RR

ENCRYPTION ALONE IS NOT ENOUGH: WHAT MAKES YOUR DATA PROTECTION INITIATIVE SUCCESSFUL?

May 2018

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

ABERDEEN

Aberdeen's analysis shows that organizations who are thinking about data protection initiatives are overwhelmingly focused on **technical controls**, while paying much less attention to **business context** and **risk**. Successful enterprise data protection initiatives incorporate technology thoughtfully into the data's *lifecycle* and *workflows*.

How Enterprises are Currently Thinking About Data Protection

To gain insights into how enterprises are currently thinking about **data protection** and **data security** initiatives, Aberdeen looked at the patterns of more than 62,300 organizations with a higher-than-baseline level of online search activity on these topics — including more than 16,700 large enterprises and 45,500 small- and mid-size businesses. The results provide valuable insights into the prevailing approach to enterprise data protection initiatives, which can be summed up as **"Fire, Ready, Aim."**

The prevailing approach to enterprise data protection initiatives emphasizes **technical controls** over **business context** and **risk** — an approach which can be summed up as **"Fire, Ready, Aim."**

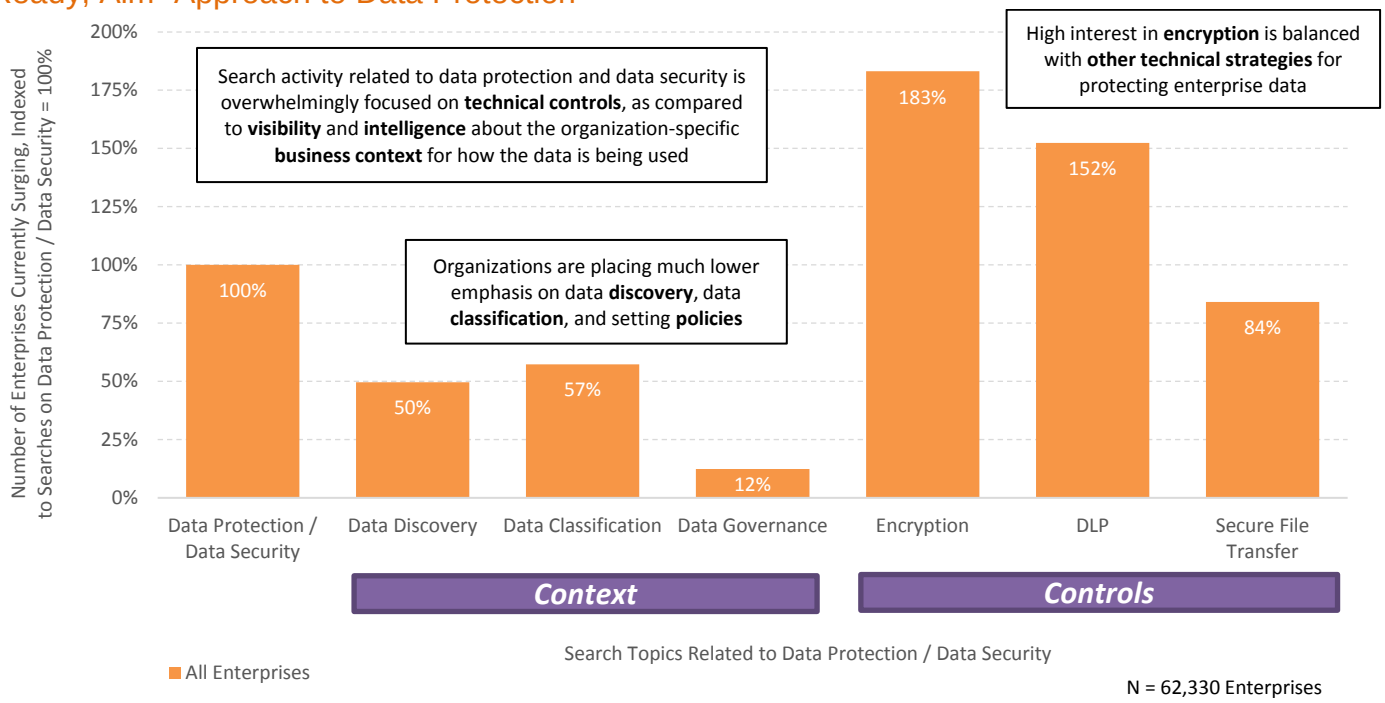
Consistent with previous research, search activity related to data protection and data security is overwhelmingly focused on specific **technical controls** (e.g., *encryption*, *data loss prevention*, *secure file transfer*), with significantly less attention being given to the means to gain crucial **visibility** and **intelligence** about the organization-specific **business context** for how and why the data is being used, such as:

