KB

3 SHORT TAKES ON SUCCESSFUL DATA PROTECTION INITIATIVES

July 2019

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

ABERDEEN

Every enterprise has initiatives in place to provide some level of protection for its valuable or regulated data. Here are three "short takes" on why they're needed, and what helps them to be more successful.

Short Take 1: Wait, Why Are We Still Talking About PCI?

It's hard to believe, but security professionals and solution providers have been talking about the need to protect **cardholder data** (i.e., payment card account numbers, cardholder names, expiration dates, and security-related information used to authenticate cardholders or authorize transactions) — wherever that data is stored, processed, and transmitted — since the 1990s.

It's hard to believe, but security professionals and solution providers have been talking about the need to protect *cardholder data* since the 1990s.

Starting with the independently developed data protection initiatives of the major card brands (i.e., Visa, Mastercard, American Express, Discover, JCB), the industry standards and best practices for this nearly universal issue have continued to mature and evolve. From the version 1.0 release of the **Payment Card Industry Data Security Standard (PCI DSS)** in December 2004, to the now-current version 3.2.1 release in May 2018, one would think that everyone would have this problem fully solved by now, right?

Wrong. Neither *time* (more than 20 years, and counting), nor *carrots* (positive impact on reputation and brand, reduced risk of a data breach), nor *sticks* (negative impact on reputation and brand, significant cost of a data breach, fines and penalties for non-compliance) have succeeded in getting all affected organizations to meet these minimum standards for protecting cardholder data. For example in a recent Aberdeen study, out of 222 organizations who create, collect, integrate, process, store, or transmit cardholder data such that it is subject to PCI compliance requirements — just 135 (61%) said that they have currently achieved, report, and certify compliance.

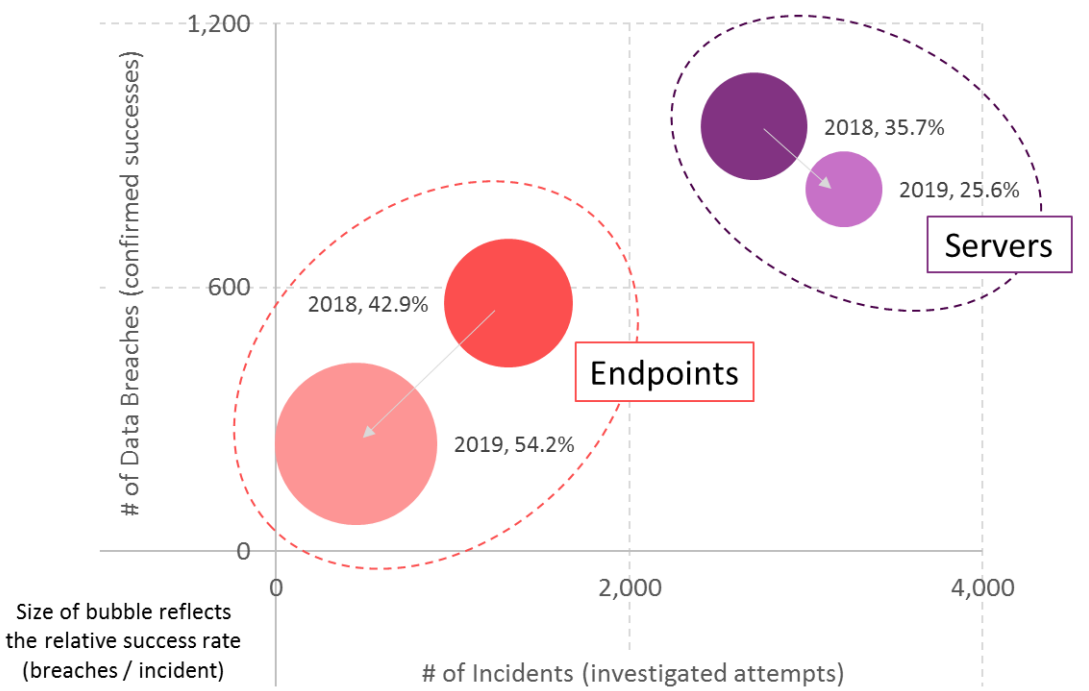
To be fair, 6 out of 7 (86%) respondents have to deal with the complexity of *multiple* types of data and / or data-related processes subject to security and privacy compliance requirements — just 1 in 7 (14%) have the relative simplicity of having to deal with only one. If Best-in-Class data protection and compliance were easier and less expensive to implement, there would be far more companies doing it.

