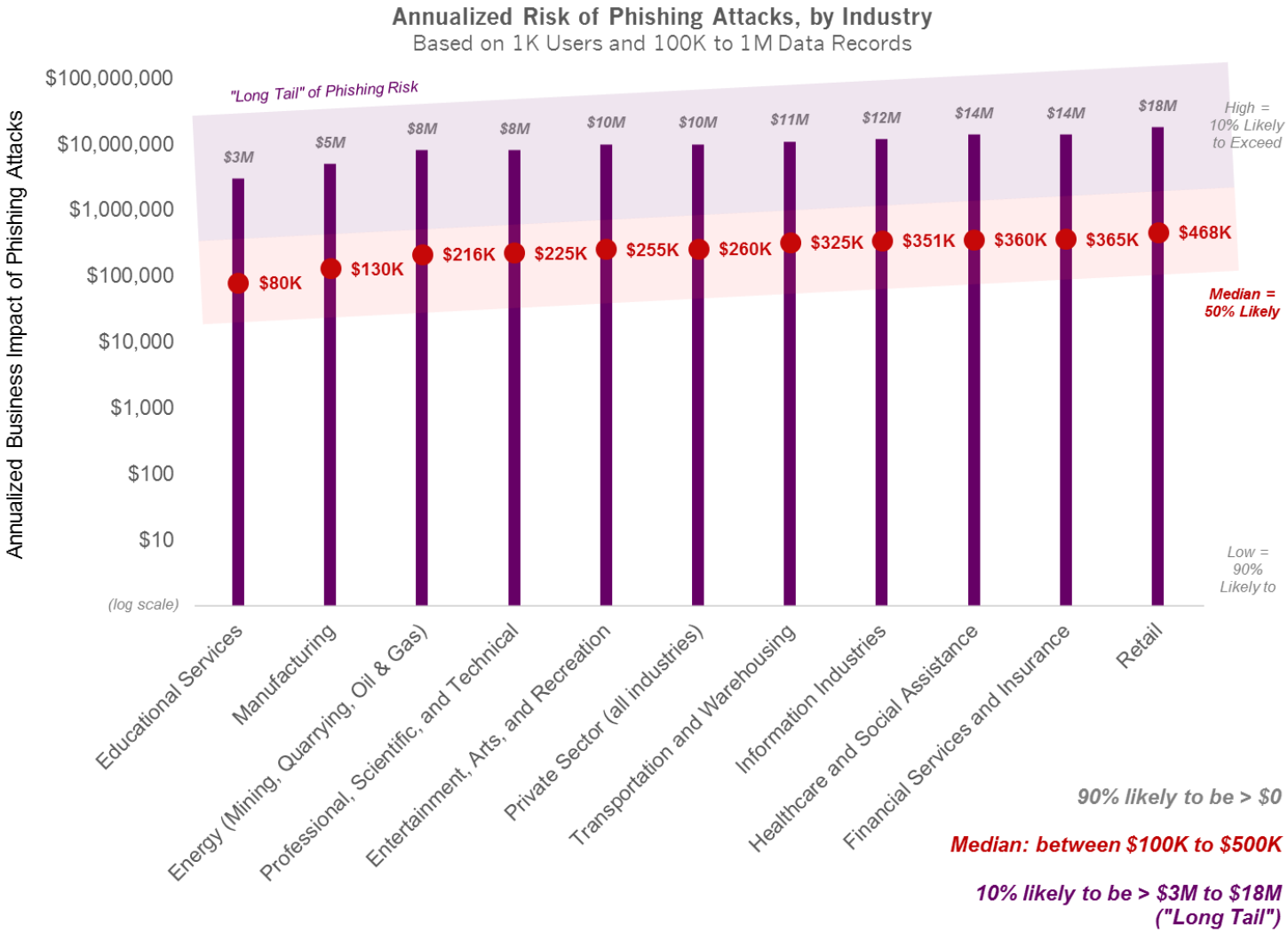
Aberdeen Group's quantitative analysis of the annualized likelihood and business impact of **phishing attacks** — based here on the lost productivity of *1,000 users* and a confirmed data breach of *100K to 1M records*, for 10 different industry sectors — helps senior business leaders to better appreciate the significant **risk** that phishing attacks represent:

- **90% likely to be more than $0** (i.e., across all industries, organizations will almost certainly incur *some* business impact because of phishing attacks)
- A **median** annualized business impact of **between $100K and $500K**
- **10% likely to be more than $3M to $18M** (i.e., there's a material likelihood of a potentially catastrophic business impact; this is the *"long tail"* of phishing risk)

**Qualitative** risk 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*, to these values.

risk-based business decisions about security are made based solely on the *intuition*, *judgment*, and *gut instinct* of the senior business leaders.