- What data do we have?
- Where is it?
- What data has value?
- Who has access? Who should and should not have access?
- What patterns of access are normal?
- What policies for access and protection should be put into place?

The prevailing emphasis on technical controls over business context and risk is depicted visually in Figure 1. To show the relative level of online search activity in these areas, the number of organizations currently *surging* on selected topic groupings are indexed to searches on data protection and data security set to 100%.

Company Surge is scored on a scale from zero to 100; a score of 60 or higher indicates online search activity which is significantly higher than normal.

Figure 1: Aberdeen's Analysis of Enterprise Online Search Activities Provides Valuable Insights into the Prevailing "Fire, Ready, Aim" Approach to Data Protection



Source: Adapted from Bombora Company Surge data; Aberdeen, May 2018

Relative to surges on **data protection** and **data security** (set to 100%):

- Organizations are placing roughly half as much emphasis on **data discovery** (50%) for identifying the data itself, **data classification** (57%) for identifying the greatest risks, and **data governance** (just 12%) for identifying the most appropriate policies.
- In contrast, organizations are placing roughly two times more emphasis on technical controls for data protection such as **data encryption** (183%), which is balanced with other technical strategies such **data loss prevention** (152%) and **secure file transfer** (84%).

Keeping in mind the overarching purpose and objective of any cyber security initiative — which is always to help **make better-informed business decisions about risks**, and to help **manage those risks to an acceptable level** — the prevailing emphasis on controls over context and risk is backwards. It puts the "Fire" before the "Ready" and the "Aim." Successful data protection initiatives need all three of these elements, ideally in the logically correct order.

The hard truth — as seen in Aberdeen's May 2018 research report *Enterprise Data in 2018: The State of Privacy and Security Compliance*, based on a study of more than 360 organizations — is that the majority of respondents are neither secure nor compliant, despite their considerable level of investment in initiatives for data protection and data security:

- About **3 out of 5 (58%)** enterprises experienced **at least one data breach** over the last 12 months (median = 3).
- About **3 out of 4 (75%)** enterprises experienced **at least one non-compliance issue** over the last 12 months (median = 3).
- A **median of 30%** of the **overall IT operations budget (OpEx)** is being allocated to the achievement and reporting / certification of compliance with data privacy and data security requirements.

The hard truth is that under the prevailing approach to data protection initiatives, most organizations are neither **secure** nor **compliant**, despite their considerable **level of investment**: a median of 30% of the overall IT operations budget.

Resources allocated to data protection and data security initiatives are unavailable for *digital transformation* or other strategic business priorities, at a potentially enormous opportunity cost. This is all the more reason to learn more about the approach that increases the likelihood for success.

More Than Just Technology: Successful Data Protection Initiatives Consider Context, Risks, and Controls

The usual logic behind making the leap to implement technical security controls sounds familiar, and it's common to hear security professionals (and solution providers) make some or all of the following arguments:

- **Our organization relies heavily on its data** — information is essential to generating revenue, serving customers, making users productive, collaborating with business partners, and countless other business-critical processes.
- **We have, generate, and share a lot of data** — and we are continuously generating and sharing even more of it, at an ever-increasing rate.
- **We have data that is valuable and / or sensitive** — a point which is reflected in an exceedingly complex mix of requirements for privacy, security, and compliance.
- **A lot of valuable and sensitive data gets compromised** — as evidenced by the endless flow of public data breach disclosures.