None of the above would matter, if data breaches rarely occurred. Unfortunately, Aberdeen's analysis of more than 3,200 public data breach disclosures from 2017-2018 shows that about 75% of all disclosed data

breaches are the result of **malicious intent** (i.e., primarily from cybercriminals and other external threat actors), while the remaining 25% are **self-inflicted** (e.g., accidental loss of data and devices). If cybercrime didn't pay, there would be far fewer cybercriminals.

Just where are these data breaches occurring? An analysis of empirical data for *security incidents* (i.e., any attempt to compromise the confidentiality, integrity, or availability of a data asset) and *data breaches* (i.e., the confirmed disclosure of a data asset to an unauthorized party) by the type of asset compromised shows that **servers** (e.g., back-end applications and databases) **are much more frequently under attack**. But **endpoints** (e.g., user devices, point of sale devices, other connected devices) **have a much higher likelihood of being compromised**. As shown in the following chart, for each of the past two years servers have been in the upper-right quadrant based on both number of investigated attempts and number of confirmed successes. But the *effective success rate* (breaches / incident) is much higher for endpoints (between 43-54%) than for servers (between 26-36%). See Figure 1.

Figure 1: Analysis of Data Breaches Shows Servers More Frequently Under Attack, But Endpoints More Likely to Be Compromised



Source: Data adapted from Verizon DBIR 2018 (N=4,020), 2019 (N=3,667); Aberdeen, July 2019

From a high-level perspective, this makes perfect sense. Back-end systems typically represent the large, concentrated repositories of **structured data** (i.e., databases) — the "crown jewels" of enterprise data assets, and a big prize for financially motivated attackers. In contrast, endpoints typically represent multi-sized, widely distributed instances of **unstructured data** (i.e., files) — which are often an integral, critical component of core business processes and workflows, with a much bigger and more complex attack surface.

What can be done to protect cardholder data more effectively in these unstructured, endpoint-oriented use cases?

Ancient and venerable best practices — such as "remove cardholder data from your environment" — are always a good place to start. This *reduces the risk of a data breach*, *reduces the scope of compliance requirements*, and as an extra bonus *reduces the burden for ongoing auditing and reporting*.

However, there's an even more fundamental first step: Before cardholder data can be removed or protected, we first have to know where it is. In other words, **discovery** of cardholder data in your environment is also a critical technical capability.

And how awesome would it then be, to not still be talking about PCI?

Short Take 2: Are You Putting the "P" in DLP?

Data Loss Prevention (DLP) solutions are designed … well, to prevent the loss of enterprise data. Said a bit more formally: By "loss," we mean the confirmed disclosure of an organization's data assets to an unauthorized party — i.e., a **data breach**. Said still another way, DLP solutions are designed to *reduce the risk of a data breach*.

This begs an obvious question, which unfortunately doesn't often get a crisp response: Just what *is* the risk of a data breach? To answer this question in a way that's useful to an organization's senior leadership team, security professionals and solution providers have to consider both the *likelihood* that a data breach may happen in a specified period of time, as well as the resulting *business impact* if it actually does occur. That's just the proper definition of risk.