Figure 1: The Annualized Risk of Phishing Attacks is Significant, Particularly When Senior Business Leaders are Provided with a Proper Understanding of the "Long Tail" of Phishing Risk




Source: Monte Carlo analysis, based on the productivity losses of 1K users and a data breach of 100K to 1M records; data adapted from Wombat Security 2016 *State of the Phish Report* and Verizon 2015 – 2016 *DBIR*; Aberdeen Group, October 2017

In sharp contrast, a **quantitative** risk assessment reflects the inherent **uncertainties** in the factors of likelihood and business impact by using the best available data to estimate 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 — and then by carrying out the relevant

Computations based on precise values, if they were even 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 better-informed business decisions about risk** than mere intuition and gut feel.

calculations based on a randomly selected value from the probability distribution for each variable, over many (say 10,000) independent iterations. The factors in Aberdeen's quantitative risk analysis are informed and influenced by empirical, publicly available insights about phishing attacks and data breaches, such as those published annually in the Wombat Security *State of the Phish* report and the Verizon *Data Breach Investigations Report* (DBIR), along with analyst estimates based on findings from Aberdeen Group's ongoing *research*.

A summary of the annualized risk of phishing attacks for several specific industry sectors — based on the availability of industry-specific empirical data on *click rates*, and conversion of security *incidents* to confirmed *data breaches* — is presented in Figure 1. For example, for the **private sector** as a whole (i.e., across all industries), Aberdeen's Monte Carlo analysis estimates the annualized risk of phishing attacks as follows:

- The **median** annual business impact of phishing attacks under the status quo is **about $260K**, based on the lost productivity of *1,000 users* and a data breach of *100K to 1M records*.
- 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 range represents the *risk distribution* for phishing attacks).

Take special note of the inherent asymmetry (*skew*) of this risk distribution — i.e., the modest difference between the lower end of the range and the median (*$0 to $260K*), as compared to the much larger difference between the median and the upper end of the range (*$260K to $10M*). This a perfect illustration of the **"long tail"** of risk that is so common in the context of cyber security, and so important for security professionals to help senior business leaders understand: *Half of the time the business impact may be below some acceptable threshold, but there is also a material likelihood that the business impact is unacceptably high*.

## Reducing the Risk of Phishing Attacks: It's About Time

*"How will an investment in a recommended countermeasure or control quantifiably reduce our organization's risk from phishing attacks?"*

The second business question that senior business leaders rely on their organization's security professionals to address is equally straightforward. Once they've determined that the risk of phishing attacks under the status quo is unacceptably high, they need **a recommendation for what to do**

**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 $10M, with a median of about $260K.**

Aberdeen's simple model for factoring the annualized risk of phishing attacks focuses on the two biggest sources of business impact:

- **Lost productivity of users** during the time of response, remediation, and recovery resulting from phishing attacks (e.g., from endpoint infections, account compromises)
- Total cost of successful **data breaches** resulting from phishing attacks

