RR

# ENCRYPTION EVERYWHERE REDUCES RISK — BUT CHOOSE THE RIGHT TOOL FOR THE JOB

June 2019

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

ABERDEEN

As the risk of a data breach continues to motivate organizations to expand their use of **encryption**, it's important to select the appropriate solutions for each respective use case. Aberdeen's analysis frames how to choose the right tool for the job.

## Why Encryption Matters: Quantifying the Risk of a Data Breach

If we want to communicate effectively about the **risk** of a data breach, we need to use the proper language. That is, for any given undesirable incident that could potentially happen to our enterprise data — whether a compromise to its *confidentiality*, *integrity*, or *availability* — we have to consider both the *likelihood* that the incident might take place in a given period of time, as well as the resulting *business impact* if it actually does occur. If we're not talking about both how likely and how much business impact in this way, we're not really talking about risk!

Too much of the time, IT and Security teams tend to focus intensely on identifying the undesirable incidents that could result in a data breach, i.e., the technology-oriented details of "who, what, and how" regarding the latest *threats*, *vulnerabilities*, and *exploits*. The senior leadership team, however, is primarily interested in the business-oriented details of "why it matters."

To help bridge this critical communications gap, Aberdeen continues to use the growing body of empirical data regarding the likelihood, size, and business impact of data breaches to *quantify* the annualized risk of a data breach, as risk is properly defined — i.e., not as a falsely precise, single-point estimate, but as *a range of possible outcomes* and their associated likelihoods.

For example, Figure 1 provides several valuable insights about the annualized risk of a data breach for the **private sector** as a whole (all industries), including the following:

- The **median** total business impact of a data breach is **about $500K** — which illustrates just how misleading it is to refer to an "average" impact of $3.86M (i.e., by a factor of about eight times)!
- More importantly, there's a **10% likelihood** that the total business impact of a data breach is **more than $1.8B**. This is the "long tail" aspect of the risk of a data breach that is so important for IT and

Aberdeen has leveraged the growing body of empirical data regarding the *likelihood*, *size*, and *business impact* of data breaches to *quantify* the annualized **risk** of a data breach, as risk is properly defined — i.e., not as a falsely precise, single-point estimate, but as *a range of possible outcomes* and their associated likelihoods.

For the private sector as a whole (all industries):

- The **median** total business impact of a data breach is **about $500K**.
- More importantly, there's a **10% likelihood** that the total business impact of a data breach is **more than $1.8B**.
- Cyber data breach insurance payouts are covering **less than 20%** of the total business impact at the median, and **less than 2%** of the total business impact at the "long tail."

This gap is **why encryption matters** — it explains, in business terms, why IT and Security teams are motivated to expand the use of encryption to protect their organization's valuable and regulated data. Even better, it helps to justify an incremental investment in the appropriate encryption solutions.

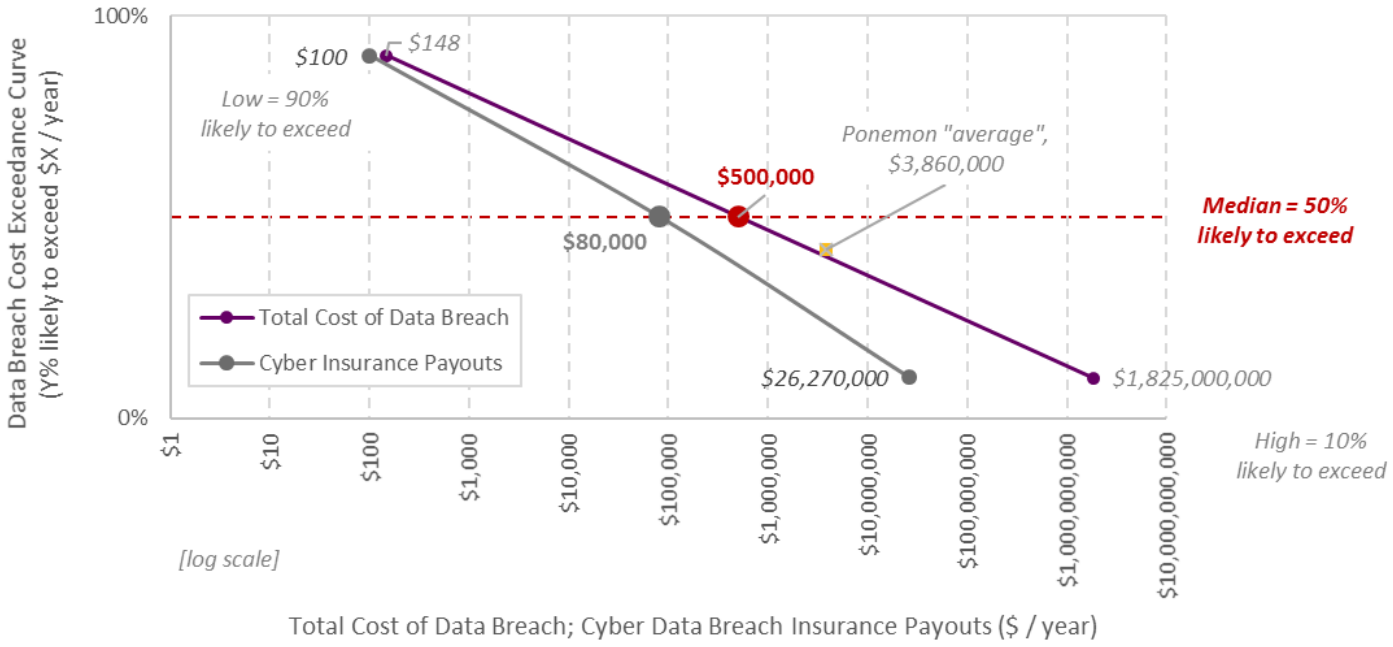
Security professionals to communicate effectively to the senior leadership team, to help them make a better-informed business decision regarding what to do about it.