To help address this glaring need, Aberdeen continues to look for ways to leverage the growing body of publicly available data regarding the **likelihood** (e.g., Verizon *DBIR*), *size* (e.g., Thales eSecurity *breachlevelindex.com*), and **business impact** (e.g., Ponemon *Cost of a Data Breach*) of data breaches to

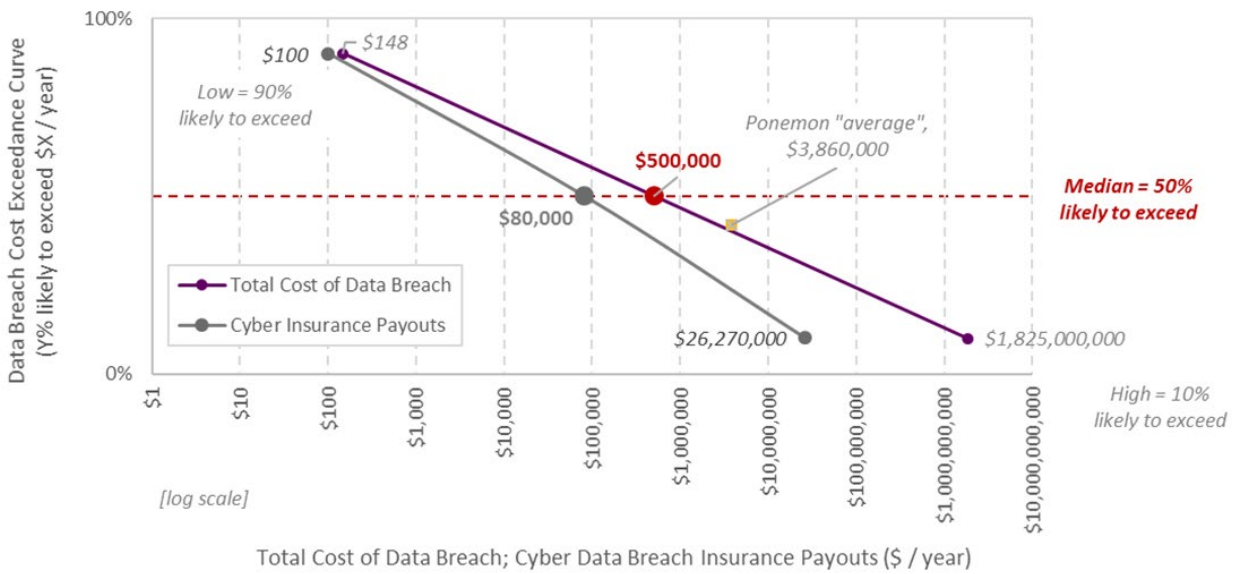
An *automated* approach to protecting valuable or regulated data is the key to putting the "P" in DLP — and helps to achieve the goal of *reduced risk*, along with support for *higher scale* at *lower overall cost*.

quantify the annualized risk of a data breach, as risk is properly defined. That is, not as a falsely precise, single-point estimate, but as an estimate of a **range of possible outcomes** and their **associated likelihoods**.

For example, for the private sector as a whole (all industries), Aberdeen's Monte Carlo analysis shows that the **median** total business impact of a data breach is **about $500K**. Even more importantly, however, there's a **10% likelihood** that the total business impact of a data breach is **more than $1.8B**. This is the "long tail" of risk that's so important to help the senior leadership team to understand — this is the part of the risk *exceedance curve* which has the greatest influence on how business decisions ultimately get made (see Figure 2).

As a point of reference, Aberdeen's analysis of publicly available data (e.g., NetDiligence *Cyber Claims Study*) also shows that the median payout of cyber data breach insurance claims is **about $80K** — which means that cyber insurance payouts are covering *less than 20%* ($80M out of $500K) of the total business impact at the median, and *less than 2%* of the total business impact ($26.3M out of $1.8B) at the long tail.

Figure 2: Quantifying the Risk of a Data Breach Supports Better-Informed Business Decisions Regarding What to Do About It



Source: Monte Carlo analysis, based on data adapted from Verizon *DBIR 2018* (breach likelihood), Thales eSecurity *breachlevelindex.com 2017-2018* (breach size), Ponemon *Cost of a Data Breach 2018* (breach impact), and NetDiligence *Cyber Claims Study 2018* (payouts); Aberdeen, June 2019

And *that* is why we need to address the issue of putting the “P” in DLP. How much of that risk is your organization’s senior leadership team willing to accept?