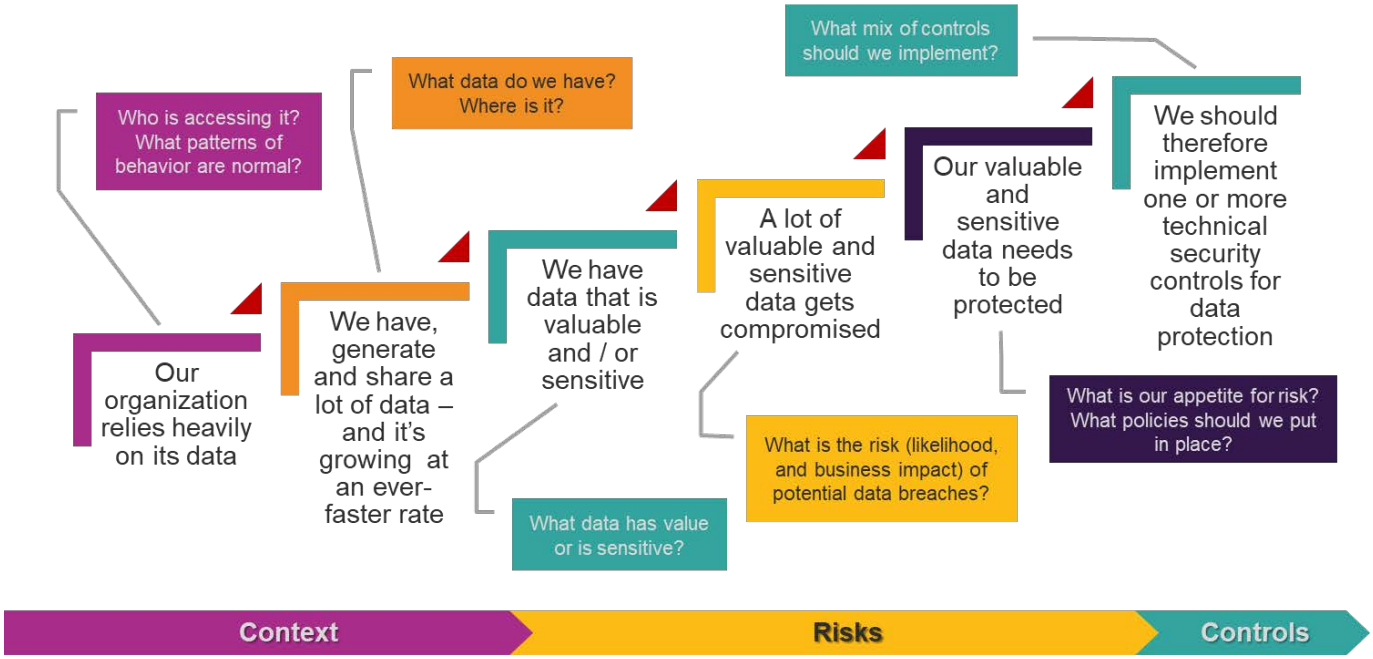
6 out of 7 enterprises (86%) must deal with the complexity of *multiple* types of data and / or data-related processes that are subject to requirements for privacy, security, or compliance.

- **Our valuable and sensitive data needs to be protected** — because a great many security professionals mistakenly believe that the over-arching objective is to counter all threats, eliminate all vulnerabilities, and minimize all risks.
- **We should therefore implement one or more technical security controls for data protection** — which are also in line with this or that framework, standard, or best practice.

Perhaps because we hear them so often, this sequence of statements seems reasonable. In reality, however, each one of these arguments covers up some extremely important questions that the senior business decision makers (who actually own the **risk**) expect their security professionals — in their dual role as *subject-matter experts*, and *trusted advisors* — to help them address (see Figure 2).

Unfortunately, the familiar arguments cover up some extremely important questions that senior business decision makers expect their security professionals — in their dual role as *subject-matter experts* and *trusted advisors* — to help them address.

Figure 2: The Familiar Arguments Seem Reasonable — But They Cover Up Some Extremely Important Questions to be Addressed



Source: Aberdeen, May 2018

Reflecting on Figure 2, we can see that successful data protection initiatives need to consider *all three* interconnected elements: **context**, **risks**, and **controls**. These elements are summarized in Table 1.