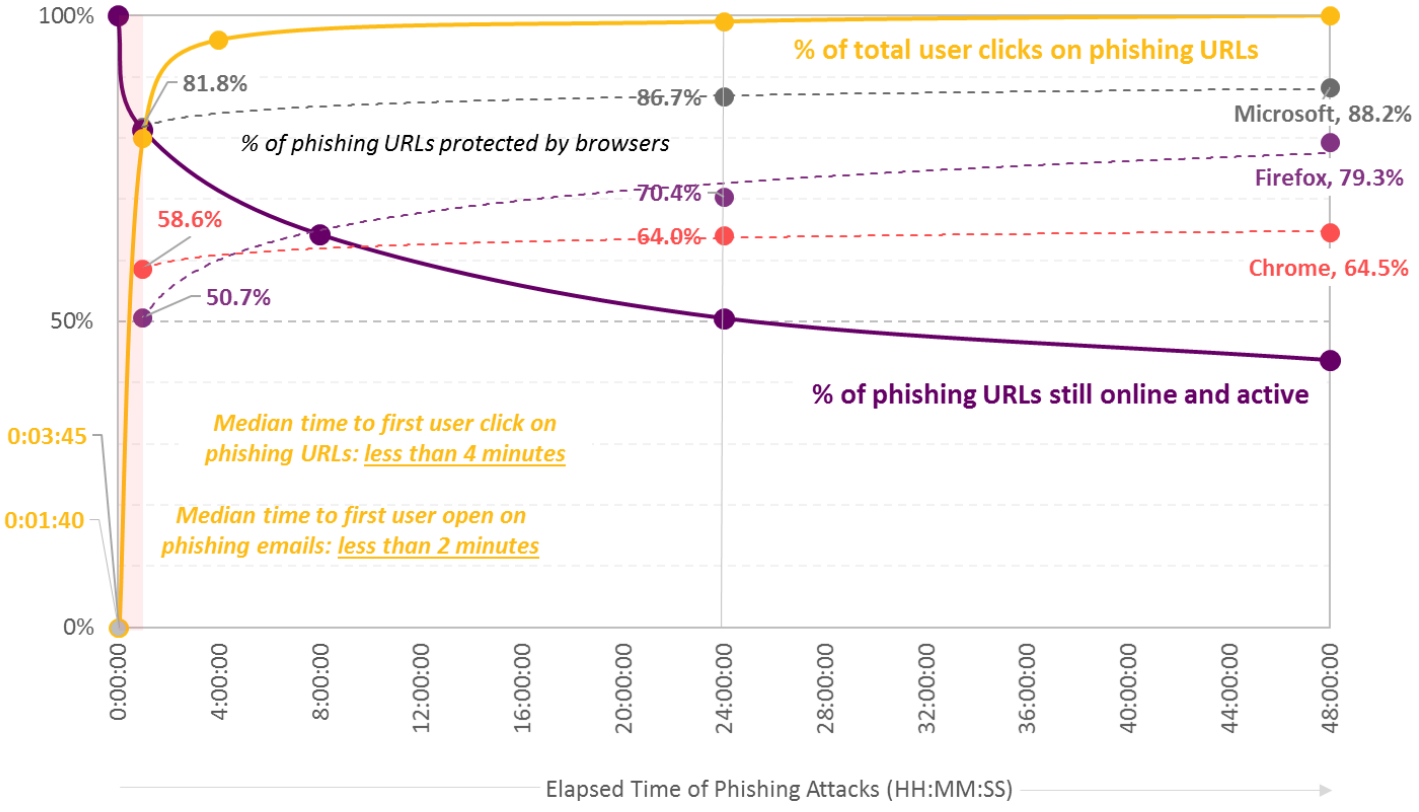
For the specific scenario described here, the median business impact of $260K is derived about 30% from the lost productivity of users, and 70% from the total cost of a data breach. For details, see the *full report*.

**about it** — and **how that recommendation will reduce the risk to an acceptable level.**

Aberdeen has previously analyzed and quantified the value of selected countermeasures for reducing the risk of phishing attacks, such as *security awareness and training for users*, and the value of incorporating *cyber insurance policies* into the traditional mix of technical, administrative, and physical security controls.

In this research report, a focus on the **timeline** of phishing attacks (see Figure 2) sheds new light on how much is at stake based on just the first few minutes of phishing attacks, and makes it clear why successful front-end protection of your organization's email and websites against phishing attacks requires a high-speed, purpose-built approach. It also shows why relying solely on browser-based protections is simply too little, too late.

Figure 2: A Good Day of Phishing is a Bad Day at the Office — From Mere Minutes to the Initial User Clicks on Phishing URLs, Attackers Hook Virtually 100% of Phishing Victims Within 24 Hours




Source: Empirical data adapted from NSS Labs 2017 *Web Browser Security Comparative Report*, Cyren 2016 *Phishing Threat Report*, and Verizon 2016 *DBIR*; Aberdeen Group, October 2017

Take a moment to study the various timelines represented in Figure 2:

- **User behaviors** (solid yellow line) — It's not surprising that email is the leading delivery mechanism for phishing attacks: empirical data shows that the median time to the *first user open of phishing emails* is **less than two minutes** (1:40); the median time to the *first user click on phishing URLs* is **less than four minutes** (3:45); and within the first 24 hours attackers have already hooked virtually 100% of their phishing victims (Source: Verizon 2016 – 2017 *DBIR*). This turns the bumper sticker adage about a bad day of fishing being better than a good day at the office inside out: a good day of *phishing* can be a very bad day at the office.
- **Browser-based protections** (dotted lines) — Empirical tests show that leading web browsers provide protection for *between 51% and 82% of phishing URLs after the first hour* of phishing attacks, and *between 64% and 87% after the first 24 hours* (Source: NSS Labs 2017 *Web Browser Security Comparative Report*). Given that the first hour yields about 80% of all user clicks on phishing URLs — which grows to virtually 100% after the first 24 hours — it's clear that relying solely on browser-based protections is simply too little, too late.
- **Attacker behaviors** (solid purple line) — Given the rapid success of phishing campaigns, it's also not surprising that by the end of the first 24 hours, attackers have already taken down nearly 50% of their phishing URLs and moved on (Source: Cyren 2016 *Phishing Threat Report*). Successful front-end protection against phishing URLs requires high-speed, purpose-built web security technology that is designed to operate *faster* than both users and attackers.

## How Faster Detection Leads to Higher Prevention, Which Reduces the Risk of Phishing Attacks

Assume for the moment the existence of such a solution — that is, high-speed, purpose-built email and web security technology that can detect and protect against phishing URLs faster than users are likely to open and click. How can we *quantify* how an investment in advanced web security reduces the annualized risk of phishing attacks?

Extending the previous risk analysis requires estimating ranges and distributions for just two additional factors: The *reduction in successful phishing attacks* as a result of the investment in advanced email and web

In the simplest possible terms, users click on phishing URLs much faster than browser-based protections against phishing URLs are put in place. By the end of the **first 60 minutes** of phishing attacks:

- About 80% of user clicks on phishing URLs have already occurred
- Attackers have already taken down about 20% of phishing URLs
- Browsers are providing protection for between 51% and 82% of phishing URLs (based on browser type)

By the end of the **first 24 hours** of phishing attacks:

- 99% of user clicks on phishing URLs have already occurred
- Attackers have already taken down nearly 50% of phishing URLs
- Browsers are providing protection for between 64% and 87% of phishing URLs (based on browser type)

Successful front-end protection against phishing URLs requires high-speed, purpose-built email and web security technology that is **designed to operate faster** than both users and attackers.

security, and the *total annual cost* of the advanced email and web security solution itself.

Based on analyst estimates for these two additional factors, Aberdeen's extended analysis for the same scenario (*private sector*, *1K users*, *100K to 1M data records*) provides the following insights, which can help senior business leaders to make a better-informed business decision about phishing risks:

- An incremental investment in advanced email and web security results in a median reduction in the annualized risk of phishing attacks of about **85%**, for a median annual return on investment of **about 11.7 times**.
- An incremental investment in advanced email and web security reduces the potentially catastrophic "long tail" of the annualized risk of phishing attacks in this scenario by **approximately 9.3 times**.
- The likelihood that an investment in advanced email and web security will "pay off" is **about 85%**. Said another way, the likelihood that a modest annual investment in advanced email and web security will cost more than the "do nothing" option is about 15% — with a potential payoff of millions from cutting off the long tail of risk.

These are insights which can only be discovered and described with a *quantitative* risk analysis. Senior business leaders would not get the benefit of these insights if security professionals provided only a single, static number (or worse, a single color). What **decision** they will make, of course, is by no means certain. That is, they may decide to:

- *Accept* the risk
- *Transfer* the risk to another party
- Take steps to *manage* the risk to an acceptable level

As always, 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.

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 data records*.

## Leading Security Solution Providers are Turning Faster Detection into More Effective Prevention, and Reduced Risk

In Aberdeen's view, **security awareness and training** for users continues to play an important — and cost-effective — role in reducing the risk of phishing attacks, and with respect to prevention, it continues to act as the organization's vital last line of defense.

For some CISOs, the solution for prevention is simply to block *all* URLs for a sufficiently long period of time (e.g., 48 hours) — which also prevents users from doing their legitimate tasks, in pursuit of the organization's strategic business objectives. In Aberdeen's view, this is an old-school, obstructive, *"Department of No"* approach to security and risk that most security leaders have rightly been working hard to cast aside and overcome.