- As a point of reference, the **median** payout of cyber data breach insurance claims is **about $80K** — which means that cyber insurance payouts are covering *less than 20%* 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.

- An **incident** refers to any attempt to compromise the confidentiality, integrity, or availability of a data asset

- A **data breach** refers to the confirmed disclosure of a data asset to an unauthorized party

## Figure 1: 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), and Ponemon *Cost of a Data Breach 2018* (breach impact); Aberdeen, June 2019

As visualized in Figure 1, the gap between the total cost of a data breach (represented by the purple line) and the total value of cyber data breach insurance payouts (represented by the gray line) highlights the **residual risk** of a data breach for the private sector.

This gap is **why encryption matters**. To the extent that the senior leadership team finds this level of risk to be unacceptably high, this gap explains — in business terms — why IT and Security teams are motivated to **expand the use of encryption** to protect their organization's valuable

and regulated data. Even more importantly, it helps to **justify an incremental investment** in the appropriate encryption solutions.

## Encryption Everywhere is the Vision — But Where to Begin?

Even if the ultimate vision for protecting the organization's data is to **encrypt everything**, the practical wisdom of "first crawl, then walk, then run" still applies. So where should IT and Security teams begin?

Analysis of more than 3,200 public data breach disclosures in 2017-2018 shows that about 75% of all disclosed data breaches are the result of **malicious intent** (primarily from external threat actors), while the remaining 25% are **self-inflicted** (e.g., accidental loss of data and devices). So as a first step, it makes sense to prioritize encryption of the organization's "crown jewels" — i.e., data that would be of greatest interest to threat actors who are financially motivated (see Table 1).

**About 75% of all disclosed data breaches are the result of malicious intent, primarily from external threat actors — while the remaining 25% are self-inflicted, e.g., accidental loss of data and devices.**

Table 1: External, Financially Motivated Threat Actors Make Encryption of the Organization's "Crown Jewels" a Top Priority