Table 1: Three Elements for Making Business Decisions About Safeguarding Sensitive Data: Context, Risks, and Controls

Context	Risks	Controls
What data do we have? Where is it? Who is accessing it? Who should and should not have access? What patterns of behavior are normal?	What data has value? What is the likelihood and business impact of potential data breaches? What is our appetite for risk? What policies should we put in place?	What mix of controls should we implement? Technical Administrative Physical
Visibility, intelligence, and understanding regarding your organization's specific environment	Better-informed business decisions about risks, properly defined	Selection and implementation of the most appropriate mix of security controls for data protection
"Ready"	"Aim"	"Fire"

Source: Aberdeen, May 2018

Ideally, the ultimate mix of technical, administrative, and physical **controls** ("Fire") are selected and implemented based on an up-to-date understanding of **risks** ("Aim"), and risks are understood based on each organization's specific business **context** ("Ready"). In practice, as discussed above, organizations have a strong tendency to be heavy on the "Fire," and light on the "Ready" and "Aim".

Some may legitimately ask: If the overarching purpose and objective of any cyber security initiative is always about *risk*, shouldn't we start there, with "what data has value?" Or shouldn't we start by implementing the "top N" controls, which other organizations have found to have a high payoff in terms of preventing known attacks?

We certainly could get started in the middle. But when it comes to information security, one size does not fit all. Better-informed business decisions about risk are always made in consideration of *context*, *trade-offs*, and management's *appetite for risk*. What's viewed as acceptable or affordable by one organization may be unacceptable or unaffordable to the next. So, focusing on risk is absolutely correct, but business decisions about both risks *and* controls are always framed in the specific context of your business processes, your infrastructure, your applications and data, your users, your industry, your regulatory requirements, your mission,

The order of first understanding *context*, then evaluating *risks*, and then making decisions about *controls* is generally recognized as best practice. For example, the *NIST Framework for Improving Critical Infrastructure Cybersecurity* recommends that organizations **identify their assets**, **understand their business environment**, **establish policies and processes for governance**, and **assess and prioritize risks** — *before* they focus on specific capabilities for **protection, detection, and response**.

your business strategies, and your organization's appetite for risk. Risk, controls, and context are always intertwined.

Characteristics of Successful Data Protection Initiatives

What do successful data protection initiatives look like? Here are three checklists of best practices, as identified by Aberdeen's research.

1. Three Foundational Capabilities for a Data Protection Initiative

To form a solid foundation for an effective data protection initiative, here are three high-level capabilities that your organization needs to have:

- **Data discovery and classification** — e.g., knowing what data you have, where it is, who has (and should have) access to it, and what patterns of access are normal. Organizations must have the ability to *identify* valuable or sensitive data throughout the enterprise, and to *classify* which data is subject to policies or requirements for privacy, security, and compliance.
- **Data governance and data handling** — e.g., implementing the definitions, criteria, awareness, and training necessary for users to *understand their responsibilities* for handling enterprise data, along with the ability to *establish and enforce consistent policies* for data protection throughout the computing infrastructure. Establishing policies for how different classes of data should be handled enables *day-to-day operational decisions*, both by people and by automated business processes.
- **Identification, assessment, and effective communication about risks** — e.g., establishing a clear understanding of the risks related to data privacy, data security, and regulatory compliance in terms of both *likelihood* and *business impact*. In their dual roles as subject-matter experts and trusted advisors, security professionals need to help the owners of data risks make better-informed business decisions regarding how best to manage those risks to an acceptable level.

2. Six Strategies for Technical Security Controls

When your organization is ready to get technology-ready for its data protection initiative, a closer look at the many available technical controls will reveal just **six basic strategies for technical security controls**:

- **Do nothing** — It may sound counterintuitive but doing nothing is always a potential option. Remember, not all risks need to be addressed; some risks are accepted. Not all data needs to be protected, as determined through the foundational capabilities of

Three foundational capabilities:

- Data **discovery** and **classification**
- Data **governance** and data **handling**
- Identification, assessment, and effective communication about **risks**

discovery, *classification*, *governance*, and *risk-based* business decisions.

- **Manage access to the data in a centralized data store** — Valuable or sensitive data is commonly centralized in network *file shares*, on *web servers*, in *enterprise content management systems*, and increasingly in the infrastructure of *cloud service providers*. Access to data in these scenarios is provided only to users who are authenticated and authorized to do so.