Using content-aware, monitoring / filtering technologies such as DLP to identify valuable or regulated data is necessary, but by itself that isn’t enough. Having the means on the front-end to accurately *identify* and *classify* data that needs to be protected is an important prerequisite for the ultimate goal: a flexible, automated capability on the back-end to enforce security policies and protect the data.

Aberdeen’s research has shown that organizations with DLP initiatives generally use three high-level strategies to enforce their security policies and protect their data:

- **None / Passive** — this approach corresponds to controls such as *logging* for audit purposes, and sending *notifications* to administrators, users, and / or managers. Many would refer to this as a “learn mode” approach, in the sense that it helps to provide a baseline of how valuable or regulated data is being used, without creating friction or disruption in the organization’s workflows.
- **User-based** — this approach requires a human (an administrator, or a user) to *make a decision* about the data that has been identified, and the controls that should be invoked to enforce the organization's policies. For example: the DLP system might identify customer data that needs to be protected in compliance with data privacy regulations, and the user needs to decide to encrypt it (and how) before it moves to the next phase of the business process.
- **Automated** — this approach refers to controls that are invoked automatically for protecting data that has been identified as valuable or regulated by content-aware technologies.

The time-tested strategy of “first crawl, then walk, then run” is a pragmatic approach for successful, enterprise-wide rollouts of data protection initiatives, and Aberdeen’s research has shown that DLP initiatives are no exception. Running a DLP solution in passive mode generates valuable visibility and insight into the current flow of information throughout the extended enterprise, and reduces the likelihood of inadvertently bringing the flow of information — and the business itself — to a halt.

As DLP initiatives mature, however, an **automated** approach to protecting valuable or regulated data is the key to putting the “P” in DLP — and helps to

achieve the goal of *reduced risk*, along with support for *higher scale* at *lower overall cost*.

Short Take 3: For Successful Data Protection, Easy Does It

In the realm of information security, the traditional trade-offs that security professionals seek to balance — i.e., **effectiveness of security**, **total cost of ownership**, and **convenience for users** — have been the relentless targets for continuous improvement by innovative solution providers. And as anyone who's been around for a while would have to admit: Compared to the security solutions that were in place 20, 10, and even 5 years ago, today's security solutions are *more capable*, *more cost-effective*, and *much easier to use*.

Even so, there were *more than 3,200* publicly disclosed data breaches in the period 2017-2018 — a run rate of *between 4 and 5 data breaches per day*. Although the median number of records disclosed to unauthorized parties was relatively small (about 1,300 records per breach), there were *114 data breaches of 1M records or more* during this two-year period — a run rate of about *one mega-breach per week* to dominate the headlines.

How can these two observations be reconciled? In Aberdeen's view:

- **Solution providers** will continue to enhance the capabilities and effectiveness of security solutions, as well as to drive down their total cost of ownership for enterprise buyers. As evidenced by the existence of an estimated 3,500 companies in this space, this is clearly viewed an important problem to solve.
- **Security professionals** must continue to mature in their ability to *quantify* security-related risks, and *communicate* more effectively about risk (in business terms) to help senior leaders make better-informed business decisions regarding what to do about it. Total cost of ownership for security solutions is only relevant in the context of how that investment reduces their risk. Said another way, it's always a question of whether the proverbial juice (reducing their risk to an acceptable level) is worth the proverbial squeeze (total cost of implementing the solution).

Which brings us directly to **convenience and ease of use**, the third leg of the traditional trade-offs. How much does this really matter?

