THE "READY, AIM, FIRE" APPROACH TO SAFEGUARDING YOUR SENSITIVE DATA

January 2016

The usual arguments in making a business case to implement some particular technical security control as the means to safeguard an organization's sensitive data sound familiar, and seem reasonable. But in reality, these decisions should actually be driven by three interconnected parts: context ("ready"), risk ("aim"), and controls ("fire"). The order is important!

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

The usual logic sounds familiar, and seems reasonable.

Whenever someone is making a business case to implement some particular technical security control or another as the means to safeguard an organization's sensitive data, it's not uncommon to hear 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, and countless other mission-critical business processes.
- **We have a lot of data** — and we are continuously generating even more of it, at an ever-faster rate.
- **A lot of our data is sensitive or valuable** — a point which is reflected in a complex mix of requirements for security, privacy, and regulatory compliance.
- **A lot of sensitive and valuable data gets compromised** — as evidenced by the never-ending headlines of public data breach disclosures.
- **Our sensitive and valuable data needs to be protected** — because the objective of information security

➔ Related research: *Understanding the Risks to Your Organization's Structured Data*

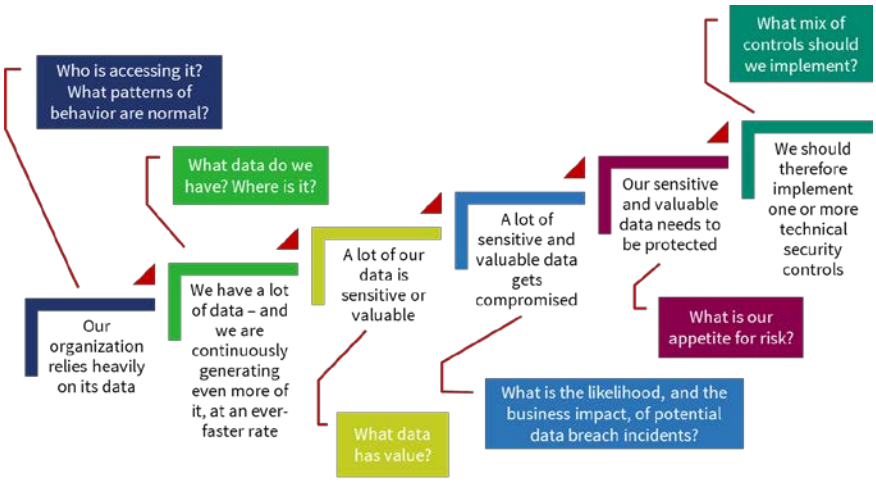
(according to a great many information security practitioners) is to counter all threats, eliminate all vulnerabilities, and minimize all risk.

➔ **We should therefore implement one or more technical controls for data security**, which are also in line with this or that standard or best practice — the case that has just been outlined is the justification for this investment.

Perhaps because we hear them so often, this sequence of points sounds very familiar, and seems pretty reasonable. In reality, however, each one of these arguments covers up some extremely important questions that business decision-makers expect security professionals — in their dual role as *subject matter experts*, and *trusted advisors* — to help them address (see Figure 1).

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

Figure 1: The Usual Logic Sounds Familiar, and Seems Reasonable — But It Covers Up Several Important Questions



Source: Aberdeen Group, December 2015

By reflecting more carefully on Figure 1, we can see that the drivers for making decisions about safeguarding sensitive data can actually be grouped into three interconnected parts: **context**, **risk**, and **controls**. These are re-summarized in Table 1.

The drivers for making business decisions about safeguarding sensitive data can be grouped into three interconnected parts: *context*, *risk*, and *controls*. The order of these considerations is actually important.

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

Context	Risk	Controls

• What data do we have?
• Where is it?
• Who is accessing it?
• What patterns of behavior are normal?
	• What data has value?
	• What is the likelihood, and the business impact, of potential data breach incidents?
	• What is our appetite for risk?
		• What mix of controls should we implement?
		  ○ Technical
		  ○ Administrative
		  ○ Physical

Visibility, intelligence, and analytics about your organization's specific environment	Smarter, more effective, risk-based business decisions	Selection of the most appropriate mix of security controls
"Ready"	"Aim"	"Fire"

Source: Aberdeen Group, December 2015

The order of these considerations is actually pretty important. Ideally, controls are implemented based on an up-to-date understanding of risk, and risk is based on each organization's specific business context. In reality, Aberdeen's benchmark data indicates that organizations have primarily been oriented towards implementing technical controls for data protection — heavy on "Fire," and light on "Ready" and "Aim" (see Figure 2):

- **Context:** although about two-thirds (63%) of all respondents currently *capture logs* related to data movements, this doesn't necessarily mean that anything is being done with this information. Just one-third (35%) have established some kind of standardized *monitoring, analysis, and reporting* about their data movements, and only one in four (26%) currently have *consistent, unified visibility* into what's happening throughout their environment.