- **Monitor and filter the data as it is being accessed and distributed** — Monitoring and filtering technologies such as *data loss prevention*, *email / web security*, *database activity monitoring*, and network-based *monitoring and analytics* are used to gain visibility into the valuable or sensitive data that is being accessed and distributed across the organization's infrastructure. These solutions are also designed to flag data movements that are potentially in violation of policies for privacy, security, and compliance, as well as to guide proper response.

- **Encrypt the data** — The use of *encryption* to protect the confidentiality and integrity of valuable or sensitive data is extremely common in every place that data can be found: in back-end systems, on the network, and on a wide variety of endpoints. A standardized, automated approach to managing the lifecycle of *encryption keys* is essential to support greater scale of encryption, and to reduce the total cost of ongoing operations and management.

- **Substitute non-data for data** — In some scenarios, valuable or sensitive data is best protected by taking it out of the business process, using technologies such as *tokenization*, *format-preserving encryption*, or *data masking*. For example, tokenization is a process that substitutes unique, randomly generated values (*tokens*) to reference valuable or sensitive data (such as payment card data), while maintaining the length and format of the original data to minimize the number of changes required to existing business processes.

- **Apply persistent controls to the data** — Some data protection technologies — including *enterprise rights management*, and some approaches to *enterprise encryption* — are designed to follow along with the data itself, wherever the data flows. This provides the organization with controls over actions which may be taken on valuable or sensitive data, even after it leaves the boundaries of enterprise-managed computing infrastructure.

Six strategies for technical security controls:

- Do nothing
- **Manage access to the data** in a centralized data store
- **Monitor and filter the data** as it is being accessed and distributed
- **Encrypt the data**
- **Substitute non-data for data**
- **Apply persistent controls to the data**

3. Five Considerations for an Enterprise-Wide Encryption Solution

The use of **encryption** is an increasingly adopted strategy for enterprise data protection initiatives. For example, in the context of the European Union **General Data Protection Regulation (GDPR)**, encryption can be used for the *anonymization* of personal data, in which case the data protection regulations for the processing of such information do not apply. Encryption is increasingly being used to help enable the *rewarded risks* of enterprise initiatives such as **digital transformation** or **enterprise collaboration**, by managing the *unrewarded risks* of potential data loss or exposure.

For data protection initiatives based on encryption, here are **five high-level considerations** for selecting an enterprise-wide encryption solution.

- **Ease of use** — Enterprise encryption solutions that are easy to use, and which minimize any kind of friction in day-to-day business processes, will gain much faster acceptance among users while maintaining (or even improving) operational efficiencies.
- **Broad application support** — Enterprise encryption solutions should support the full range of the organization's applications and information resources (e.g., user devices, file servers, mainframes, network storage, cloud-based storage, databases, backup media, and so on).
- **Key management** — As encryption initiatives expand throughout the extended enterprise, a standardized, automated approach to managing the lifecycle of encryption keys becomes essential to support greater scale and complexity, and to reduce the total cost of ongoing operations and management.
- **Standards-based** — The encryption algorithms, cryptographic operations, and encryption key management operations in an enterprise encryption solution should be based on industry standards (e.g., AES, FIPS series, KMIP) and standards-based APIs (e.g., PKCS #11).
- **Platform-based** — In contrast to encryption based on multiple point products, a platform-based approach to enterprise encryption will be easier to integrate, scale, manage, and support over time, minimizing the total cost of ownership for protecting valuable and sensitive data.

Risk is always defined properly in terms of both *how likely*, and *how much business impact*. In many ways, managing risk is like managing cholesterol: it comes in two types, both "bad" and "good." Both involve inherent *uncertainty* — that's what makes them a risk.

Unrewarded risks such as privacy, security, and compliance have to do with *defending assets*, *minimizing downside,* and *protecting value*.

Rewarded risks such as digital transformation and collaboration, have to do with *enabling assets*, *maximizing upside*, and *creating value*.

Five considerations for enterprise-wide encryption:

- **Ease of use**
- **Broad application support**
- **Key management**
- **Standards-based**
- **Platform-based**

Summary and Key Takeaways

- Aberdeen's analysis of the online search activities of more than 62,300 organizations shows that the prevailing approach to enterprise **data protection initiatives** emphasizes **technical controls** over **business context** and **risk** — an approach which can be summed up as "Fire, Ready, Aim."