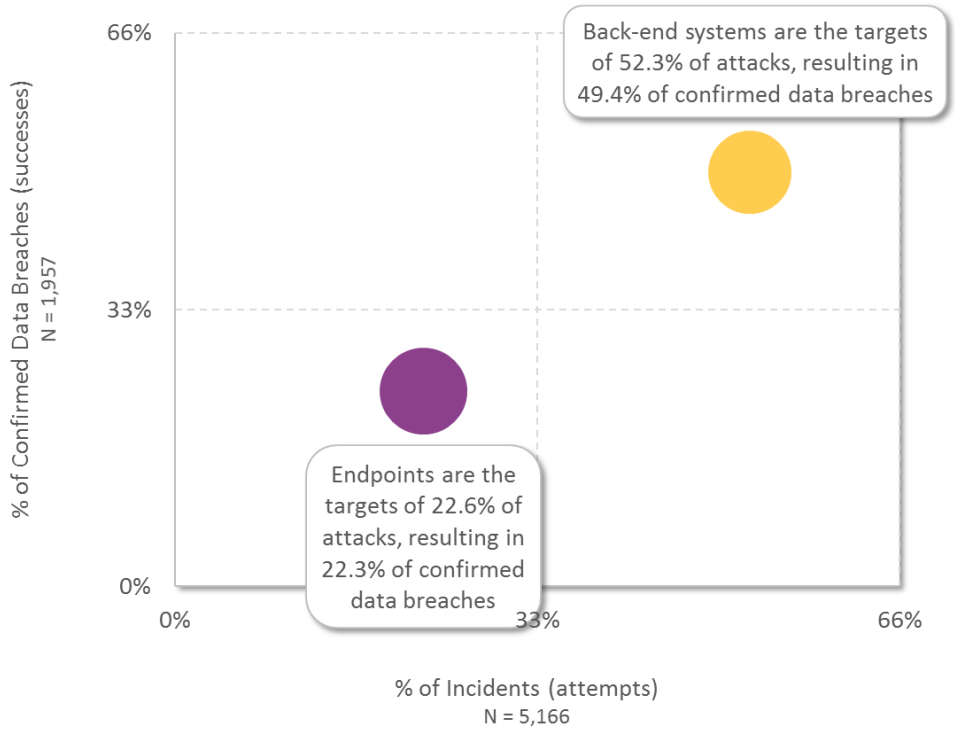
| Type of Data Breach, By Source of Breach | Identity Theft | Financial Access | Account Access | Existential Data | Nuisance | Total |
|---|---|---|---|---|---|---|
| **With Intent** | **1,588** | **423** | **214** | **87** | **86** | **2,398** |
| Malicious Outsider | 1,398 | 390 | 193 | 51 | 72 | 2,104 |
| Malicious Insider | 159 | 31 | 11 | 35 | 7 | 243 |
| Hacktivist | 16 | 2 | 9 | 1 | 2 | 30 |
| Stolen Device | 14 | | | | 1 | 15 |
| Ransomware | 1 | | | | 4 | 5 |
| State Sponsored | | | 1 | | | 1 |
| **Self-Inflicted** | **581** | **60** | **115** | **23** | **58** | **837** |
| Accidental Loss | 576 | 60 | 115 | 23 | 58 | 832 |
| Lost Device | 5 | | | | | 5 |
| **Total** | **2,169** | **483** | **329** | **110** | **144** | **3,235** |

Source: Data adapted from Thales eSecurity *breachlevelindex.com 2017-2018*; Aberdeen, June 2019

A separate analysis of more than 5,100 security incident investigations (which resulted in nearly 2,000 confirmed data breaches) points towards giving priority to encrypting enterprise data in **back-end systems** over data on **endpoints**. As seen in Figure 2, successful data breaches are

**two to three times more likely** to occur for data in back-end systems than for data on endpoints — since back-end systems tend to be where the "crown jewels" of enterprise data assets are located, it's only logical that these are the most attractive targets for attackers.

Figure 2: From the Likelihood Perspective of Risk, Attackers Find Enterprise Data in Back-End Systems the Most Attractive Targets




Source: Data adapted from Verizon *DBIR 2018*; Aberdeen, June 2019

## All Encryption Solutions are Not Created Equal: Choosing the Right Tool for the Job

Aberdeen's research reflects continued growth in the use of encryption to protect valuable or regulated enterprise data, wherever it flows — in back-end systems, on endpoints, and on the network. But the motivation for implementing encryption — i.e., the **threats** that organizations intend for encryption to help them address, to reduce their risk — can be markedly different from one use case to another. As always, decisions about which security controls to deploy have to be made in a specific *context*.

For enterprise data on **endpoints** (e.g., PCs, laptops, and a wide variety of mobile devices), the primary threat is that these assets are very commonly *lost*, *stolen*, or simply *unaccounted* for. For these threat

Interestingly, the **likelihood of attacker success** (i.e., number of confirmed breaches / number of incidents) is similar for both asset categories:

- **36% for back-end systems** (966 breaches; 2,704 incidents)
- **39% for endpoints** (455 breaches; 1,169 incidents)

scenarios, **full-disk encryption** provides a high level of assurance that data protection is actually in place, requires no day-to-day involvement or decisions on the part of the organization's users, and has little to no impact on endpoint performance or user experience. When used in conjunction with a *hardware root of trust* (e.g., a **trusted platform module**), full-disk encryption solutions can also assure that endpoints and platform-level software boot up in a known, unaltered, and trusted state — i.e., free of rootkits or other malware.

- **Self-encrypting drives** refers to full-disk encryption that has been implemented natively in the hardware of the storage device.

For enterprise data on **back-end systems** (e.g., file servers, network servers, or cloud-based storage), the biggest threats are infiltration and unauthorized access by *external attackers*, fraud or theft by *trusted insiders*, and non-malicious *errors* made by authorized, well-intended users. In these threat scenarios, **file-level encryption** — which unlike full-disk encryption is actively protecting the organization's data whenever these back-end systems are online, available, and accessible, even if unauthorized access has been successfully achieved — stands out as the most appropriate choice.