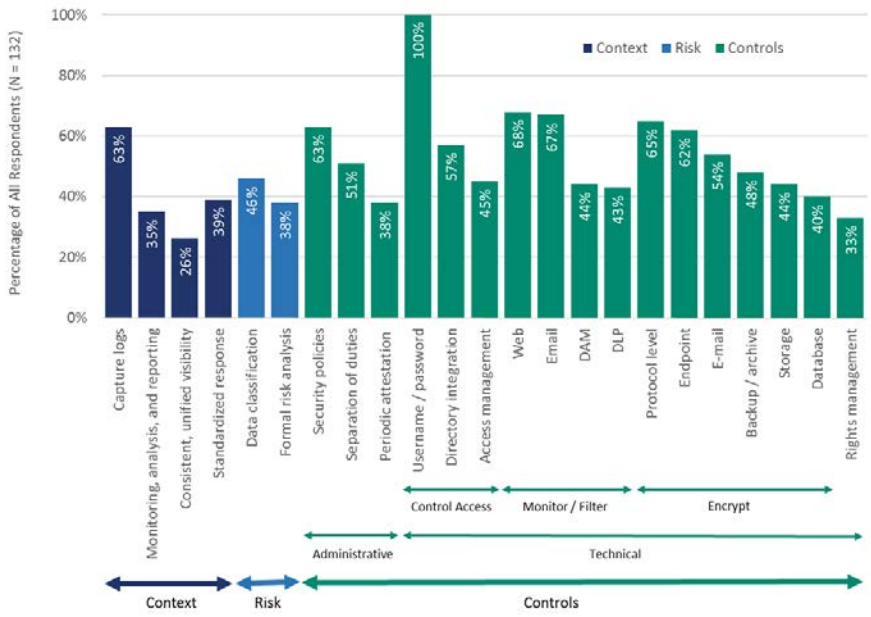
- **Risk:** less than half (46%) of all respondents have *classified* their data, e.g., based on requirements for confidentiality, integrity, and availability, or based on the

The order of understanding *context* first, then evaluating *risk*, 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**.

value of the business processes it supports. Even fewer (38%) have done a formal *risk analysis*.

➔ **Controls:** about two-thirds (63%) of all respondents have established and communicated *policies* about information security, but only half (51%) have implemented foundational administrative controls such as *separation of duties*, and fewer still (38%) perform periodic *attestation* that the right users have the right access to the right information. A majority of organizations, however, have implemented one or more technical controls to safeguard their sensitive information, using a variety of implicit strategies. The current level of adoption for several illustrative examples of these controls is shown in Figure 2.

Figure 2: Organizations Have Primarily Been Oriented Towards Implementing Technical Controls for Data Protection – Heavy on "Fire," Light on "Ready" and "Aim"



Source: Aberdeen Group, December 2015

Examples of Foundational Administrative Controls:

- **Need to Know** — Limit access to the specific information required to perform the currently assigned task.
- **Least Privilege** — Limit access to the minimum amount of information for the minimum amount of time to perform the required duties.
- **Separation of Duties** — Split up tasks in such a way that more than one individual is responsible for their completion.
- **Attestation** — Periodic review of identities, roles, and access privileges to ensure ongoing alignment with policies and necessary capabilities.

A superabundance of options for technical security controls can make it painfully difficult for the security team in any given organization to evaluate all the alternatives, and to make the necessary choices for the mix of controls that represents the best fit for their specific context and appetite for risk.

Why Controls-First Strategies Makes Less Sense, But Still Happen

The single biggest problem with a controls-first strategy for safeguarding your sensitive data is that **there are so many technical security controls from which to choose**! As Aberdeen noted in *Flash Forward: Putting "Critical Security Controls" in Perspective* (January 2015), solution providers have made available a rich and complex array of data security technologies. On the one hand, the result of such innovation and investment is a testament to the importance of safeguarding sensitive data. On the other hand, having such a superabundance of options can make it painfully difficult for the security team in any given organization to evaluate all the alternatives, and to make the necessary choices for the mix of controls that represents the best fit for their specific context and appetite for risk.

In reality, the challenge is even worse than that. Security teams have the Sisyphean task of not only **figuring out what to do** (through "the fog of more"), but also **persuading business decision-makers that it's worth doing**, actually **doing it**, and **sustaining those activities over time** — all in rapidly evolving conditions.

One industry response has been a gravitation towards a set of so-called "top 20 technical security controls." Aberdeen has abstracted these 20 technical controls into eight higher-level, foundational capabilities — four of which are particularly relevant to this discussion:

- ➔ Understand what users, systems, applications, and data are in your environment
- ➔ Maintain visibility into what's happening in your environment
- ➔ Protect your important data
- ➔ Be in a position to respond when something goes wrong

Once again, these bring us back to exactly the same conclusion about *context*, *risk*, and *controls*: controls should be implemented based on an up-to-date understanding of risk, and risk assessments should be based on each organization's specific business context. **The fundamental question becomes whether your organization has the visibility and insights it needs into its own data to make risk-based decisions about what controls to implement.**

Said another way, having visibility, intelligence, and analytics relevant to your specific environment is the foundation for making smarter, more effective, risk-based decisions about the most appropriate mix of technical, administrative, and physical controls for safeguarding your sensitive data. If your organization doesn't currently have these capabilities, they should move to the top of your wish list for security budgets and initiatives in 2016 and beyond.

Having visibility, intelligence, and analytics relevant to your specific environment is the foundation for making smarter, more effective, risk-based decisions about the most appropriate mix of technical, administrative, and physical controls for safeguarding your sensitive data.