- Relative to searches on **data protection** / **data security** = 100%:

  - Organizations are placing roughly half as much emphasis on **data discovery** (50%) for identifying the data itself, **data classification** (57%) for identifying the greatest risks, and **data governance** (just 12%) for identifying the most appropriate policies.

  - In contrast, organizations are placing roughly three times as much emphasis on technical controls for data protection such as **data encryption** (183%), which is balanced with other technical strategies such **data loss prevention** (152%) and **secure file transfer** (84%).

- Keeping in mind the over-arching purpose and objective of any cyber security initiative — which is always to help **make better-informed business decisions about risks**, and to help **manage those risks to an acceptable level** — the prevailing emphasis on controls over context and risk is backwards. It puts the "Fire" before the "Ready" and the "Aim." Successful data protection initiatives need all three of these elements, ideally in the logically correct order.

- The hard truth is that under the prevailing approach to data protection initiatives, most organizations are neither **secure** nor **compliant**, despite their considerable **level of investment**:

  - About **3 out of 5 (58%)** enterprises experienced **at least one data breach** over the last 12 months (median = 3).

  - About **3 out of 4 (75%)** enterprises experienced **at least one non-compliance issue** over the last 12 months (median = 3).

  - A **median of 30%** of the **overall IT operations budget (OpEx)** is being allocated to the achievement and reporting / certification of compliance with data privacy and data security requirements.

- Perhaps because we hear them so often, the usual logic behind making the leap to implement technical security controls seems reasonable. In reality, however, each of these arguments covers up some extremely important questions that the senior business

decision makers (who actually *own* the risk) expect their security professionals to help them address. Successful data protection initiatives need to consider *all three* interconnected elements: **context**, **risks**, and **controls**.

- What do successful data protection initiatives look like? Aberdeen's research has helped to identify three checklists of selected best practices.

- Three foundational capabilities for a data protection initiative:

  - **Data discovery and classification**, to identify the data that's valuable or sensitive

  - **Data governance and data handling**, to help users *understand their responsibilities*, and to enable *day-to-day operational decisions*

  - **Identification, assessment, and effective communication about risks**, to help the owners of data risks make better-informed business decisions regarding how to manage those risks to an acceptable level

- Six strategies for technical security controls:

  - **Do nothing**, because not all data needs to be protected

  - **Manage access to the data in a centralized data store**, providing access only to authenticated and authorized users

  - **Monitor and filter the data as it is being accessed and distributed**, to flag data movements that are potentially in violation of policies for privacy, security, and compliance, and to guide proper response

  - **Encrypt the data**, to protect confidentiality and integrity

  - **Substitute non-data for data**, to protect it by removing it from the business process

  - **Apply persistent controls to the data**, to provide the organization with controls over actions which may be taken on valuable or sensitive data, even after it leaves the boundaries of enterprise-managed computing infrastructure

- Five considerations for an enterprise-wide encryption solution:
  - **Ease of use**, to minimize friction in day-to-day business processes and gain faster acceptance by users
  - **Broad application support**, to enable the full range of the organization's applications and information resources
  - **Key management**, to support greater scale and complexity, and to reduce the total cost of ongoing operations and management
  - **Standards-based**, to support flexibility and choice
  - **Platform-based**, to make it easier to integrate, scale, manage, and support the use of encryption over time, and to minimize the total cost of ownership for protecting valuable and sensitive data

Related Research

Ready or Not, GDPR Enforcement is Here: What You Should Probably Be Doing Next; May 2018

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

Overcoming the Two Biggest Obstacles to an Effective Data Security Program; September 2016

The "Ready, Aim, Fire" Approach to Safeguarding Your Sensitive Data; January 2016

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.

This document is the result of primary research performed by Aberdeen Group and represents the best analysis available at the time of publication. Unless otherwise noted, the entire contents of this publication are copyrighted by Aberdeen Group and may not be reproduced, distributed, archived, or transmitted in any form or by any means without prior written consent by Aberdeen Group.

17453