Specifically for *structured* data (i.e., databases) in back-end systems, widely deployed database products from Oracle, IBM, Microsoft, and others include native capabilities for **database encryption** (sometimes referred to as **transparent data encryption**). For organizations dealing with the complexity, diversity, and scale of multiple databases from multiple vendors, Aberdeen has previously quantified how using a *common platform* for database encryption reduces risk by making it easier and more cost-effective to rotate encryption keys more frequently, and by improving the time and consistency of database recovery.

**Related Research:**
***A Common Platform for Database Encryption: Lower Cost, Reduced Risk*, June 2018**

**Application-level encryption** refers to the use of application programming interfaces (APIs) to make it easier for software developers — who need not be experts in cryptography or encryption key management — to integrate *encryption*, *tokenization*, *data masking*, and other cryptographic capabilities into new or existing applications. Application-level encryption provides the most granular level of protection against the threats to data in back-end systems, which must be balanced against the time and resources required for development, testing, and ongoing support.

- **Tokenization** refers to the substitution of unique, randomly generated values (*tokens*) to *reference* valuable or regulated data, while maintaining the length and format of the original data — one example of protecting enterprise data by taking it out of the business process in the first place.

High-level selection criteria for choosing between full-disk encryption, file-level encryption, database encryption, and application-level encryption are summarized in Table 2. In general, the level of data protection increases from left to right — as does the effort for implementation.

## Table 2: Reduce the Risk of a Data Breach with Encryption — Choose the Right Tool for the Job

| High-Level Solution Selection Criteria | Full-Disk Encryption | File-Level Encryption | Database Encryption | Application-Level Encryption |
|---|---|---|---|---|
| ▪ **Threat:** Unauthorized access to valuable or regulated data on systems which are *lost*, *stolen*, or *unaccounted for* | ▪ Protects all enterprise data on endpoint devices which are lost, stolen, or unaccounted for | ▪ Not a priority threat for back-end systems | ▪ Not a priority threat for back-end systems | ▪ Not a priority threat for back-end systems |
| ▪ **Threat:** Unauthorized access to valuable or regulated data by *external attackers*<br>▪ **Threat:** Fraud or theft resulting from access to valuable or regulated data by *trusted insiders*<br>▪ **Threat:** Non-malicious *errors* which result in compromises to data confidentiality, integrity, or availability | ▪ When used in conjunction with hardware, can assure that endpoints and platform-level software boot up in a known, unaltered, and trusted state (i.e., free of rootkits or other malware)<br>▪ Provides no additional protections to data or systems when endpoints are online, available, and accessible | ▪ Protects against unauthorized access to both unstructured data (*files*) and structured data (*databases*) — even while back-end systems are online, available, and accessible<br>▪ Guards against abuse by trusted insiders<br>▪ Includes logging, monitoring, and integration with existing detection and response capabilities | ▪ Protects against unauthorized access to valuable or regulated data in databases<br>▪ Encrypts data in *selected columns or tables* of a database — but not configuration files, system logs, or reports | ▪ Protects against unauthorized access to valuable or regulated data in enterprise-developed applications, including exploits based on SQL injection attacks<br>▪ Guards against abuse by trusted insiders<br>▪ Encrypts granular subsets of data, such as *selected fields* in a database, before it is transmitted or stored |
| ▪ **Deployment considerations** | ▪ Simple to deploy — particularly for full-disk encryption that has been implemented natively in self-encrypting drives<br>▪ Transparent to users and applications — no changes required | ▪ Requires implementation of platform-specific *software agents* for every file server, network server, or cloud-based storage, along with associated *management infrastructure*<br>▪ Transparent to users and applications — no changes required | ▪ Widely deployed database products (e.g., Oracle, IBM, Microsoft) include native capabilities for database encryption<br>▪ Native database encryption from multiple vendors results in greater complexity, higher costs, and increased risk | ▪ *APIs* enable software developers — who need not be experts in cryptography or encryption key management — to integrate encryption into new or existing applications<br>▪ Requires development, testing, and ongoing support |

Source: Aberdeen, June 2019

## Summary and Key Takeaways

Aberdeen's quantification of the risk of a data breach strongly supports the motivation to **expand the use of encryption** to protect valuable and regulated data, and helps to **justify an incremental investment** in the appropriate encryption solutions. Being clear about the *context* for each use case for encryption — including both the *threats* that represent the highest priority, as well as the tradeoffs between the *level of protection* and the *effort of implementation* for different solutions — go a long way towards **choosing the right tool for the job**:

- Full-disk encryption
- File-level encryption
- Database encryption
- Application-level encryption

## Related Research

*A Common Platform for Database Encryption: Lower Cost, Reduced Risk;* June 2018

*Enterprise Data in 2018: The State of Compliance, Privacy, and Security;* June 2018

*Why 6 Out of 7 Enterprises Need a Common Platform for Database Encryption;* January 2018

*It's About Time: How Faster Database Recovery Reduces Risk;* November 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.



17921