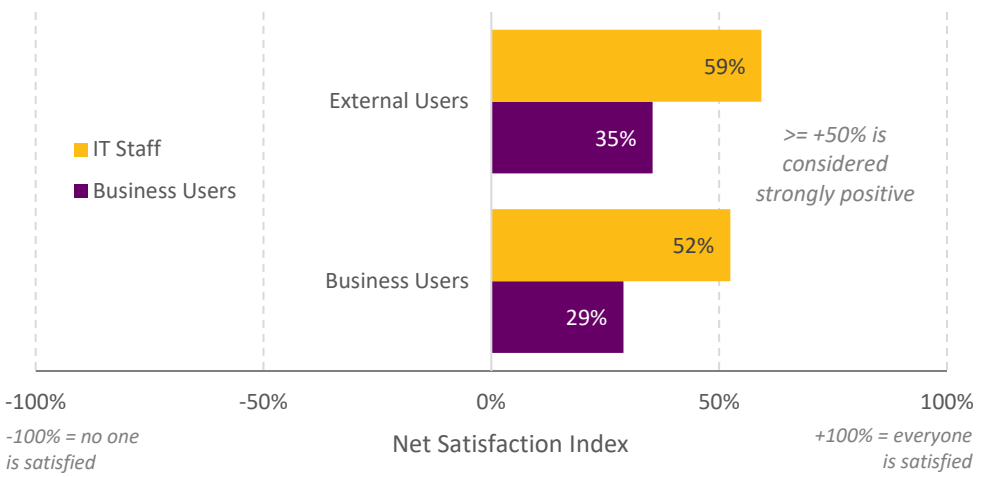
As it turns out, it matters quite a bit. For example, on the topic of **enterprise collaboration** Aberdeen's benchmark research revealed a significant

Data protection solutions that make it easy for business users to collaborate securely with external parties when valuable or regulated data is legitimately involved — using familiar productivity tools — will have the fastest path to user acceptance, and the highest likelihood for success.

misalignment between *business users* and *technical staff* on this important question:

- Both groups agreed that **data privacy** and **data security** is a leading concern — e.g., when collaboration involves enterprise data which is *valuable* (e.g., intellectual property, confidential information) or *regulated* (e.g., cardholder data, personal health information, personally identifiable information).
- But business users and technical staff had significantly different views on **cost**, and on the **ability of IT** to support business needs. The issue is not that these projects aren't being sufficiently funded — in Aberdeen's study, most respondents indicated a **year-over-year increase** in the resources being allocated. The issue is that business users perceive that their needs are changing faster than the ability of technical staff to keep up.
- When it comes to *results*, however, the **net satisfaction** of business users (both internal and external) with current enterprise collaboration initiatives was **about 60% less** than what technical staff perceived it to be. For business users, convenience and ease of use has a significant impact on their net satisfaction, and the extent to which they will embrace a given solution in their daily activities — or continue to look for shortcuts and workarounds.

Figure 3: User Satisfaction with Current Enterprise Collaboration Initiatives is Perceived Differently by Business Users and IT Staff



Source: Aberdeen, July 2019

Unless you work in an organization with a strict command-and-control, "do it my way or hit the highway" kind of culture, solutions that are not convenient

and easy to use are unlikely to fully achieve their intended business objectives. For example:

- Aberdeen's study on web site performance confirmed what most of us already know from firsthand experience: The longer the response time, the more likely users are to abandon the site and move on — with 20% abandonment after a delay of just 3 seconds.
- In another dimension, a user experience that required an additional, overt authentication step to be taken was found to result in abandonment rates of as high as 20%, with a most likely range between 4% and 10%.

For these reasons, data protection solutions that make it easy for business users to collaborate securely with external parties when valuable or regulated data is legitimately involved — using familiar productivity tools — will have the fastest path to user acceptance, and the highest likelihood for success.

For successful data protection initiatives, "easy" does it.

About Aberdeen

Since 1988, Aberdeen 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. Aberdeen provides intent-based marketing and sales solutions that deliver performance improvements in advertising click-through rates and sales pipelines, resulting in a measurable ROI. Aberdeen is headquartered in Waltham, Massachusetts, USA.

17956