Innovative security solution providers are now combining the **visibility** and **scale** of a global, cloud-based security platform with continuous, automated **analysis** and **correlation** of data across billions of email and web transactions per day — at speeds which are fast enough to turn *detection* of email-based phishing attacks and malicious phishing URLs into more effective *prevention*.

In Aberdeen's view, the superiority of information that comes from this emerging kind of integration, automation, and analytics — across a broad observation space — reflects the agile approach to security that defenders need to successfully manage the highly dynamic risk of phishing attacks.

**In Aberdeen's view, the superiority of information that comes from this emerging kind of integration, automation, and analytics — across a broad observation space — reflects the agile approach to security that defenders need to successfully manage the highly dynamic risk of phishing attacks.**

## Summary and Key Takeaways

- Aberdeen Group's quantitative analysis of the annualized likelihood and business impact of **phishing attacks** — for literally hundreds of scenarios, based on the selection of *industry sector*, *number of users*, and *number of data records* — helps senior business leaders to better appreciate the significant **risk** that phishing attacks represent.
- For example, for the **private sector** as a whole (i.e., across all industries), Aberdeen's Monte Carlo analysis estimates the annualized risk of phishing attacks as follows:
    - The **median** annual business impact of phishing attacks under the status quo is **about $260K**, based on the lost

productivity of *1,000 users* and a data breach of *100K to 1M records*.

- 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 range represents the *risk distribution* for phishing attacks).
- The modest difference between the lower end of the range and the median (*$0 to $260K*), as compared to the much larger difference between the median and the upper end of the range (*$260K to $10M*) is a perfect illustration of the **"long tail"** of risk that is so common in the context of cyber security, and so important for security professionals to help senior business leaders understand.

- A focus on the **timeline** of phishing attacks sheds new light on how much is at stake based on just the first few minutes, and makes it clear why successful front-end protection of your organization's email and websites against phishing attacks requires a high-speed, purpose-built approach. It also shows why relying solely on browser-based protections is simply too little, too late.
- In the simplest possible terms, users click on phishing URLs much faster than browser-based protections against phishing URLs are put in place. By the end of the **first 60 minutes** of phishing attacks:
  - About 80% of user clicks on phishing URLs have already occurred
  - Attackers have already taken down about 20% of phishing URLs
  - Browsers are providing protection for between 51% and 82% of phishing URLs (based on browser type)
- By the end of the **first 24 hours** of phishing attacks:
  - 99% of user clicks on phishing URLs have already occurred
  - Attackers have already taken down nearly 50% of phishing URLs
  - Browsers are providing protection for between 64% and 87% of phishing URLs (based on browser type)
- Successful front-end protection against phishing URLs requires high-speed, purpose-built email and web security technology that

is **designed to operate faster** than both users and attackers. Based on analyst estimates for the speed and cost of such a solution, Aberdeen's extended analysis for the same scenario provides the following insights, which can help senior business leaders to make a better-informed business decision about phishing risks:

- An incremental investment in advanced email and web security results in a median reduction in the annualized risk of phishing attacks of about **85%**, for a median annual return on investment of **about 11.7 times**.
- An incremental investment in advanced email and web security reduces the potentially catastrophic "long tail" of the annualized risk of phishing attacks in this scenario by **approximately 9.3 times**.
- The likelihood that an investment in advanced email and web security will "pay off" is **about 85%**. Said another way, the likelihood that a modest annual investment in advanced email and web security will cost more than the "do nothing" option is about 15% — with a potential payoff of millions from cutting off the long tail of risk.

- Innovative security solution providers are now combining the **visibility** and **scale** of a global, cloud-based security platform with continuous, automated **analysis** and **correlation** of data across billions of email and web transactions per day — at speeds which are fast enough to turn *detection* of email-based phishing attacks and malicious phishing URLs into more effective *prevention*.
- In Aberdeen's view, the superiority of information that comes from this emerging kind of integration, automation, and analytics — across a broad observation space — reflects the agile approach to security that defenders need to successfully manage the highly dynamic risk of phishing attacks.

## Related Research

*Enterprise Email: Are You Adequately Addressing Your Risks?; August 2017*

*Security Awareness Training: Small Investment, Large Reduction in Risk; July 2017*

*Smaller Businesses Have Bigger Risk: Quantifying the Risk of a Data Breach; July 2017*

*Cyber Security in 2017 and Beyond: For the Defenders, It's About Time; April 2017*

### 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.



17062